MINISTERUL FINANŢELOR PUBLICE
UNITATEA CENTRALĂ DE ARMONIZARE PENTRU AUDITUL PUBLIC INTERN

GHID PRACTIC

MISIUNEA DE AUDIT INTERN ACTIVITATEA IT

- ACTUALIZAT -

AVIZAT
GHIŢĂ MARCEL
Şef serviciu pentru Strategie şi Metodologie Generală

ACTUALIZAT
CROITORU ION
Auditor superior

VOINEA DANIEL
Auditor principal

Ghidul practic privind realizarea unei misiuni de audit intern privind activitatea IT constituie un model pentru desfăşurarea misiunilor în baza Legii nr. 672/2002 privind auditul public intern şi a Normelor generale pentru exercitarea auditului public intern aprobate prin OMFP nr. 38/2003, cu modificările şi completările ulterioare.

Aşteptăm sugestiile dumneavoastră pe adresa UCAAPI sau pe e-mail:

marcel.ghita@mfinante.ro
ion.croitoru@mfinante.ro
daniel.voinea@mfinante.ro

BUCUREŞTI
2009

CUVÂNT ÎNAINTE

Ghidul de audit intern privind auditarea activităţii IT **reprezintă un model practic de desfăşurare a unei misiuni de audit intern, prin parcurgerea in detaliu, a fiecărui pas, într-o manieră didactică. Ghidul poate fi utilizat de entităţile din sectorul public şi în acelaşi timp va reprezenta suportul pentru realizarea, de către fiecare structură de audit intern a propriului ghid practic specific activităţii IT desfăşurate în cadrul entităţii.**

Actualizarea ghidului are la bază prevederile art. 8 lit. c) din *Legea nr. 672/2002 privind auditul public intern şi punctul 4, Partea I din Normele generale de exercitare a auditului public intern, aprobate prin OMFP nr. 38/2003* referitoare la dezvoltarea şi implementarea unor proceduri şi metodologii uniforme, bazate pe standardele internaţionale.

În conformitate cu prevederile punctului 4, Partea I din *Normele generale de exercitare a auditului public intern,* aprobate prin OMFP nr. 38/2003 (Manualul de audit intern), misiunea de audit intern are drept scop evaluarea sistemelor de management şi control intern ale entităţii, urmărind transparenţa şi conformitatea cu cadrul normativ.

Actualizarea ghidului practic a presupus respectarea procedurilor şi documentelor specifice structurate pe cele patru etape ale derulării unei misiunii de audit public intern, prezentate prin normele generale, respectiv:

- *în etapa de pregătire a misiunii de audit intern* au fost elaborate şi actualizate documentele prevăzute de normele generale, fiind aduse clarificări, în special, cu privire la modul concret de dezvoltare a procedurii de *Analiza riscurilor*, succesiunea documentelor, structura acestora şi modul de completare, nivelul de apreciere şi împărţire a riscurilor în mari, medii şi mici, clasarea şi ierarhizarea acestora în vederea finalizării procedurii pe baza căreia se va elabora *Programul intervenţiei la faţa locului* şi se va concentra munca pe teren.
- *în etapa de intervenţie la faţa locului* s-a realizat testarea pe teren a operaţiilor auditabile, pe baza *Programului intervenţiei la faţa locului*, prin utilizarea diferitelor tehnici şi instrumente de audit, tehnici de eşantionare, liste de verificare, teste, foi de lucru, interviuri sau note de relaţii, elemente care s-au constituit în probe de audit şi care au stat la baza întocmirii FIAP-urilor şi FCRI-urilor, documente avute în vedere la elaborarea raportului de audit intern.
- *în etapa de elaborare a Raportului de audit intern* s-a urmărit structurarea acestuia pe *Tematica în detaliu a misiunii de audit* obţinută în procedura de *Analiza riscurilor* şi ca acesta să comunice clar cititorului atât obiectivele, perioada de timp acoperită de audit, aria de cuprindere, constatările, concluziile auditului, recomandările formulate, cât şi nivelul de asigurare. Totodată s-a avut în vedere ca faptele prezentate să fie susţinute cu dovezi de audit suficiente, iar recomandările să abordeze chestiunea performanţei, a eficacităţii gestionării şi optimizării utilizării resurselor.
- *în etapa de urmărire a recomandărilor* s-a urmărit caracterul adecvat, eficacitatea şi oportunitatea acţiunilor întreprinse pentru implementarea recomandărilor formulate şi în afara documentelor stabilite de normele generale au fost propuse unele modele de documente pentru evaluarea internă şi externă a activităţii de audit intern.

Obiectivele misiunii de audit intern privind activitatea IT, stabilite prin planul de audit au fost următoarele:

- *Strategia şi planificarea sistemelor informatice;*
- *Organizarea şi funcţionarea departamentului IT;*
- *Operaţii ale sistemului informatic;*
- *Securitatea informaţiilor;*
- *Achiziţionarea şi testarea programelor şi aplicaţiilor;*
- *Elaborarea şi implementarea proiectelor IT;*
- *Proiectarea şi menţinerea în funcţiune a unei reţele.*

În continuare, prezentăm desfăşurarea misiunii de audit intern pentru *Activitatea IT*, structurată pe etapele, procedurile şi documentele care se elaborează pe baza acestora în conformitate cu *Schema de derulare a misiunilor de audit intern.*

ENTITATEA PUBLICĂ
Serviciul Audit Intern
Nr. 11/12.08.2009

ORDIN DE SERVICIU

În conformitate cu prevederile art. 8, litera c) din Legea nr. 672/2002 privind auditul public intern, a OMFP nr. 38/2003 de aprobare a normelor metodologice generale privind exercitarea activităţii de audit intern, cu modificările şi completările ulterioare şi a Planului de audit intern pentru anul 2009, se va efectua o **misiune de audit intern privind Activitatea IT,** în perioada 01.09.2009 – 20.10.2009.

Scopul misiunii de audit este de a da asigurări asupra modului de organizare şi desfăşurare a activităţii IT, în conformitate cu cadrul legislativ şi normativ, iar obiectivele acestuia au în vedere:

- *Strategia şi planificarea sistemelor informatice;*
- *Organizarea şi funcţionarea departamentului IT;*
- *Operaţii ale sistemului informatic;*
- *Securitatea informaţiilor;*
- *Proiectarea şi testarea programelor şi aplicaţiilor;*
- *Elaborarea şi implementarea proiectelor IT;*
- *Proiectarea şi menţinerea în funcţiune a unei reţele.*

Menţionăm că se va efectua un audit de conformitate privind modul de organizare şi desfăşurare a activităţii IT.

Echipa de auditori interni este formată din următorii auditori:

- **Popescu Sorin, auditor superior, coordonator**
- **Radu George, auditor superior**

Şef Serviciu Audit Intern,
Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern

DECLARAŢIA DE INDEPENDENŢĂ

Nume şi prenume: Popescu Sorin
Misiunea de audit : Activitatea IT Data: 14.08.2009

Incompatibilităţi în legătură cu entitatea/structura auditată	**DA**	**NU**
Aţi avut/aveţi vreo relaţie oficială, financiară sau personală cu cineva care ar putea să vă limiteze măsura în care puteţi să vă interesaţi, să descoperiţi sau să constataţi slăbiciuni de audit în orice fel?	-	X
Aveţi idei preconcepute faţă de persoane, grupuri, organizaţii sau obiective care ar putea să vă influenţeze în misiunea de audit?	-	X
Aţi avut/aveţi funcţii sau aţi fost/sunteţi implicat(ă) în ultimii 3 ani într-un alt mod în activitatea entităţii/structurii ce va fi auditată?	X	-
Aveţi responsabilităţi în derularea programelor şi proiectelor finanţate integral sau parţial de Uniunea Europeană?	-	X
Aţi fost implicat în elaborarea şi implementarea sistemelor de control ale entităţii/structurii ce urmează a fi auditată?		X
Sunteţi soţ/soţie, rudă sau afin până la gradul al patrulea inclusiv cu conducătorul entităţii/structurii ce va fi auditată sau cu membrii organului de conducere colectivă?	-	X
Aveţi vreo legătură politică, socială care ar rezulta dintr-o fostă angajare sau primirea de redevenţe de la vreun grup anume, sau organizaţie sau nivel guvernamental?	-	X
Aţi aprobat înainte facturi, ordine de plată şi alte instrumente de plată pentru entitatea/structura ce va fi auditată?	X	-
Aţi ţinut anterior contabilitatea la entitatea/structura ce va fi auditată?	-	X
Aveţi vreun interes direct sau unul de fond financiar indirect la entitatea/structura ce va fi auditată?	-	X
Puteţi să selectaţi responsabilităţile şi problemele, să stabiliţi riscurile specifice activităţilor supuse auditări şi să construiţi proceduri specifice de identificare a disfuncţiilor şi abaterilor?	X	-
Stăpâniţi tehnicile şi metodele de colectare, analiză şi interpretare a datelor şi informaţiilor specifice unui audit al conformităţii?	X	-
Dacă în timpul misiunii de audit apare orice incompatibilitate personală, externă sau organizaţională care ar putea să vă afecteze abilitatea de a lucra şi a face rapoartele de audit imparţiale, notificaţi şeful Serviciului de audit intern de urgenţă?	X	-

Auditor, **Şef serviciu**
Popescu Sorin Dumitru Daniel

1**. Incompatibilităţi personale**: Cu aproximativ 2 ani în urma am a lucrat la compartimentul contabilitate şi am realizat plata salariilor personalului IT.
2. **Pot fi eliminate incompatibilităţile:** Da
3. **Dacă da, explicaţi cum anume**: Misiunea planificata nu are nici o tangenţă cu activitatea de salarizare a personalului departamentului. Totodată prezenta misiune are ca obiective modul de funcţionare a sistemelor IT.

Data: 14.08.2009 Semnătura: Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern

DECLARAŢIA DE INDEPENDENŢĂ

Nume şi prenume: Radu George Data: 14.08.2009
Misiunea de audit: Activitatea IT

Incompatibilităţi în legătură cu entitatea/structura auditată	**DA**	**NU**
Aţi avut/aveţi vreo relaţie oficială, financiară sau personală cu cineva care ar putea să vă limiteze măsura în care puteţi să vă interesaţi, să descoperiţi sau să constataţi slăbiciuni de audit în orice fel?	-	X
Aveţi idei preconcepute faţă de persoane, grupuri, organizaţii sau obiective care ar putea să vă influenţeze în misiunea de audit?	-	X
Aţi avut/aveţi funcţii sau aţi fost/sunteţi implicat(ă) în ultimii 3 ani într-un alt mod în activitatea entităţii/structurii ce va fi auditată?	X	-
Aveţi responsabilităţi în derularea programelor şi proiectelor finanţate integral sau parţial de Uniunea Europeană?	-	X
Aţi fost implicat în elaborarea şi implementarea sistemelor de control ale entităţii/structurii ce urmează a fi auditată?	-	X
Sunteţi soţ/soţie, rudă sau afin până la gradul al patrulea inclusiv cu conducătorul entităţii/structurii ce va fi auditată sau cu membrii organului de conducere colectiva?	-	X
Aveţi vreo legătură politică, socială care ar rezulta dintr-o fostă angajare sau primirea de redevenţe de la vreun grup anume, sau organizaţie sau nivel guvernamental?	-	X
Aţi aprobat înainte facturi, ordine de plată şi alte instrumente de plată pentru entitatea/structura ce va fi auditată?	-	X
Aţi ţinut anterior contabilitatea la entitatea/structura ce va fi auditată?	-	X
Aveţi vreun interes direct sau unul de fond financiar indirect la entitatea/structura ce va fi auditată?	-	X
Puteţi să selectaţi responsabilităţile şi problemele, să stabiliţi riscurile specifice activităţilor supuse auditări şi să construiţi proceduri specifice de identificare a disfuncţiilor şi abaterilor?	X	-
Stăpâniţi tehnicile şi metodele de colectare, analiză şi interpretare a datelor şi informaţiilor specifice unui audit al conformităţii?	-	X
Dacă în timpul misiunii de audit apare orice incompatibilitate personală, externă sau organizaţională care ar putea să vă afecteze abilitatea de a lucra şi a face rapoartele de audit imparţiale, notificaţi şeful Serviciului de audit intern de urgenţă?	X	-

Auditor, **Şef serviciu**
Radu George Dumitru Daniel

1. Incompatibilităţi personale:
a) nu am cunoştinţe solide privind managementul IT, astfel încât să pot face o analiză obiectivă a modului de funcţionare a programelor şi aplicaţiilor.
2. Pot fi eliminate incompatibilităţile:
a) Da;
3. Dacă da, explicaţi cum anume:
a) pentru evaluarea sistemelor, aplicaţiilor sau programelor echipa de audit se va suplimenta cu un auditor cu experienţă în acest domeniu, respectiv Ionescu Gabriel, acesta va avea ca responsabilităţi să evalueze modul de funcţionare a acestora în comparaţie cu necesităţile şi să formuleze constatările de audit.
Data: 14.08.2009 Semnătura: Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern
Nr. 3452 / 15.08.2009

NOTIFICAREA PRIVIND DECLANŞAREA MISIUNII DE AUDIT INTERN

Către: Departamentul Tehnologia Informaţiei
De la: Şeful Serviciului Audit Intern

Referitor la misiunea de audit intern „Activitatea IT"

Stimate domnule director Pătrulescu George

În conformitate cu Planul de audit intern pe anul 2009, urmează ca în perioada 01.09.2009 - 30.09.2009 să efectuăm o misiune de audit intern având ca temă **Activitatea IT.**

Echipa de auditori va examina responsabilităţile asumate de către Departamentul IT cu privire la organizarea şi realizarea activităţilor şi va determina dacă acesta îşi îndeplineşte obligaţiile în mod efectiv şi eficient.

Perioada supusă evaluării este 01.01.2008 – 30.06.2009;

Obiectivele misiuni de audit intern vor fi reprezentate de:

- *Strategia şi planificarea sistemelor informatice;*
- *Organizarea şi funcţionarea departamentului IT;*
- *Operaţii ale sistemului informatic;*
- *Securitatea informaţiilor;*
- *Testarea programelor şi aplicaţiilor;*
- *Elaborarea şi implementarea proiectelor IT;*
- *Proiectarea şi menţinerea în funcţiune a unei reţele.*

Vă vom contacta ulterior pentru a stabili de comun acord şedinţa de deschidere în vederea discutării diverselor aspecte ale misiunii de audit intern, cuprinzând:

- prezentarea auditorilor;
- prezentarea si discutarea obiectivelor misiunii de audit intern;
- scopul misiunii de audit intern;
- programul intervenţiei la faţa locului;
- alte aspecte privind organizarea si desfăşurarea misiunii.

Pentru o mai bună înţelegere a activităţii dumneavoastră, vă rugăm sa ne puneţi la dispoziţie următoarea documentaţie necesară:

- cadrul legal si de reglementare aplicabil entităţii;
- organigrama departamentului;
- Regulamentul de organizare şi funcţionare;
- fişele posturilor;

- procedurile scrise care descriu activităţile ce se desfăşoară în cadrul compartimentului;
- rapoartele de audit intern anterioare;
- alte rapoarte, note, dosarele anterioare care se referă la aceasta temă.

Dacă aveţi unele întrebări privind aceasta acţiune, vă rog să contactaţi pe domnul Popescu Sorin – auditor intern, coordonatorul misiunii sau pe şeful structurii de audit intern.

Şef Serviciu Audit Intern,
Dumitru Daniel

Data: 15.08.2009

Procedura – P04: COLECTAREA ŞI PRELUCRAREA INFORMAŢIILOR

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

COLECTAREA INFORMAŢIILOR

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 02.09.2009
Avizat: Dumitru Daniel Data: 02.09.2009

Colectarea informaţiilor				
Nr. crt.	**Departamentul IT**	**DA**	**NU**	**Observaţii**
1.	Identificarea legilor şi regulamentelor aplicabile Departamentului IT;	X	-	
2.	Obţinerea organigramei departamentului IT;	X	-	
3.	Obţinerea Regulamentului de organizare şi funcţionare aferent departamentului IT;	X	-	ROF-ul nu este actualizat în conformitate cu noua structură organizatorică a departamentului.
4.	Obţinerea fişelor posturilor pentru personalul departamentului;		X	
5.	Obţinerea procedurilor de lucru elaborate la nivelul departamentului;		X	Procedurile de lucru sunt elaborate doar pentru o parte din activităţile desfăşurate la nivelul departamentului.
6.	Obţinerea fişelor postului pentru personalul departamentului;	X	-	
7.	Obţinerea Raportului de audit intern anterior;	X	-	Anterior nu au fost realizate misiuni de audit intern privind activitatea IT
8.	Obţinerea strategiei şi politicilor de dezvoltare ale departamentului;	X		
9.	Obţinerea statului de funcţii pentru personalul departamentului;	X		
10.	Obţinerea rapoartelor de evaluare pentru personalul departamentului;	X		
11.	Obţinerea planului de continuare a activităţilor în caz de dezastre;	X		
12.	Obţinerea circuitului documentelor la nivelul departamentului;		X	Nu există stabilit un circuit al documentelor.
13.	Identificarea obiectivelor generale şi specifice definite la nivelul departamentului;	X		
14.	Obţinerea planului de recuperare a activităţilor în caz de dezastre;	X		
15	Obţinerea listei tuturor aplicaţiilor, programelor, sistemelor achiziţionate sau derulate în cadrul entităţii	X		

16	Obţinerea listei privind fiecare post IT şi numele utilizatorilor	X		
17	Obţinerea tuturor metodologiilor de lucru privind funcţionarea aplicaţiilor şi programelor instalate în cadrul organizaţiei	X		

Notă:

Colectarea şi prelucrarea reprezintă etapa de procurare a informaţiilor în vederea efectuării analizei de risc şi pentru identificarea informaţiilor necesare, fiabile, pertinente şi utile pentru a atinge obiectivele misiunii de audit intern.

Activităţile realizate în această fază contribuie substanţial la cunoaşterea domeniului auditabil care îl ajută pe auditor să se familiarizeze cu entitatea auditată.

Procedura PO4 : COLECTAREA ŞI PRELUCRAREA INFORMAŢIILOR

Entitatea Publică
Serviciul de Audit Intern

CHESTIONAR DE LUARE LA CUNOŞTINŢĂ

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 02.09.2009
Avizat: Dumitru Daniel Data: 02.09.2009

Nr. crt.	ÎNTREBAREA	DA	NU	OBSERVAŢII
	Cunoaşterea contextului socio-economic de funcţionare a departamentului IT			
1	Care este numărul salariaţilor departamentului?			25 salariaţi.
2	Există un buget al departamentului?			Există buget la nivel de organizaţie, iar achiziţiile IT sunt stabilite separat.
3	Care sunt atribuţiile generale ale compartimentului?			Elaborarea strategiei de informatizare a organizaţiei şi realizarea sistemului informatic integrat
4	Atribuţiile generale sunt acoperite în totalitate de sarcinile stabilite posturilor?			
5	Care este nivelul de competenţe al salariaţilor?			Salariaţii deţin competenţe privind funcţionarea echipamentelor, aplicaţiilor şi programelor, în a realiza testarea şi implementarea noilor aplicaţii, în soluţionarea problemele apărute în funcţionarea aplicaţiilor.
6	Care este nivelul de calificare al personalului?			8 salariaţi sunt asistenţi, 9 sunt principali şi 8 sunt superiori.
7	Tot personalul are calificare IT?			
8	Personalul este evaluat cel puţin anual?			
9	Complexitatea obiectivele individuale este îmbunătăţită anual, în corelaţie de cunoştinţele acumulate?			Sunt menţinute anual la acelaşi nivel.
10	Aprecierea realizării obiectivelor este realizată în funcţie de nivelul de criteriile de performanţă?			
11	Posturile existente asigură realizarea activităţilor?			Însă acestea au un grad de ocupare de 85%.
12	Există un sistem de motivare al salariaţilor?	Da		Motivarea se face financiar
13	Motivarea morală a salariaţilor există în cadrul compartimentului?		Nu	
14	Există un plan de carieră definit pentru funcţia de operator IT?		Nu	
15	Există o politică elaborată la nivelul domeniului de activitate?		Nu	
16	Există strategie elaborată privind dezvoltarea IT?	Da		
17	Există o evaluare a funcţionalităţii compartimentului IT?		Nu	
18	Abilităţile de comunicare şi profesionale ale personalului se urmăresc a fi dezvoltate?		Nu	

19	Relaţiile de autoritate sunt definite şi aplicate la nivelul departamentului IT?	Da		
20	Relaţiile ierarhice asigură o bună colaborare între posturile de conducere şi cele de execuţie?	Da		
21	Sarcinile sunt astfel definite încât să asigure o bună cooperare între posturile de acelaşi nivel în vederea soluţionării problemelor?	Da		
22	Relaţiile de control stabilite personalului conduc la o evaluare adecvată a modului de utilizare a echipamentelor şi aplicaţiilor de către utilizatori?	Da		
23	Capacitatea managerială a personalului asigură furnizarea adecvată a informaţiilor către utilizatorii aplicaţiilor?	Da		
24	Structura organizatorică este capabilă să răspundă cerinţelor organizaţiei sau a mediului în care acţionează?	Da		
25	Există o analiză SWOT la nivelul departamentului?		Nu	
B	**Cunoaşterea contextului organizaţional al departamentului IT**			
1	Care este subordonarea departamentului şi compartimentelor componente?			În subordinea conducătorului organizaţiei.
2	Cu cine are relaţii de colaborare?			Cu toate celelalte compartimente.
3	Care sunt relaţiile ierarhice?			Subordonat conducătorului instituţiei, nu are compartimente în subordine.
4	În cadrul compartimentului care sunt relaţiile ierarhice?			Directorul este subordonat conducătorului entităţii, şefii de servicii sunt subordonaţi directorului, iar salariaţii sunt subordonaţi sefului de serviciu.
5	Mai există şi alte funcţii de conducere?		Nu	
6	Există organigramă la nivelul departamentului?	Da		
7	Organigrama exprimă corect relaţiile ierarhice?	Da		
8	Organigrama exprimă relaţiile cu celelalte compartimente?	Da		
9	Există obiective definite la nivelul departamentului şi în cadrul serviciilor?	Da		
10	Există obiective individuale la nivelul posturilor de lucru?	Da		
11	Există fişe ale posturilor pentru toate posturile existente în cadrul compartimentului?	Da		
12	Fişele posturilor sunt întocmite în funcţie de complexitatea activităţilor stabilite postului sau pregătirea persoanei care îl ocupă?			În funcţie de complexitatea activităţilor
13	Sarcinile sunt definite clar în cadrul postului?	Da		
14	În cadrul fişelor posturilor sunt definite responsabilităţi?	Da		
15	Atribuţiile posturilor de conducere diferă faţă de cele ale posturilor de execuţie?	Da		
16	Există asigurată continuitatea activităţilor în cadrul compartimentului?	Da		
17	Există o diagramă funcţională la nivelul compartimentului?		Nu	
18	Nivelul de conducere are putere decizională?			Doar în ce priveşte asigurarea funcţionării echipamentelor, aplicaţiilor sau programelor
19	Există un circuit al documentelor în cadrul departamentului?		Nu	
20	Toate documentele elaborate la nivelul departamentului sunt cuprinse în circuitul documentelor?	Da		
21	Sarcinile sunt comunicate zilnic salariaţilor?	Da		
22	Urmărirea realizării sarcinilor de către salariaţi este realizată	Da		

	zilnic?			
23	Structura organizatorică răspunde necesităţilor activităţilor derulate?			Toţi salariaţi sunt implicaţi în realizarea tuturor activităţilor. Este necesară o compartimentare a activităţilor şi o specializare pe acestea a salariaţilor
24	Ştatul de funcţii corespunde posturilor existente?	Da		
25	Există un sistem de promovare al salariaţilor?			Promovare se face în condiţiile stabilite de lege
26	Posturile de lucru asigură flexibilitate în realizarea activităţilor alocate?	Da		
27	Există o situaţie a raportărilor de efectuat?	Da		
28	Pentru fiecare raportare există o metodologie de colectare, prelucrare şi transmitere a datelor?			Datele sunt preluate din registrele de evidenţă şi dosarele de instanţă
29	Structura organizatorică corespunde scopurilor şi obiectivelor generale ale organizaţiei?	Da		
30	Nivelurile de conducere sunt reduse?			Există două nivele de conducere
31	Funcţiile compartimentelor sunt definite clar şi concis în comparaţie cu atribuţiile alocate departamentului?	Da		
32	Funcţiile managementului se regăsesc în atribuţiile personalului de conducere?			Nu în totalitate
33	Atribuţiile stabilite departamentului IT asigură realizarea atribuţiilor generale ale organizaţiei?	Da		
34	Activităţile sunt identificate în totalitate la nivelul departamentului?	Da		
35	Realizarea activităţilor are la bază un set de indicatori stabiliţi?		Nu	
36	Activităţile asigură conformitatea cu reglementările şi metodologiilor?	Da		
37	Activităţile asigură conformitatea cu procedurile elaborate?	Da		
38	Este respectat principiul echilibrului dintre sarcini şi competenţe?	Da		
39	Concordanţa cerinţelor postului cu caracteristicile titularului asigură corespondenţa dintre volumul, natura şi complexitatea sarcinilor, competenţelor şi responsabilităţilor postului cu aptitudinile, deprinderile şi experienţa acestuia?	Da		
40	Elaborarea rapoartelor de activitate respectă conţinutul tematic?	Da		
41	Lucrările de sinteză şi raportare sunt aprobate de conducerea entităţii?	Da		
C	**Cunoaşterea funcţionării departamentului IT**			
1	Fisa postului defineşte clar cerinţele postului?	Da		
2	Nivelul de cunoştinţe al salariatului asigură realizarea sarcinilor postului pe care îl ocupă?	Da		
3	În cadrul departamentului sunt elaborate procedurile de lucru?	Da		
4	Procedurile de lucru acoperă toate activităţile?	Da		
5	Procedurile de lucru descriu corect activităţile ce trebuie desfăşurate?	Da		
6	Procedurile de lucru definesc corect responsabilităţile?	Da		
7	Procedurile de lucru sunt cunoscute şi aplicate de salariaţi?	Da		
8	Procedurile de lucru asigură separarea sarcinilor?	Da		
9	Există regulament de organizare şi funcţionare?	Da		
10	Regulamentul de organizare şi funcţionare defineşte corect	Da		

	atribuţiile compartimentului?			
11	Există registru de corespondenţă la nivelul departamentului?	Da		
12	Care sunt problemele la nivelul departamentului?			Lipsa de personal. Insuficienţa bugetului pentru achiziţionarea echipamentelor şi integrarea datelor Tehnica învechită, ceea ce creează a serie de probleme în exploatarea aplicaţiilor Instruirea insuficientă a utilizatorilor
13	Care sunt reformele la nivelul departamentului?			Nu există elaborată nici o reformă.
14	Există a procedură de lucru prin care sunt stabilite sau reglementate raporturile de lucru între compartimentele din cadrul organizaţiei?		Nu	
15	Există realizată în cadrul departamentului IT o analiză a posturilor?		Nu	
16	Există un program de pregătire a personalului?	Da		
17	Programul de pregătire are la bază necesităţile rezultate din evaluarea performanţelor individuale şi nevoile individuale?			Programul este realizat pe baza solicitărilor formulate de salariaţi
18	Documentele primite la nivelul departamentului se înregistrează şi repartizează pentru soluţionare?	Da		

Auditori interni,
Popescu Sorin
Radu George

Procedura PO5 :	Analiza riscului

Entitatea Publică
Serviciul de Audit Intern

LISTA CENTRALIZATOARE A OBIECTELOR AUDITABILE

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 04.09.2009
Avizat: Dumitru Daniel Data: 04.09.2009

Nr. crt.	Domeniul	Activităţi/obiective	Obiecte auditabile	Observaţii
1.	Strategia şi planificarea sistemelor informatice	1.1. Strategia IT este concordantă cu scopurile organizaţiei	1.1.1. Strategia IT defineşte necesităţile şi priorităţile	
			1.1.2. Strategia IT face trimitere la nevoile viitoare ale organizaţiei	
			1.1.3. Strategia defineşte direcţiile şi obiectivele de dezvoltare a IT	
		1.2. Planurile IT se adresează întregii organizaţii	1.2.1. Strategia IT este transpusă în planuri IT	
			1.2.2. Planurile IT ajută la îndeplinirea misiunii organizaţiei	
			1.2.3. Planurile IT oferă asigurare cu privire la faptul că resursele IT sunt alocate în concordanţă cu necesităţile	
		1.3. Obiectivele IT îndeplinesc obiectivele organizaţiei	1.3.1. Strategia IT este concordantă cu scopurile organizaţiei	
			1.3.2. Planurile IT se adresează întregii organizaţii	
			1.3.3. Obiectivele IT îndeplinesc obiectivele organizaţiei	
		1.4. Comitetul IT determină strategia IT	1.4.1. Strategia IT este stabilită de un comitet IT	
			1.4.2. Comitetul IT transpune strategia în planuri pe termen scurt şi pe termen mediu	
			1.4.3. Comitetul IT stabileşte priorităţile proiectelor între dezvoltarea sistemelor şi activităţile realizate	
		1.5. Organizarea IT corespunde necesităţilor organizaţiei	1.5.1. Organizarea adecvată a funcţiei IT	
			1.5.2. Personalul IT are calificarea şi competenţele adecvate	
			1.5.3. Adecvarea practicilor şi procedurilor IT la procesele existente	
		1.6. Elaborarea strategiei IT corespunde strategiei entităţii	1.6.1. Dotarea actuală cu tehnică de calcul a stat la baza elaborării strategiei IT	
			1.6.2. Realizarea strategiei IT pe baza evaluării sistemelor existente	
2.	Organizarea şi funcţionarea departamentului IT	2.1. Definirea atribuţiilor şi activităţilor	2.1.1. Definirea atribuţiilor şi responsabilităţilor în cadrul departamentului IT	
			2.1.2. Atribuţiile specifice departamentului sunt stabilite în cadrul atribuţiilor generale ale entităţii	

Nr. crt.	Domeniul	Activităţi/obiective	Obiecte auditabile	Observaţii
			2.1.3. Atribuţiile stabilite asigură realizarea activităţilor necesare implementării obiectivelor	
			2.1.4. Identificarea tuturor activităţilor care concură la realizarea obiectivelor	
			2.1.5. Corelaţia între atribuţiile postului şi competenţele ocupantului postului	
			2.1.6. Definirea activităţilor în cadrul structurii organizatorice	
		2.2. Stabilirea structurii organizatorice	2.2.1. Organizarea funcţională a departamentului IT	
			2.2.2. Definirea relaţiilor organizatorice între compartimente	
			2.2.3. Examinarea sistemului de gestionare a riscurilor generale la nivelul departamentului IT	
			2.2.4. Riscurile legate de securitatea datelor, programelor şi echipamentelor sunt identificate şi evaluate cât mai corect şi complet	
		2.3. Stabilirea responsabilităţilor	2.3.1. Definirea limitelor de competenţă	
			2.3.2. Definirea responsabilităţilor în realizarea activităţilor	
			2.3.3. Definirea sarcinilor prin fişa postului	
3.	Operaţii ale sistemului informatic	3.1 Managementul operaţiunilor	3.1.1. Existenţa listei operaţiunilor zilnice de realizat	
			3.1.2. Performanţa, capacitatea şi disponibilitatea sistemelor informatice este monitorizată de administratori	
			3.1.3. Responsabilitatea pentru supravegherea sarcinilor pe seturi de programe revine administratorilor	
			3.1.4. Elaborarea Planului anual de activitate	
		3.2. Managementul problemelor	3.2.1. Incidentele privind funcţionarea normală a serviciilor IT sunt rezolvate sau prevenite în termen	
			3.2.2. Programele antivirus asigură protecţia aplicaţiilor	
			3.2.3. Problemele apărute sunt prioritizate şi luate în calcul pentru remediere	
			3.2.4. Implementarea subsistemelor IT	
			3.2.5. Activităţile operaţionale sunt conforme cu instrucţiunile din manualele de utilizare	
		3.3. Funcţionalitatea activităţilor în cadrul departamentului IT	3.3.1. Activităţile sunt bine organizate pentru asigurarea bunei funcţionării a departamentului	
			3.3.2. Organizarea funcţională a activităţilor în cadrul departamentului IT	
			3.3.3. Activităţile în cadrul departamentului sunt definite respectând criteriile de calitate	
			3.3.4. Evidenţa datelor aflate pe mediile de stocare	
			3.3.5. Distribuirea cu precizie a informaţiei către utilizatori şi mediile de stocare	
			3.3.6. Asigurarea caracterului secret al datelor	

Nr. crt.	Domeniul	Activităţi/obiective	Obiecte auditabile	Observaţii
			3.3.7. Soluţionarea problemelor presupune parcurgerea etapelor: iniţierea, planificarea, execuţia, monitorizarea şi analiza, încheierea	
		3.4. Mentenanţa echipamentelor	3.4.1. Obţinerea de rapoarte de activitate utile	
			3.4.2. Întreţinerea calculatorului şi a echipamentelor	
			3.4.3. Instalarea şi configurarea calculatorului	
			3.1.1. Sistemul este întreţinut pentru a se asigura că este conform cu nevoile organizaţiei	
		3.5. Utilizarea echipamentelor	3.5.1. Realizarea eficientă a operaţiilor în cadrul departamentului IT	
			3.5.2. Identificarea şi raportarea pericolelor	
			3.5.3. Administrarea eficientă a aplicaţiilor şi programelor	
			3.5.4. Evaluarea problemelor şi soluţionarea acestora	
			3.5.5. Programele corespund cerinţelor stabilite	
			3.5.6. Echipamentele sunt utilizate adecvat asigurând un confort în exploatare	
4.	Securitatea informaţiilor	4.1. Organizarea securităţii informaţiilor	4.1.1. Crearea politicii de securitate a informaţiei	
			4.1.2. Crearea standardelor şi practicilor pentru securitatea informaţiei	
			4.1.3. Stabilirea responsabilităţilor privind securitatea informaţiei	
			4.1.4. Elaborarea politicii privind securitatea informaţiei	
			4.1.5. Stabilirea responsabilităţilor în cadrul politicii de securitate	
			4.1.6. Securitatea informaţiilor asigură integritatea acestora	
			4.1.7. Securitatea datelor asigură disponibilitatea acestora doar pentru utilizatori autorizaţi	
		4.2. Disponibilitatea datelor	4.2.1. Protejarea împotriva atacurilor informatice	
			4.2.2. Protejarea datelor împotriva viruşilor	
			4.2.3. Asigurarea continuităţii activităţilor	
			4.2.4. Recuperarea datelor în caz de dezastru	
			4.2.5. Protejarea împotriva asumării unei identităţii false	
		4.3. Asigurarea funcţionării programelor şi aplicaţiilor	4.3.1. Asigurarea introducerii corecte a datelor şi informaţiilor pentru prelucrare	
			4.3.2. Existenţa licenţelor pentru programele utilizate	
			4.3.3. Prelucrarea datelor	
			4.3.4. Asigurarea securităţii datelor şi informaţiilor	
		4.4. Implementarea instrumentelor de control	4.4.1. Accesul la aplicaţie este oferit pe baza necesităţilor utilizatorului	
			4.4.2. Mecanismele de securitate configurate şi implementate verifică şi limitează accesul la aplicaţii	

Nr. crt.	Domeniul	Activităţi/obiective	Obiecte auditabile	Observaţii
			4.4.3. Introducerea instrumentelor de control fizic	
			4.4.4. Stabilirea de chei de control pentru fiecare program sau aplicaţie	
		4.5. Securitatea reţelei	4.5.1. Mecanismele de securitate configurate şi implementate asigură securitatea informaţiilor în cadrul reţelei	
			4.5.2. Monitorizarea securităţii reţelelor	
		4.6. Gestionarea parolelor	4.6.1. Utilizatorii au parole de acces individuale	
			4.6.2. Schimbarea periodică a parolelor	
			4.6.3. Conturile şi parolele generice sunt folosite pentru accesul la sisteme şi aplicaţii	
			4.6.4. Protejarea parolelor	
			4.6.5. Persoanele autorizate au acces la sistemul de operare	
		4.7. Securitatea logică	4.7.1. Asigurarea securităţii funcţionării programelor şi aplicaţiilor	
			4.7.2.Protejarea sistemelor informatice împotriva factorilor de mediu !!	
			4.7.3. Protejarea informaţiei din reţea	
5	Proiectarea şi testarea programelor şi aplicaţiilor	5.1. Proiectarea şi elaborarea programelor şi aplicaţiilor	5.1.1. Proiectarea programului informatic	
			5.1.2. Elaborarea programului informatic	
			5.1.3. Proiectarea unui program sau aplicaţie tine cont de necesităţile organizaţiei	
			5.1.4. Proiectarea unui program sau aplicaţie pe baza existenţei resurselor financiare	
			5.1.5. Respectarea cerinţelor în achiziţia unei aplicaţii	
		5.2. Testarea şi implementarea programelor şi aplicaţiilor	5.2.1. Utilizarea de date ipotetice în testarea unui program	
			5.2.2. Testarea programului şi aplicaţiei	
			5.2.3. Asigurarea corectitudinii rezultatelor	
			5.2.4. Implementarea unui program după realizarea testării acestuia	
6.	Elaborarea şi implementarea proiectelor IT	6.1. Dezvoltarea proiectelor IT (programe şi aplicaţii)	6.1.1. Metodologia pentru dezvoltarea şi achiziţia aplicaţiei	
			6.1.2. Iniţierea şi elaborarea proiectelor IT	

Nr. crt.	Domeniul	Activităţi/obiective	Obiecte auditabile	Observaţii
			6.1.3. Monitorizarea performanţelor soluţiilor IT implementate	
		6.2. Implementarea şi funcţionarea programelor şi aplicaţiilor	6.2.1. Reproiectarea soluţiilor IT pentru programe şi aplicaţii	
			6.2.2. Implementarea adecvată a aplicaţiilor	
			6.2.3. Întreţinerea aplicaţiilor garantează funcţionarea proceselor la parametrii optimi	
7.	Proiectarea şi menţinerea în funcţiune a unei reţele	7.1. Proiectarea, instalarea şi administrarea reţelei de calculatoare	7.1.1. Asigurarea bunei funcţionări a sistemelor bazate pe existenţa şi funcţionarea reţelei de calculatoare	
			7.1.2. Monitorizarea performanţelor reţelelor	
			7.1.3. Administrarea serverelor	
			7.1.4. Reţeaua de calculatoare corespunde cerinţelor funcţionale	
		7.2. Interconectarea şi securitatea reţelei	7.2.1. Interconectarea reţelelor	
			7.2.2. Proiectarea şi asigurarea securităţii reţelei	
			7.2.3. Urmărirea adecvării performanţelor unei reţele	

Auditori,

Popescu Sorin
Radu George

Procedura PO5 :	ANALIZA RISCULUI

Entitatea Publică
Serviciul de Audit Intern

IDENTIFICAREA RISCURILOR

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 04.09.2009
Avizat: Dumitru Daniel Data: 04.09.2009

Nr. crt.	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Obs.
1.	Strategia şi planificarea sistemelor informatice	1.1. Strategia IT este concordantă cu scopurile organizaţiei	1.1.1. Strategia IT defineşte necesităţile şi priorităţile	Achiziţia şi implementarea programelor şi aplicaţiilor nu este corelată cu obiectivele propuse;	
			1.1.2. Strategia IT face trimitere la nevoile viitoare ale organizaţiei	Sistemele nu sunt dezvoltate într-o manieră planificată şi controlată	
			1.1.3. Strategia defineşte direcţiile şi obiectivele de dezvoltare a IT	Strategia IT nu are o viziune orientată spre viitor, fiind o extrapolare a tendinţelor trecute	
		1.2. Planurile IT se adresează întregii organizaţii	1.2.1. Strategia IT este transpusă în planuri IT	Dezvoltarea IT nu acoperă toate procesele;	
			1.2.2. Planurile IT ajută la îndeplinirea misiunii organizaţiei	Planurile IT nu contribuie la realizarea scopului entităţii în domeniul IT;	
			1.2.3. Planurile IT oferă asigurare cu privire la faptul că resursele IT sunt alocate în concordanţă cu necesităţile	Resursele IT nu sunt identificate pentru fiecare element al planului;	
		1.3. Obiectivele IT îndeplinesc obiectivele organizaţiei	1.3.1. Strategia IT este concordantă cu scopurile organizaţiei	Utilizatorii şi IT nu au aceleaşi opinii cu privire la responsabilităţile şi autoritatea lor	
			1.3.2. Planurile IT se adresează întregii organizaţii	Planul IT nu acoperă cerinţele pe termen mediu;	
			1.3.3. Obiectivele IT îndeplinesc obiectivele organizaţiei	Obiectivele în domeniul IT nu derivă şi nu contribuie la realizarea obiectivelor entităţii;	
		1.4. Comitetul IT determină strategia IT	1.4.1. Strategia IT este stabilită de un comitet IT	Strategia IT este definită de departamentul IT;	
			1.4.2. Comitetul IT transpune strategia în planuri pe termen scurt şi pe termen mediu	Comitetul IT nu contribuie la dezvoltarea şi implementarea strategiei în domeniu;	
			1.4.3. Comitetul IT stabileşte priorităţile proiectelor între dezvoltarea sistemelor şi operaţiile realizate	Stabilirea dezvoltării IT de către departamentul IT;	
		1.5. Organizarea IT corespunde	1.5.1. Organizarea adecvată a funcţiei IT	Responsabilităţile nu sunt definite clar în cadrul compartimentelor şi posturilor;	

Nr. crt.	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Obs.
		necesităţilor organizaţiei	1.5.2. Personalul IT are calificarea şi competenţele adecvate	Lipsa calificărilor necesare;	
			1.5.3. Adecvarea practicilor şi procedurilor IT la procesele existente	Programele şi aplicaţiile nu sunt integrate şi nu răspund cerinţelor activităţilor;	
		1.6. Elaborarea strategiei IT corespunde strategiei entităţii	1.6.1. Dotarea actuală cu tehnică de calcul a stat la baza elaborării strategiei IT	Infrastructura IT existentă nu asigură implementarea strategiei IT;	
			1.6.2. Realizarea strategiei IT pe baza evaluării sistemelor existente	Elaborarea strategiei nu are la bază şi o evaluare şi identificare a posibilităţilor financiare;	
2	Organizarea şi funcţionarea departamentului IT	2.1. Definirea atribuţiilor şi activităţilor	2.1.1. Definirea atribuţiilor şi responsabilităţilor în cadrul departamentului IT	Lipsa ariei de competenţă pentru realizarea activităţilor stabilite structurii funcţionale	
			2.1.2. Atribuţiile specifice departamentului sunt stabilite în cadrul atribuţiilor generale ale entităţii	Definirea de atribuţii care nu se regăsesc in ROF	
			2.1.3. Atribuţiile stabilite asigură realizarea activităţilor necesare implementării obiectivelor	Definirea atribuţiilor sub formă de sarcini	
			2.1.4. Identificarea tuturor activităţilor care concură la realizarea obiectivelor	Activităţi stabilite incorect pentru realizarea obiectivelor	
			2.1.5. Corelaţia între atribuţiile postului şi competenţele ocupantului postului	Stabilirea de sarcini diferite pentru aceleaşi funcţii sau aceleaşi sarcini pentru funcţii diferite	
			2.1.6. Definirea activităţilor în cadrul structurii organizatorice	Activităţile realizate la nivelul structurii funcţionale nu se regăsesc în totalitate în cadrul sarcinilor stabilite posturilor	
		2.2. Stabilirea structurii organizatorice	2.2.1. Organizarea funcţională a departamentului IT	Structura funcţională nu este adaptată complexităţii activităţilor derulate	
			2.2.2. Definirea relaţiilor organizatorice între compartimente	Repartizarea activităţilor şi relaţiilor organizatorice fără a se ţine cont de natură organizării compartimentului	
			2.2.3. Examinarea sistemului de gestionare a riscurilor generale la nivelul departamentului IT	Riscurile nu sunt identificate şi gestionate la nivelul structurii funcţionale	
			2.2.4. Riscurile legate de securitatea datelor, programelor şi echipamentelor sunt identificate şi evaluate cât mai corect şi complet	Gestionarea slabă a riscurilor privind securitatea informaţiilor	
		2.3. Stabilirea responsabilităţilor	2.3.1. Definirea limitelor de competenţă	Autoritatea formală în realizarea activităţilor este insuficient stabilită postului	
			2.3.2. Definirea responsabilităţilor în realizarea activităţilor	Definirea doar a atribuţiilor, nu şi a limitei până unde răspunde ocupantul postului în realizarea activităţilor	
			2.3.3. Definirea sarcinilor prin fişa postului	Sarcinile stabilite postului potrivit fişei postului nu corespund cu acţiunile efectiv realizate de ocupantul postului	
	Operaţii ale	3.1 Managementul	3.1.1. Existenţa listei operaţiunilor zilnice de realizat	Activităţile se realizează fără o prioritizare a operaţiilor	

Nr. crt.	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Obs.
3.	sistemului informatic	operaţiunilor	3.1.2. Performanţa, capacitatea şi disponibilitatea sistemelor informatice este monitorizată de administratori	Lipsa analizelor privind scopul şi cerinţele de realizare a activităţilor şi calitatea aplicaţiilor sau programelor utilizate	
			3.1.3. Responsabilitatea pentru supravegherea sarcinilor pe seturi de programe revine administratorilor	Responsabilităţile operatorilor nu sunt delimitate şi stabilite în funcţie de specializarea fiecăruia şi tipurile de aplicaţii şi programe utilizate	
			3.1.4. Elaborarea Planului anual de activitate	Activităţile sunt derulate în cadrul departamentului fără a exista o planificare anuală sau periodică	
		3.2. Managementul problemelor	3.2.1. Incidentele privind funcţionarea normală a serviciilor IT sunt rezolvate sau prevenite în termen	Soluţionarea cu întârziere a problemelor apărute în utilizarea aplicaţiilor şi programelor	
			3.2.2. Programele antivirus asigură protecţia aplicaţiilor	Utilizarea neadecvată a programelor antivirus	
			3.2.3. Problemele apărute sunt prioritizate şi luate în calcul pentru remediere	Soluţionarea problemelor apărute nu este realizată potrivit gravităţii şi asigurând eficienţa realizării activităţilor entităţii	
			3.2.4. Implementarea subsistemelor IT	Programele şi aplicaţiile derulate la nivelul organizaţiei nu sunt actualizate potrivit noilor necesităţi ca urmare a modificării acţiunilor de realizare a activităţilor	
			3.2.5. Activităţile operaţionale sunt conforme cu instrucţiunile din manualele de utilizare	Neconcordanţe între utilizarea unei aplicaţii sau program şi precizările din caietul tehnic, privind execuţia acelei operaţii	
		3.3. Funcţionalitatea activităţilor în cadrul departamentului IT	3.3.1. Activităţile sunt bine organizate pentru asigurarea bunei funcţionării a departamentului	Lipsa revizuirii şi urmării contractelor la nivel de service şi a celor la nivel operativ	
			3.3.2. Organizarea funcţională a activităţilor în cadrul departamentului IT	Activităţile şi acţiunile necesare realizării acestora nu sunt repartizate eficient şi omogen pe compartimente în cadrul departamentului IT	
			3.3.3. Activităţile în cadrul departamentului sunt definite respectând criteriile de calitate	Activităţi şi acţiuni neresponsabilizate	
			3.3.4. Evidenţa datelor aflate pe mediile de stocare	Acces nerestricţionat la date şi informaţii	
			3.3.5. Distribuirea cu precizie a informaţiei către utilizatori şi mediile de stocare	Dependenţa de terţe părţi în centralizarea informaţiei şi oferirea rapoartelor	
			3.3.6. Asigurarea caracterului secret al datelor	Accesul la datele şi informaţiile organizaţiei nu este limitat doar pentru persoanele îndreptăţite	
			3.3.7. Soluţionarea problemelor presupune parcurgerea etapelor: iniţierea, planificarea, execuţia, monitorizarea şi analiza, încheierea	Soluţionarea unei probleme prin luarea în calcul doar a execuţiei acesteia	
		3.4. Mentenanţa echipamentelor	3.4.1. Obţinerea de rapoarte de activitate utile	Rapoartele obţinute nu oferă informaţii suficiente pentru luarea deciziilor	

Nr. crt.	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Obs.
			3.4.2. Întreţinerea calculatorului şi a echipamentelor	Disfuncţiile identificate nu sunt analizate şi înlăturate în conformitate cu instrucţiunile şi manualele de întreţinere	
			3.4.3. Instalarea şi configurarea calculatorului	Echipamentele periferice nu sunt instalate şi conectate conform documentaţiei	
			3.1.1. Sistemul este întreţinut pentru a se asigura că este conform cu nevoile organizaţiei	Întreţinerea sistemului doar la solicitările utilizatorilor;	
		3.5. Utilizarea echipamentelor	3.5.1. Realizarea eficientă a operaţiilor în cadrul departamentului IT	Suportul tehnic cu privire la utilizarea programelor nu este furnizat în mod corespunzător utilizatorilor;	
			3.5.2. Identificarea şi raportarea pericolelor	Costuri ridicate cu remedierea defecţiunilor, frecvenţă mare a acestora, timpi mari până la reluarea lucrului;	
			3.5.3. Administrarea eficientă a aplicaţiilor şi programelor	Controlul intern asupra datelor de intrare nu este asigurat corespunzător;	
			3.5.4. Evaluarea problemelor şi soluţionarea acestora	Lipsa revizuirii şi urmării măsurilor privind corectarea erorilor conduce la persistenţa unora dintre acestea;	
			3.5.5. Programele corespund cerinţelor stabilite	Neadaptarea la schimbările rapide ale tehnologiei informaţiei;	
			3.5.6. Echipamentele sunt utilizate adecvat asigurând un confort în exploatare	Lipsa cunoştinţelor privind exploatarea echipamentelor la potenţialul maxim;	
4.	Securitatea informaţiilor	4.1. Organizarea securităţii informaţiilor	4.1.1. Crearea politicii de securitate a informaţiei	Organizarea şi responsabilităţile privind securitatea informaţiilor nu constituie o prioritate a politicii de securitate	
			4.1.2. Crearea standardelor şi practicilor pentru securitatea informaţiei	Standardele privind securitatea informaţiei nu sunt definite formal	
			4.1.3. Stabilirea responsabilităţilor privind securitatea informaţiei	Responsabilităţile nu sunt separate clar între cele ale administratorilor şi cele ale operatorilor;	
			4.1.4. Elaborarea politicii privind securitatea informaţiei	Datele şi informaţiile prelucrate şi stocate nu sunt asigurate în condiţii de confidenţialitate, integritate şi disponibilitate	
			4.1.5. Stabilirea responsabilităţilor în cadrul politicii de securitate	Politica de securitate nu defineşte responsabilităţile cu privire la securitatea datelor şi informaţiilor	
			4.1.6. Securitatea informaţiilor asigură integritatea acestora	Datele şi informaţiile nu sunt stocate în condiţii de securitate;	
			4.1.7. Securitatea datelor asigură disponibilitatea acestora doar pentru utilizatori autorizaţi	Accesul la informaţii şi pentru persoanele neautorizate;	
		4.2. Disponibilitatea datelor	4.2.1. Protejarea împotriva atacurilor informatice	Lipsa programelor de protecţie adecvate pentru aplicaţii şi programe;	
			4.2.2. Protejarea datelor împotriva viruşilor	Vulnerabilitate sporită în faţa viruşilor;	
			4.2.3. Asigurarea continuităţii activităţilor	Planurile privind continuitatea activităţilor nu stabilesc măsuri concrete pentru reluarea activităţii;	

Nr. crt.	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Obs.
			4.2.4. Recuperarea datelor în caz de dezastru	Lipsa planurilor de recuperare a datelor şi informaţiilor	
			4.2.5. Protejarea împotriva asumării unei identităţii false	Sustragerea informaţiilor sau echipamentelor, fără autorizare;	
		4.3. Asigurarea funcţionării programelor şi aplicaţiilor	4.3.1. Asigurarea introducerii corecte a datelor şi informaţiilor pentru prelucrare	Aplicaţiile informatice nu sunt utilizate în conformitate cu instrucţiunile de exploatare	
			4.3.2. Existenţa licenţelor pentru programele utilizate	Plata unor despăgubiri urmare implementării unor programe fără licenţă	
			4.3.3. Prelucrarea datelor	Introducerea incorectă a datelor şi informaţiilor în cadrul programelor şi aplicaţiilor	
			4.3.4. Asigurarea securităţii datelor şi informaţiilor	Accesul la datele şi informaţiile stocate nu este restricţionat şi autorizat pe niveluri ierarhice	
		4.4. Implementarea instrumentelor de control	4.4.1. Accesul la aplicaţie este oferit pe baza necesităţilor utilizatorului	Accesul la program, aplicaţie este oferit pentru întregul personal ce posedă o parolă	
			4.4.2. Mecanismele de securitate configurate şi implementate verifică şi limitează accesul la aplicaţii	Pentru vulnerabilităţile sistemelor nu sunt stabilite şi implementate instrumente de control;	
			4.4.3. Introducerea instrumentelor de control fizic asupra echipamentelor IT	Accesul fizic la echipamente şi aplicaţii este restricţionat	
			4.4.4. Stabilirea de chei de control pentru fiecare program sau aplicaţie	Posibilitatea de a obţine şi utiliza rezultate nesigure, neverificate;	
		4.5. Securitatea reţelei	4.5.1. Mecanismele de securitate configurate şi implementate asigură securitatea informaţiilor în cadrul reţelei	Metodele de criptare nu asigură protecţia integrităţii şi confidenţialităţii datelor sensibile	
			4.5.2. Monitorizarea securităţii reţelelor	Comunicarea în reţea nu este monitorizată;	
		4.6. Gestionarea parolelor	4.6.1. Utilizatorii au parole de acces individuale	Accesul la aplicaţii se realizează direct, fără a fi permis doar pentru personalul îndreptăţit;	
			4.6.2. Schimbarea periodică a parolelor	Risc crescut de spargere a parolei;	
			4.6.3. Conturile şi parolele generice sunt folosite pentru accesul la sisteme şi aplicaţii	Conturile şi parolele generice iniţiale nu sunt personalizate, după începerea prelucrărilor de către utilizatori;	
			4.6.4. Protejarea parolelor	Descărcarea ilegală a unor informaţii;	
			4.6.5. Persoanele autorizate au acces la sistemul de operare	Accesul la servere este permis întregului personal, nefiind înregistrat şi monitorizat;	
		4.7. Securitatea logică	4.7.1. Asigurarea securităţii funcţionării programelor şi aplicaţiilor	Lipsa controalelor sau controale slabe de acces	
			4.7.2.Protejarea sistemelor informatice împotriva factorilor de mediu	Lipsa controalelor de mediu, respectiv detectoare de foc, incendiu etc.	

Nr. crt.	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Obs.
			4.7.3. Protejarea informaţiei din reţea	Funcţii de siguranţă sau control nu sunt prevăzute în cadrul sistemelor de aplicaţii	
5	Proiectarea şi testarea programelor şi aplicaţiilor	5.1. Proiectarea şi elaborarea programelor şi aplicaţiilor	5.1.1. Proiectarea programului informatic	În proiectarea programului/aplicaţiei, fluxul de date nu este stabilit adecvat rezultatelor aşteptate	
			5.1.2. Elaborarea programului informatic	Graficul de realizare a programului şi bugetul aprobat nu sunt respectate	
			5.1.3. Proiectarea unui program sau aplicaţie tine cont de necesităţile organizaţiei	Elaborarea de programe şi aplicaţii fără o analiză strategică la nivelul utilizatorilor	
			5.1.4. Proiectarea unui program sau aplicaţie pe baza existenţei resurselor financiare	Lipsa resurselor financiare în elaborarea şi implementarea unui program sau aplicaţie	
			5.1.5. Respectarea cerinţelor în achiziţia unei aplicaţii	Costuri suplimentare în achiziţia unui program sau aplicaţie	
		5.2. Testarea şi implementarea programelor şi aplicaţiilor	5.2.1. Utilizarea de date ipotetice în testarea unui program	Efectuarea de prelucrări asupra datelor reale, în cadrul testării programelor;	
			5.2.2. Testarea programului şi aplicaţiei	Neconformităţile şi erorile constatate în cursul testării unui program nu sunt analizate cu atenţie	
			5.2.3. Asigurarea corectitudinii rezultatelor	Opţiunile şi parametrii de lucru ai programului/aplicaţiei nu sunt stabiliţi conform specificaţiilor din documentaţiile tehnice	
			5.2.4. Implementarea unui program după realizarea testării acestuia	Programele sau aplicaţiile achiziţionate sunt implementate fără a fi testate	
6.	Elaborarea şi implementarea proiectelor IT	6.1. Dezvoltarea proiectelor IT (programe şi aplicaţii)	6.1.1. Metodologia pentru dezvoltarea şi achiziţia aplicaţiei	Lipsa proiectelor de dezvoltare a achiziţiilor	
			6.1.2. Iniţierea şi elaborarea proiectelor IT	Obiectivele generale ale proiectului nu sunt stabilite cu respectarea strategiei generale a organizaţiei	
			6.1.3. Monitorizarea performanţelor soluţiilor IT implementate	Parametri de referinţă şi valorile etalon ale programelor elaborate nu respectă specificaţiile şi nu se încadrează în standarde	
		6.2. Implementarea şi funcţionarea programelor şi aplicaţiilor	6.2.1. Reproiectarea soluţiilor IT pentru programe şi aplicaţii	Soluţiile privind îmbunătăţirea programelor şi aplicaţiilor nu ţin cont de punctele slabe şi critice, precum şi evoluţiile tehnologice	
			6.2.2. Implementarea adecvată a aplicaţiilor	Rapoartele nu corespund cerinţelor;	
			6.2.3. Întreţinerea aplicaţiilor garantează funcţionarea proceselor la parametrii optimi	Supravegherea proceselor aflate în execuţie şi a performanţelor aplicaţiilor, sistemelor sau programelor nu respectă procedurile şi instrucţiunile	
7.	Proiectarea şi menţinerea în funcţiune a unei	7.1. Proiectarea, instalarea şi administrarea reţelei	7.1.1. Asigurarea bunei funcţionări a sistemelor bazate pe existenţa şi funcţionarea reţelei de calculatoare	Subsistemele existente nu sunt configurate şi supravegheate individual	

Nr. crt.	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Obs.
	reţele	de calculatoare	7.1.2. Monitorizarea performanţelor reţelelor.	Scăderea performanţelor reţelelor;	
			7.1.3. Administrarea serverelor	Accesul şi utilizarea datelor şi informaţiilor stocate pe server nu respectă strategia de securitate a reţelei	
			7.1.4. Reţeaua de calculatoare corespunde cerinţelor funcţionale	Reţeaua de calculatoare nu asigură integrarea informaţiilor şi elaborarea rapoartelor	
		7.2. Interconectarea şi securitatea reţelei	7.2.1. Interconectarea reţelelor	Conexiunile dintre reţele nu sunt conforme cu arhitectura prevăzută de instrucţiuni şi nu respectă standardele	
			7.2.2. Proiectarea şi asigurarea securităţii reţelei	Vulnerabilităţile şi ameninţările nu sunt identificate şi prioritizate	
			7.2.3. Urmărirea adecvării performanţelor unei reţele de calculatoare	Proiectarea reţelei de calculatoare nu asigură integrarea programelor.	

Auditori,

Popescu Sorin
Radu George

Notă:

Identificarea riscurilor asociate obiectelor auditabile presupune ataşarea riscurilor semnificative la operaţiile stabilite în *Lista centralizatoare a obiectelor auditabile*, în prima fază a procedurii *Analiza riscurilor*.

Lista privind identificarea riscurilor reprezintă documentul prin care pe baza obiectelor audiabile identificate, a funcţionalităţii controalelor interne stabilite şi implementate de entitate sunt identificate şi stabilite riscurile aferente pentru fiecare obiect audiabil.

La un obiect auditabil se pot asocia unul sau mai multe riscuri posibile, determinate de auditorii interni pe baza informaţiilor colectate, dar si din propria experienţă. În situaţia în care la operaţiile audiabile se ataşează mai multe riscuri analiza acestora se va putea realiza pentru fiecare risc în parte, pe grupe de riscuri sau pe total operaţie/obiect audiabil.

Procedura PO5 :	ANALIZA RISCULUI

Entitatea Publică
Serviciul de Audit Intern

CHESTIONAR DE CONTROL INTERN

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 04.09.2009
Avizat: Dumitru Daniel Data: 04.09.2009

A. INTREBĂRI ADRESATE MANAGEMENTULUI GENERAL	**DA**	**NU**	**OBSERVAŢII**
Există un sistem de proceduri care sa reglementeze activitatea departamentului IT?	X		
Procedurile de lucru sunt scrise si formalizate?	X		
Există proceduri scrise privind achiziţionarea programelor şi aplicaţiilor informatice?		X	
Există proceduri scrise privind întreţinerea aplicaţiilor informatice?		X	Sunt realizate pe bază de contracte de prestări de servicii
Există o strategie clară şi obiective stabilite pentru IT?	X		
Strategia IT are viziunea orientată spre viitor?	X		
Managementul este mulţumit cu rolul sau valoarea IT în cadrul organizaţiei?	X		
Sistemul IT este dezvoltat într-o manieră planificată şi controlată?	X		Anual se realizează o evaluare a indicatorilor
Este supravegheată respectarea strategiei?	X		
Utilizatorii contribuie la priorităţile şi la dezvoltarea în domeniul IT?	X		Există un sistem prin care utilizatorii pot formula propuneri si soluţii, care apoi sunt analizate
Planurile IT sunt aplicate în practică?	X		Numai în caz de necesitate
Răspunderea şi responsabilitatea pentru sistemele de informaţii aparţine personalului de conducere?	X		
Utilizatorii au o bună percepţie asupra capacităţilor sau performanţei departamentului IT?	X		
Rotaţie personalului este redusă în cadrul departamentului IT?	X		
Ocuparea posturilor este adecvată în cadrul departamentului?			Grad de ocupare 95%
Managementul are cunoştinţă asupra tehnologiilor prezente şi viitoare necesare entităţii pentru asigurarea realizării activităţilor şi mandatului?	X		
Există capacitate adecvată de a planifica şi implementa resursele IT?	X		
Există capacitate de a monitoriza performanţa IT?	X		
Există o strategie adecvată de achiziţii IT?	X		
Există concordanţă între obiective şi strategii de achiziţii IT?	X		
Riscurile legate de achiziţii IT sunt administrate atât de entitate, cât şi de furnizori?		X	Nu există un proces de identificare şi gestionare a riscurilor la nivelul entităţii
B. INTREBARI ADRESATE MANAGEMENTULUI DE LINIE	**DA**	**NU**	**Auditorii**
Strategia şi planificarea sistemelor informatice			
Strategia defineşte principalele direcţii în IT?	X		
Strategia defineşte principalele obiective ale entităţii?	X		Defineşte obiectivele strategice
Strategia IT este concordantă cu strategia entităţii?	X		
Există planuri de dezvoltare IT?	X		Planuri de continuitate a activităţii şi planuri de recuperare a datelor

Planurile IT pe termen scurt sau mediu asigură dezvoltarea informaţională la nivelul entităţii?	X		
Obiectivele IT îndeplinesc planurile entităţii?	X		
Competenţele şi funcţionarea comitetului IT sunt definite clar?	X		nu există un regulament de organizare şi funcţionare al acestui comitat
Comitetul IT determină strategia IT?		X	Realizează doar o evaluare a necesităţilor de achiziţii IT
Comitetul IT transpune strategia IT în planuri IT?		X	Realizează doar o evaluare a necesităţilor de achiziţii IT
Comitetul IT stabileşte priorităţile proiectelor de dezvoltare?		X	Realizează doar o evaluare a necesităţilor de achiziţii IT
Funcţia IT este organizată adecvat în concordanţă cu strategia IT?	X		
Personalul IT asigură calitatea serviciilor IT?	X		
Personalul IT asigură competenţa necesară continuităţii activităţilor?	X		
Separarea sarcinilor există între dezvoltarea sistemelor şi deservirea acestora?	X		
Separarea sarcinilor există între dezvoltarea sistemelor şi operaţii?	X		
Separarea sarcinilor există între deservirea sistemelor şi securitatea informaţiei?	X		
Separarea sarcinilor există între operaţii şi utilizatori?	X		
Personalul a luat la cunoştinţă de sarcinile posturilor?	X		
Există cooperare interdepartamentală pentru dezvoltarea sistemelor integrate?	X		
Achiziţiile electronice sunt legate cu profilurile performanţei aşteptate?		X	Sunt legate doar de necesităţile de îmbunătăţire a activităţilor
Sistemele informatice achiziţionate asigură calitatea informaţiilor potrivit nevoilor?	X		
Planificarea continuităţii activităţilor			
Scopul planului de continuitate a activităţii este de a limita pierderile?	X		
Toate activităţile critice şi resursele sunt incluse în planul de continuitate a activităţilor?	X		
În cadrul planului de continuitate a activităţilor sunt stabilite responsabilităţi clare?	X		
Planurile de continuitate a activităţilor sunt comunicate ?		X	Sunt cunoscute doar de departamentul IT
Eficienţa planurilor de continuitate a activităţilor a fost testată?	X		
Planul de continuitate a activităţilor este testat regulat?	X		
Planul de continuitate a activităţilor este aprobat de conducere?	X		
Planul de continuitate a activităţilor a fost realizat urmare unei analize a riscurilor?		X	
Planul de continuitate a activităţilor are la bază şi o evaluare a impactului?		X	
Priorităţile sunt stabilite corect în cadrul planului de continuitate a activităţilor?	X		
Locaţia de recuperare este disponibilă?	X		
Infrastructura locaţiei de recuperare permite recuperarea la timp a activităţilor?	X		
Echipamentul necesar este instalat în cadrul locaţiei de recuperare?	X		
Există o bună relaţie între utilizatori şi personalul IT?	X		
Există pârghii de siguranţă sau control prevăzute în funcţionarea sistemelor?	X		
Cerinţele de recuperare ale activităţilor sunt revizuite periodic?	X		
Planul de continuitate cuprinde întregul sistem informatic din entitate?	X		
Sunt realizate informării periodice ale conţinutului planului de continuitate?		X	
Există o gestiune adecvată a riscurilor legate de departamentul IT?		X	nu există o gestionare a riscurilor legate de IT
Impactul materializării riscurilor legate de IT este cunoscut şi evaluat?		X	nu sunt cunoscute consecinţele materializării riscurilor
Personalul entităţii este pregătit şi capabil să răspundă Planurilor de continuitate?		X	nu cunoaşte aceste planuri
Implementarea software şi hardware este concepută şi realizată conform programelor?	X		
Implementarea software şi hardware este realizată după testarea corespunzătoare?	X		
IT asigură continuitatea şi eficienţa operaţiilor în derularea activităţilor entităţii?	X		
Planurile de rezervă sunt actuale, comprehensive şi complet testate?	X		
Securitatea informaţiilor			

Există o politică de securitatea informaţiei?	X		
Există o practică privind securitatea informaţiei?	X		
Există proceduri privind securitatea informaţiei?	X		
Politica de securitate este definită şi aprobată de conducere?	X		
Securitatea informaţiei este cunoscută şi însuşită de conducere?	X		
Politica de securitate a informaţiei este cunoscută de utilizatori?	X		Doar în legătură cu obligaţiile cei revin postului respectiv
Descrierile şi responsabilităţile posturilor în raport cu securitatea informaţiilor este clar definită şi cunoscută?	X		
Există disponibile descrieri clare ale sarcinilor?	X		
Responsabilităţile sunt clar definite privind securitatea informaţiei?	X		
Responsabilităţile şi sarcinile sunt comunicate corespunzător?	X		
Administrarea utilizatorilor este adecvată?	X		
Drepturile de acces sunt alocate corect?	X		
Drepturile de acces sunt alocate pe baza nevoii utilizatorului de a executa sarcinile atribuite?	X		
Drepturile de acces sunt alocate/schimbate corect şi la timp?		X	Există cazuri în care dreptul de acces este lăsat şi după eliberarea postului
Drepturile de acces sunt verificate regulat?		X	Numai la solicitări
Utilizatorii au parole de autorizare individuale?	X		
Parolele au lungimea adecvată şi sunt greu de aflat?	X		
Parolele sunt regulat schimbate?		X	Există cazuri în care aceeaşi parolă este menţinută şi chiar un an de zile
Parolele şi profilurile utilizatorilor privilegiaţi sunt folosite la accesul la sisteme şi aplicaţii cu un grad înalt de securitate?	X		
Utilizarea parolelor şi profilurilor utilizatorilor privilegiaţi este urmărita cu strictețe?	X		
Mecanismele de securitate logică au fost implementate şi configurate pentru a verifica şi limita accesul la sistemul de operare?	X		
La sistemele de operare au acces doar persoanele autorizate?	X		
Accesul la funcţiile aplicaţiei este permis pe baza necesităţilor utilizatorului de a-şi realiza sarcinile?	X		
Mecanismele de securitate logică verifică şi limitează accesul la aplicaţie?	X		
Confidenţialitatea şi integritatea datelor este suficient de securizată?	X		
Mecanismele de securitate logică implementate şi configurate asigură securitatea informaţiilor din cadrul reţelei?	X		
Informaţia din reţea este protejată de viruşi?	X		
Accesul neautorizat la reţea este blocat suficient?	X		
Criptarea este folosită ca protecţie necesară integrităţii şi confidenţialităţii datelor?	X		
Sistemele informatice sunt adecvat protejate împotriva factorilor de catastrofă?	X		
Securitatea informaţiei impune o analiză de risc în mod regulat?	X		
Securitatea informaţiei asigură protejarea informaţiei şi raportarea deficienţelor?	X		Raportarea deficienţelor numai în caz de probleme la aplicaţii, programe etc.
Securitatea informaţiei permite protejarea informaţiei prin respectarea cerinţelor de confidenţialitate, integritate şi disponibilitate?	X		
Politica de securitate a informaţiei interzice utilizarea informaţiilor şi sistemelor fără autorizaţie şi pentru scopuri care nu au legătură cu munca?	X		
Politica de securitate interzice copierea sau scoaterea neautorizată din sediu a informaţiei fără autorizare?	X		
Ieşirea din sistem este realizată ori de câte ori un terminal este lăsat nesupravegheat?		X	Ieşirea din sistem este realizat pentru fiecare terminal manual
Politica de securitate este comunicată şi cunoscută de întregul personal şi părţile externe cu acces la informaţiile şi sistemele entităţii?		X	
Accesul fizic la sistemele de calculatoare este restricţionat pentru personalul autorizat în afara programului de lucru?	X		
Mijloacele şi documentaţia „critică” este asigurată atunci când nu este în uz?	X		

Echipamentele sunt protejate împotriva furtului?	X		Se află în gestiunea utilizatorului
Utilizatorii sistemului au acces numai pentru scopuri clare şi autorizate?	X		Accesul le este permis doar dacă sunt autorizaţi
Utilizatorii sistemului sunt instruiţi cu privire la cerinţele de siguranţă şi sunt supravegheaţi permanent?		X	Informaţiile critice sunt securizate suplimentar
Implementarea aplicaţiilor şi administrarea lor			
Metodologia de achiziţionare sau dezvoltare a noilor aplicaţii este conformă cu scopurile entităţii?	X		
Metodologia aplicată garantează că aplicaţiile corespund nevoilor?	X		
Achiziţia de noi aplicaţii este aprobată de conducere?	X		
Aplicaţiile sunt testate suficient şi eficient?	X		
Testările aplicaţiei garantează că aceasta funcţionează corect şi corespunde cerinţelor?	X		
Implementarea unei aplicaţii asigură continuitatea activităţilor?	X		
Întreţinerea unei aplicaţii garantează funcţionalitatea proceselor?	X		
Modificările aplicaţiilor sunt autorizate?	X		
Există metodologie pentru dezvoltarea sau achiziţia unei aplicaţii?	X		
Metodologia este asigurată de proceduri?	X		
Sunt respectate criteriile de licitaţie la achiziţia unei aplicaţii?	X		
Există o analiză funcţională a cerinţelor de lucru pentru dezvoltarea unei aplicaţii?		X	
Utilizatorii sunt implicaţi în analiza funcţională?		X	
Analiza funcţională este confirmată printr-o analiză tehnică?		X	
Limbajele de programare sunt adecvate?	X		
Sunt stabilite planuri de testare a unei aplicaţii?	X		
Utilizatorii sunt implicaţi în testarea aplicaţiilor?		X	Numai în implementarea aplicaţiilor
Datele folosite pentru testare sunt protejate?	X		
Transferarea unei aplicaţii din mediul de dezvoltare în mediul de producţie este realizată de personalul responsabilizat?	X		
Programatorii au acces la mediul de producţie?	X		
Există analize de calitate privind dezvoltarea unei aplicaţii?	X		
Rezultatele controalelor de calitate sunt documentate?		X	
Sunt comparate funcţionalităţile aplicaţiei cu cerinţele iniţiale?	X		
Există un control adecvat din punct de vedere temporal al tranzacţiilor?		X	
Funcţiunile de introducere de date şi de autorizare sunt restricţionate şi separate?	X		
Introducerea parametrilor şi altor date ce urmează a fi procesate este strict controlată?	X		
Sunt efectuate verificări pentru detectarea posibilelor înregistrări duble?	X		
Procesarea datelor se realizează în mod planificat şi este înţeleasă de utilizatori şi personalul operativ?	X		
Datele, inclusiv cele transferate din alte sisteme,sunt supuse validării în timpul prelucrării?	X		
Programele furnizează confirmări cu privire la finalizarea procesării şi există proceduri de recuperare şi de reintroducere în caz de anomalii în funcţionare?	X		
Înregistrările sunt armonizate în cazurile în care sunt trecute dintr-un sistem în altul?	X		
Utilizatorii sunt responsabili de introducerea, modificarea sau ştergerea operaţiilor înregistrate în cadrul unui sistem?	X		
Fişierele sunt salvate la intervale regulate de timp în timpul prelucrării pentru a permite recuperarea operaţiunilor?	X		
Implementarea şi gestionarea bazelor de date			
Achiziţia unui program de baze de date este aprobată de conducere?	X		
Programul de baze de date este selectat conform nevoilor?	X		
Programul de baze de date este standardizat?	X		
Baza de date este testată înainte de implementare?	X		
Modificările asigură un impact minim asupra proceselor?	X		
Performanţa unei baze de date este urmărită adecvat?	X		
Programele de baze de date posedă licenţe?	X		
Integritatea bazelor de date sunt verificate periodic şi se reţin copii de siguranţă de		X	

la o verificare la alta?			
Instrucţiunile operatorilor şi utilizatorilor specifică clar procedurile de urmat în cazul unei deficienţe a aplicaţiei în timpul prelucrărilor?	X		
Accesul la echipamente este protejat prin securitatea fizică şi/sau supravegherea continuă?	X		
Autorizarea fizică la echipamente este realizată în conformitate cu standardele sau proceduri?	X		
Măsurile de control a accesului ţin seama de politica de securitate a informaţiilor?	X		
Utilizatori sunt pregătiţi corespunzător cu privire la implementarea bazelor de date?	X		
Este acordată asistenţă utilizatorilor pe perioada implementării bazei de date?	X		
Timpul de răspuns la un apel de la operatori este scăzut?	X		
Măsurile de control a accesului asigură răspunderea personală?	X		
Măsurile de control a accesului asigură punerea în practică a unor instrumente suplimentare de control în cazul utilizatorilor cu acces special?	X		
Măsurile de control intern privind utilizarea sistemelor asigură separarea sarcinilor?		X	
Operaţiuni ale sistemelor informatice			
Organizarea operaţiunilor de sistem sigură funcţionarea eficientă şi eficace?	X		
Activităţile operaţionale sunt conforme cu instrucţiunile date de operatori?	X		
Problemele sunt identificate şi rezolvate în termen?	X		
Problemele sunt administrate şi urmărite adecvat?	X		
Problemele sunt prioritizate şi planificate?	X		
Rezultatul procesului este stocat cu precizie?	X		
Rezultatul procesului este asigurat împotriva accesului neautorizat?	X		
Mediile de stocare sunt păstrate adecvat?	X		
Integritatea datelor de pe mediile de stocare este asigurată?	X		
Procedurile de back-up şi recuperare asigură disponibilitatea datelor şi informaţiilor importante?	X		
Recuperarea este testată regulat?	X		
Sarcinile realizate de operatori sunt monitorizate?	X		
Identitatea utilizatorilor este controlată?	X		
Există procese prin care se asigură remedierea deficienţelor de funcţionare?	X		
Există numită o persoană responsabilă cu supervizarea noilor dezvoltări şi cu întreţinerea şi integrarea sistemelor în fiecare arie de activitate?	X		
Utilizatorii sunt instruiţi pentru fiecare aplicaţie a sistemului?	X		
Departamentul măsoară aspectele cheie ale performanţei IT?	X		
Mecanismele de control sunt potrivite pentru minimizarea riscurilor?	X		
Administrarea reţelelor software şi hardware			
Achiziţia hardware şi software este aprobată de conducere?	X		
Hardware şi software sunt selectate pe baza criteriilor stabilite în funcţie de necesităţi?	X		
Hardware şi softul sunt standardizate?	X		
Hardware şi softul sunt testate înainte de implementare?	X		
Modificările asigură un impact minim asupra proceselor?	X		
Programele de reţea au licenţe?	X		
Există contracte la nivel de service privind întreţinerea sistemelor şi aplicaţiilor?	X		
Timpul mediu de intervenţie şi soluţionare a defecţiunii este redus?	X		
Controlul implementat funcţionează asupra informaţiilor la care accesul este limitat?	X		
Abuzul de informaţii este gestionat corespunzător?	X		
Normele de siguranţă privind computerele sunt dezvoltate?	X		

Auditori,

Popescu Sorin
Radu George

Notă:

Chestionarul de control intern este structurat pe obiectivele misiunii de audit intern şi permit prin intermediul întrebărilor formulate şi răspunsurilor primite, identificarea controalelor interne instituite de management şi aprecierea funcţionalităţii acestora, astfel încât riscurile să poată fi identificate în totalitate şi apreciat corect nivelul acestora.

Procedura – P05:	**ANALIZA RISCULUI**

Entitatea Publică
Serviciul de Audit Intern

STABILIREA FACTORILOR DE RISC, A PONDERILOR ACESTORA ŞI APRECIEREA NIVELURILOR RISCURILOR

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 04.09.2009
Avizat: Dumitru Daniel Data: 04.09.2009

Factori de risc (F_i)	**Ponderea factorilor de risc (P_i)**	**Nivelul de apreciere al riscului (N_i)**		
		N_1	**N_2**	**N_3**
Aprecierea controlului intern F1	**P1 – 50%**	Există proceduri şi se aplică	Există proceduri, sunt cunoscute, dar nu se aplică	Nu există proceduri
Aprecierea cantitativă F2	**P2 – 30%**	Impact financiar scăzut	Impact financiar mediu	Impact financiar ridicat
Aprecierea calitativă F3	**P3 – 20%**	Vulnerabilitate mică	Vulnerabilitate medie	Vulnerabilitate mare

Auditori,

Popescu Sorin
Radu George

Notă:
Prin acest document se stabilesc, în funcţie de importanţa şi greutatea factorilor de risc, ponderile şi nivelurile de apreciere ale riscurilor.
Cei trei factori de risc sunt stabiliţi prin normele generale şi sunt acoperitori pentru entitate, însă dacă se doreşte evidenţierea şi a altor factori de risc, cu nivelurile de apreciere corespunzătoare, trebuie să se aibă în vedere ca suma ponderilor factorilor de risc să rămână 100%.

Procedura PO5 :	ANALIZA RISCULUI

Entitatea Publică
Serviciul de Audit Intern

STABILIREA NIVELULUI RISCULUI ŞI A PUNCTAJULUI TOTAL AL RISCURILOR

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 04.09.2009
Avizat: Dumitru Daniel Data: 04.09.2009

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Criterii de analiză a riscurilor						Punctaj total
					Aprecierea controlului intern		Aprecierea cantitativă		Aprecierea calitativă		
					P1 50%	N1	P2 30%	N2	P3 20%	N3	
1.	Strategia şi planificarea sistemelor informatice	1.1. Strategia IT este concordantă cu scopurile organizaţiei	1.1.1. Strategia IT defineşte necesităţile şi priorităţile	Achiziţia şi implementarea programelor şi aplicaţiilor nu este corelată cu obiectivele propuse;	0,5	3	0,3	1	0,2	2	2,20
			1.1.2. Strategia IT face trimitere la nevoile viitoare ale organizaţiei	Sistemele nu sunt dezvoltate într-o manieră planificată şi controlată	0,5	2	0,3	1	0,2	3	1,90
			1.1.3. Strategia defineşte direcţiile şi obiectivele de dezvoltare a IT	Strategia IT nu are o viziune orientată spre viitor, fiind o extrapolare a tendinţelor trecute	0,5	1	0,3	1	0,2	1	1,00
		1.2. Planurile IT se adresează întregii organizaţii	1.2.1. Strategia IT este transpusă în planuri IT	Dezvoltarea IT nu acoperă toate procesele;	0,5	2	0,3	1	0,2	1	1,50
			1.2.2. Planurile IT ajută la îndeplinirea misiunii organizaţiei	Planurile IT nu contribuie la realizarea scopului entităţii în domeniul IT;	0,5	2	0,3	2	0,2	2	2,00
			1.2.3. Planurile IT oferă asigurare cu privire la faptul că resursele IT sunt alocate în concordanţă cu necesităţile	Resursele IT nu sunt identificate pentru fiecare element al planului;	0,5	2	0,3	2	0,2	2	2,00

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Criterii de analiză a riscurilor						Punctaj total
					Aprecierea controlului intern		Aprecierea cantitativă		Aprecierea calitativă		
					P1 50%	N1	P2 30%	N2	P3 20%	N3	
		1.3. Obiectivele IT îndeplinesc obiectivele organizaţiei	1.3.1. Strategia IT este concordantă cu scopurile organizaţiei	Utilizatorii şi IT nu au aceleaşi opinii cu privire la responsabilităţile şi autoritatea lor	0,5	2	0,3	3	0,2	1	2,10
			1.3.2. Planurile IT se adresează întregii organizaţii	Planul IT nu acoperă cerinţele pe termen mediu;	0,5	2	0,3	1	0,2	1	1,50
			1.3.3. Obiectivele IT îndeplinesc obiectivele organizaţiei	Obiectivele în domeniul IT nu derivă şi nu contribuie la realizarea obiectivelor entităţii;	0,5	2	0,3	1	0,2	2	1,70
		1.4. Comitetul IT determină strategia IT	1.4.1. Strategia IT este stabilită de un comitet IT	Strategia IT este definită de departamentul IT;	0,5	2	0,3	2	0,2	2	2,00
			1.4.2. Comitetul IT transpune strategia în planuri pe termen scurt şi pe termen mediu	Comitetul IT nu contribuie la dezvoltarea şi implementarea strategiei în domeniu;	0,5	3	0,3	2	0,2	3	2,70
			1.4.3. Comitetul IT stabileşte priorităţile proiectelor de dezvoltare a sistemelor IT	Stabilirea dezvoltării IT de către departamentul IT;	0,5	2	0,3	3	0,2	3	2,50
		1.5. Organizarea IT corespunde necesităţilor organizaţiei	1.5.1. Organizarea adecvată a funcţiei IT	Responsabilităţile nu sunt definite clar în cadrul compartimentelor şi posturilor;	0,5	2	0,3	2	0,2	2	2,00
			1.5.2. Personalul IT are calificarea şi competenţele adecvate	Lipsa calificărilor necesare;	0,5	2	0,3	1	0,2	2	1,70
			1.5.3. Adecvarea practicilor şi procedurilor IT la procesele existente	Programele şi aplicaţiile nu sunt integrate şi nu răspund cerinţelor activităţilor;	0,5	2	0,3	3	0,2	3	2,50
		1.6. Elaborarea strategiei IT corespunde strategiei entităţii	1.6.1. Dotarea actuală cu tehnică de calcul a stat la baza elaborării strategiei IT	Infrastructura IT existentă nu asigură implementarea strategiei IT;	0,5	3	0,3	3	0,2	3	3,00
			1.6.2. Realizarea strategiei IT pe baza evaluării sistemelor existente	Elaborarea strategiei nu are la bază şi o evaluare şi identificare a posibilităţilor financiare;	0,5	2	0,3	1	0,2	1	1,50
2	Organizarea şi funcţionarea departamentul	2.1. Definirea atribuţiilor şi activităţilor	2.1.1. Definirea atribuţiilor şi responsabilităţilor în cadrul departamentului IT	Lipsa ariei de competenţă pentru realizarea activităţilor stabilite structurii funcţionale	0,5	3	0,3	1	0,2	3	2,40

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Criterii de analiză a riscurilor						Punctaj total
					Aprecierea controlului intern		Aprecierea cantitativă		Aprecierea calitativă		
					P1 50%	N1	P2 30%	N2	P3 20%	N3	
	ui IT		2.1.2. Atribuţiile specifice departamentului sunt stabilite în cadrul atribuţiilor generale ale entităţii	Definirea de atribuţii care nu se regăsesc in ROF	0,5	2	3	1	0,2	1	1,50
			2.1.3. Atribuţiile stabilite asigură realizarea activităţilor necesare implementării obiectivelor	Definirea atribuţiilor sub formă de sarcini	0,5	2	0,3	2	0,2	1	1,80
			2.1.4. Identificarea tuturor activităţilor care concură la realizarea obiectivelor	Activităţi stabilite incorect pentru realizarea obiectivelor	0,5	2	0,3	2	0,2	1	1,80
			2.1.5. Corelaţia între atribuţiile postului şi competenţele ocupantului postului	Stabilirea de sarcini diferite pentru aceleaşi funcţii sau aceleaşi sarcini pentru funcţii diferite	0,5	2	0,3	1	0,2	1	1,50
			2.1.6. Definirea activităţilor în cadrul structurii organizatorice	Activităţile realizate la nivelul structurii funcţionale nu se regăsesc în totalitate în cadrul sarcinilor stabilite posturilor	0,5	3	0,3	1	0,2	3	2,40
		2.2. Stabilirea structurii organizatorice	2.2.1. Organizarea funcţională a departamentului IT	Structura funcţională nu este adaptată complexităţii activităţilor derulate	0,5	2	0,3	1	0,2	3	1,90
			2.2.2. Definirea relaţiilor organizatorice între compartimente	Repartizarea activităţilor şi relaţiilor organizatorice fără a se ţine cont de natura organizării compartimentului	0,5	2	0,3	1	0,2	1	1,50
			2.2.3. Examinarea sistemului de gestionare a riscurilor generale la nivelul departamentului IT	Riscurile nu sunt identificate şi gestionate la nivelul structurii funcţionale	0,5	2	0,3	3	0,2	3	2,50
			2.2.4. Riscurile legate de securitatea datelor, programelor şi echipamentelor sunt identificate şi evaluate cât mai corect şi complet	Gestionarea slabă a riscurilor privind securitatea informaţiilor	0,5	2	0,3	1	0,2	3	2,40
		2.3. Stabilirea responsabilităţilor	2.3.1. Definirea limitelor de competenţă	Autoritatea formală în realizarea activităţilor este insuficient stabilită postului	0,5	1	0,3	3	0,2	1	1,60

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Criterii de analiză a riscurilor						Punctaj total
					Aprecierea controlului intern		Aprecierea cantitativă		Aprecierea calitativă		
					P1 50%	N1	P2 30%	N2	P3 20%	N3	
			2.3.2. Definirea responsabilităţilor în realizarea activităţilor	Definirea doar a atribuţiilor, nu şi a limitei până unde răspunde ocupantul postului în realizarea activităţilor	0,5	1	0,3	3	0,2	2	1,80
			2.3.3. Definirea sarcinilor prin fişa postului	Sarcinile stabilite postului potrivit fişei postului nu corespund cu acţiunile efectiv realizate de ocupantul postului	0,5	2	0,3	3	0,2	3	2,50
3.	Operaţii ale sistemului informatic	3.1 Managementul operaţiunilor	3.1.1. Existenţa listei operaţiunilor zilnice de realizat	Activităţile se realizează fără o prioritizare a operaţiilor	0,5	2	0,3	1	0,2	1	1,50
			3.1.2. Performanţa, capacitatea şi disponibilitatea sistemelor informatice este monitorizată de administratori	Lipsa analizelor privind scopul şi cerinţele de realizare a activităţilor şi calitatea aplicaţiilor sau programelor utilizate	0,5	2	0,3	2	0,2	3	2.20
			3.1.3. Responsabilitatea pentru supravegherea sarcinilor pe seturi de programe revine administratorilor	Responsabilităţile operatorilor nu sunt delimitate şi stabilite în funcţie de specializarea fiecăruia şi tipurile de aplicaţii şi programe utilizate	0,5	3	0,3	2	0,2	2	2,50
			3.1.4. Elaborarea Planului anual de activitate	Activităţile sunt derulate în cadrul departamentului fără a exista o planificare anuală sau periodică	0,5	2	0,3	2	0,2	3	2,20
		3.2. Managementul problemelor	3.2.1. Incidentele privind funcţionarea normală a serviciilor IT sunt rezolvate sau prevenite în termen	Soluţionarea cu întârziere a problemelor apărute în utilizarea aplicaţiilor şi programelor	0,5	1	0,3	1	0,2	1	1,00
			3.2.2. Programele antivirus asigură protecţia aplicaţiilor	Utilizarea neadecvată a programelor antivirus	0,5	2	0,3	3	0,2	3	2,50
			3.2.3. Problemele apărute sunt prioritizate şi luate în calcul pentru remediere	Soluţionarea problemelor apărute nu este realizată potrivit gravităţii şi asigurând eficienţa realizării activităţilor entităţii	0,5	1	0,3	1	0,2	3	1,40
			3.2.4. Implementarea subsistemelor IT	Programele şi aplicaţiile derulate la nivelul organizaţiei nu sunt actualizate potrivit noilor necesităţi ca urmare a modificării acţiunilor de realizare a activităţilor	0,5	3	0,3	1	0,2	2	2,20

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Criterii de analiză a riscurilor						Punctaj total
					Aprecierea controlului intern		Aprecierea cantitativă		Aprecierea calitativă		
					P1 50%	N1	P2 30%	N2	P3 20%	N3	
			3.2.5. Activităţile operaţionale sunt conforme cu instrucţiunile din manualele de utilizare	Neconcordanţe între utilizarea unei aplicaţii sau program şi precizările din caietul tehnic, privind execuţia acelei operaţii	0,5	1	0,3	3	0,2	2	1,80
		3.3. Funcţionalitatea activităţilor în cadrul departamentului IT	3.3.1. Activităţile sunt bine organizate pentru asigurarea bunei funcţionării a departamentului	Lipsa revizuirii şi urmării contractelor la nivel de service şi a celor la nivel operativ	0,5	1	0,3	2	0,2	2	1,50
			3.3.2. Organizarea funcţională a activităţilor în cadrul departamentului IT	Activităţile şi acţiunile necesare realizării acestora nu sunt repartizate eficient şi omogen pe compartimente în cadrul departamentului IT	0,5	3	0,3	2	0,2	2	2,50
			3.3.3. Activităţile în cadrul departamentului sunt definite respectând criteriile de calitate	Activităţi şi acţiuni neresponsabilizate	0,5	1	0,3	1	0,2	3	1,40
			3.3.4. Evidenţa datelor aflate pe mediile de stocare	Acces nerestricţionat la date şi informaţii	0,5	2	0,3	1	0,2	2	1,70
			3.3.5. Distribuirea cu precizie a informaţiei către utilizatori şi mediile de stocare	Dependenţa de terţe părţi în centralizarea informaţiei şi oferirea rapoartelor	0,5	2	0,3	2	0,2	1	1,80
			3.3.6. Asigurarea caracterului secret al datelor	Accesul la datele şi informaţiile organizaţiei nu este limitat doar pentru persoanele îndreptăţite	0,5	3	0,3	2	0,2	1	2,30
			3.3.7. Soluţionarea problemelor presupune parcurgerea etapelor: iniţierea, planificarea, execuţia, monitorizarea şi analiza, încheierea	Soluţionarea unei probleme prin luarea în calcul doar a execuţiei acesteia	0,5	2	0,3	1	0,2	1	1,50
		3.4. Mentenanţa echipamentelor	3.4.1. Obţinerea de rapoarte de activitate utile	Rapoartele obţinute nu oferă informaţii suficiente pentru luarea deciziilor	0,5	2	0,3	2	0,2	2	2,00
			3.4.2. Întreţinerea calculatorului şi a echipamentelor	Disfuncţiile identificate nu sunt analizate şi înlăturate în conformitate cu instrucţiunile şi manualele de întreţinere	0,5	2	0,3	2	0,2	3	2,20

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Criterii de analiză a riscurilor						Punctaj total
					Aprecierea controlului intern		Aprecierea cantitativă		Aprecierea calitativă		
					P1 50%	N1	P2 30%	N2	P3 20%	N3	
			3.4.3. Instalarea şi configurarea calculatorului	Echipamentele periferice nu sunt instalate şi conectate conform documentaţiei	0,5	3	0,3	3	0,2	2	2,80
			3.1.1. Sistemul este întreţinut pentru a se asigura că este conform cu nevoile organizaţiei	Întreţinerea sistemului doar la solicitările utilizatorilor	0,5	1	0,3	1	0,2	2	1,20
		3.5. Utilizarea echipamentelor	3.5.1. Realizarea eficientă a operaţiilor în cadrul departamentului IT	Suportul tehnic cu privire la utilizarea programelor nu este furnizat în mod corespunzător utilizatorilor	0,5	2	0,3	3	0,2	2	2,30
			3.5.2. Identificarea şi raportarea pericolelor	Costuri ridicate cu remedierea defecţiunilor, frecvenţă mare a acestora, timpi mari până la reluarea lucrului	0,5	1	0,3	1	0,2	3	1,40
			3.5.3. Administrarea eficientă a aplicaţiilor şi programelor	Controlul intern asupra datelor de intrare nu este asigurat corespunzător	0,5	3	0,3	2	0,2	3	2,70
			3.5.4. Evaluarea problemelor şi soluţionarea acestora	Lipsa revizuirii şi urmării măsurilor privind corectarea erorilor conduce la persistenţa unora dintre acestea	0,5	2	0,3	1	0,2	3	1,90
			3.5.5. Programele corespund cerinţelor stabilite	Neadaptarea la schimbările rapide ale tehnologiei informaţiei	0,5	1	0,3	1	0,2	3	1,40
			3.5.6. Echipamentele sunt utilizate adecvat asigurând un confort în exploatare	Lipsa cunoştinţelor privind exploatarea echipamentelor la potenţialul maxim	0,5	1	0,3	2	0,2	2	1,50
4.	Securitatea informaţiilor	4.1. Organizarea securităţii informaţiilor	4.1.1. Crearea politicii de securitate a informaţiei	Organizarea şi responsabilităţile privind securitatea informaţiilor nu constituie o prioritate a politicii de securitate	0,5	2	0,3	1	0,2	1	1,50
			4.1.2. Crearea standardelor şi practicilor pentru securitatea informaţiei	Standardele privind securitatea informaţiei nu sunt definite formal	0,5	3	0,3	2	0,2	2	2,50
			4.1.3. Stabilirea responsabilităţilor privind securitatea informaţiei	Responsabilităţile nu sunt separate clar între cele ale administratorilor şi cele ale operatorilor;	0,5	1	0,3	2	0,2	2	1,50

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Criterii de analiză a riscurilor						Punctaj total
					Aprecierea controlului intern		Aprecierea cantitativă		Aprecierea calitativă		
					P1 50%	N1	P2 30%	N2	P3 20%	N3	
			4.1.4. Elaborarea politicii privind securitatea informaţiei	Datele şi informaţiile prelucrate şi stocate nu sunt asigurate în condiţii de confidenţialitate, integritate şi disponibilitate	0,5	3	0,3	2	0,2	2	2,50
			4.1.5. Stabilirea responsabilităţilor în cadrul politicii de securitate	Politica de securitate nu defineşte responsabilităţile cu privire la securitatea datelor şi informaţiilor	0,5	2	0,3	2	0,2	2	2,00
			4.1.6. Securitatea informaţiilor asigură integritatea acestora	Datele şi informaţiile nu sunt stocate în condiţii de securitate	0,5	2	0,3	1	0,2	1	1,50
			4.1.7. Securitatea datelor asigură disponibilitatea acestora doar pentru utilizatori autorizaţi	Accesul la informaţii şi pentru persoanele neautorizate	0,5	3	0,3	2	0,2	2	2,50
		4.2. Disponibilitatea datelor	4.2.1. Protejarea împotriva atacurilor informatice	Lipsa programelor de protecţie adecvate pentru aplicaţii şi programe	0,5	2	0,3	2	0,2	1	1,80
			4.2.2. Protejarea datelor împotriva viruşilor	Vulnerabilitate sporită în faţa viruşilor	0,5	3	0,3	2	0,2	3	2,70
			4.2.3. Asigurarea continuităţii activităţilor	Planurile privind continuitatea activităţilor nu stabilesc măsuri concrete pentru reluarea activităţii	0,5	1	0,3	2	0,2	2	1,50
			4.2.4. Recuperarea datelor în caz de dezastru	Lipsa planurilor de recuperare a datelor şi informaţiilor	0,5	1	0,3	2	0,2	2	1,50
			4.2.5. Protejarea împotriva asumării unei identităţii false	Sustragerea informaţiilor sau a echipamentelor, fără autorizare;	0,5	1	0,3	2	0,2	3	1,70
		4.3. Asigurarea funcţionării programelor şi aplicaţiilor	4.3.1. Asigurarea introducerii corecte a datelor şi informaţiilor pentru prelucrare	Aplicaţiile informatice nu sunt utilizate în conformitate cu instrucţiunile de exploatare	0,5	3	0,3	2	0,2	1	2,30
			4.3.2. Existenţa licenţelor pentru programele utilizate	Plata unor despăgubiri urmare implementării unor programe fără licenţă	0,5	2	0,3	1	0,2	1	1,50
			4.3.3. Prelucrarea datelor	Introducerea incorectă a datelor şi informaţiilor în cadrul programelor şi aplicaţiilor	0,5	3	0,3	2	0,2	2	2,50
			4.3.4. Asigurarea securităţii datelor şi informaţiilor	Accesul la datele şi informaţiile stocate nu este restricţionat şi autorizat pe niveluri ierarhice	0,5	2	0,3	2	0,2	2	2,00

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Criterii de analiză a riscurilor						Punctaj total
					Aprecierea controlului intern		Aprecierea cantitativă		Aprecierea calitativă		
					P1 50%	N1	P2 30%	N2	P3 20%	N3	
		4.4. Implementarea instrumentelor de control	4.4.1. Accesul la aplicaţie este oferit pe baza necesităţilor utilizatorului	Accesul la program, aplicaţie este oferit pentru întregul personal ce posedă o parolă	0,5	3	0,3	1	0,2	3	2,40
			4.4.2. Mecanismele de securitate configurate şi implementate verifică şi limitează accesul la aplicaţii	Pentru vulnerabilităţile sistemelor nu sunt stabilite şi implementate instrumente de control	0,5	2	0,3	1	0,2	1	1,50
			4.4.3. Introducerea instrumentelor de control fizic asupra echipamentelor IT	Accesul fizic la echipamente şi aplicaţii este restricţionat	0,5	3	0,3	2	0,2	2	2,50
			4.4.4. Stabilirea de chei de control pentru fiecare program sau aplicaţie	Posibilitatea de a obţine şi utiliza rezultate nesigure, neverificate	0,5	1	0,3	3	0,2	2	1,20
		4.5. Securitatea reţelei	4.5.1. Mecanismele de securitate configurate şi implementate asigură securitatea informaţiilor în cadrul reţelei	Metodele de criptare nu asigură protecţia integrităţii şi confidenţialităţii datelor sensibile	0,5	2	0,3	1	0,2	1	1,50
			4.5.2. Monitorizarea securităţii reţelelor	Comunicarea în reţea nu este securizată	0,5	2	0,3	2	0,2	1	1,80
		4.6. Gestionarea parolelor	4.61. Utilizatorii au parole de acces individuale	Accesul la aplicaţii se realizează direct, fără a fi permis doar pentru personalul îndreptăţit	0,5	2	0,3	2	0,2	2	2,00
			4.6.2. Schimbarea periodică a parolelor	Risc crescut de spargere a parolei	0,5	2	0,3	3	0,2	1	2,10
			4.6.3. Conturile şi parolele generice sunt folosite pentru accesul la sisteme şi aplicaţii	Conturile şi parolele generice iniţiale nu sunt personalizate după începerea prelucrărilor de către utilizatori	0,5	1	0,3	2	0,2	2	1,50
			4.6.4. Protejarea parolelor	Descărcarea ilegală a unor informaţii	0,5	3	0,3	2	0,2	1	2,30
			4.6.5. Persoanele autorizate au acces la sistemul de operare	Accesul la servere este permis întregului personal, nefiind înregistrat şi monitorizat	0,5	3	0,3	2	0,2	2	2,50
		4.7. Securitatea logică	4.7.1. Asigurarea securităţii funcţionării programelor şi aplicaţiilor	Lipsa controalelor sau controale slabe de acces	0,5	3	0,3	2	0,2	2	2,50

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Criterii de analiză a riscurilor						Punctaj total
					Aprecierea controlului intern		Aprecierea cantitativă		Aprecierea calitativă		
					P1 50%	N1	P2 30%	N2	P3 20%	N3	
			4.7.2.Protejarea sistemelor informatice împotriva factorilor de mediu	Lipsa controalelor de mediu, respectiv detectoare de foc, incendiu etc.	0,5	2	0,3	1	0,2	1	1,50
			4.7.3. Protejarea informaţiei din reţea	Funcţii de siguranţă sau control nu sunt prevăzute în cadrul sistemelor de aplicaţii	0,5	2	0,3	2	0,2	1	1,80
5	Proiectarea şi testarea programelor şi aplicaţiilor	5.1. Proiectarea şi elaborarea programelor şi aplicaţiilor	5.1.1. Proiectarea programului informatic	În proiectarea programului/aplicaţiei, fluxul de date nu este stabilit adecvat rezultatelor aşteptate	0,5	2	0,3	2	0,2	2	2,00
			5.1.2. Elaborarea programului informatic	Graficul de realizare a programului şi bugetul aprobat nu sunt respectate	0,5	3	0,3	2	0,2	2	2,50
			5.1.3. Proiectarea unui program sau aplicaţie tine cont de necesităţile organizaţiei	Elaborarea de programe şi aplicaţii fără o analiză strategică la nivelul utilizatorilor	0,5	2	0,3	2	0,2	1	1,80
			5.1.4. Proiectarea unui program sau aplicaţie pe baza existenţei resurselor financiare	Lipsa resurselor financiare în elaborarea şi implementarea unui program sau aplicaţie	0,5	2	0,3	2	0,2	2	1,80
			5.1.5. Respectarea cerinţelor în achiziţia unei aplicaţii	Costuri suplimentare în achiziţia unui program sau aplicaţie	0,5	1	0,3	1	0,2	3	1,40
		5.2. Testarea şi implementarea programelor şi aplicaţiilor	5.2.1. Utilizarea de date ipotetice în testarea unui program	Efectuarea de prelucrări asupra datelor reale în cadrul testării programelor	0,5	3	0,3	2	0,2	2	2,50
			5.2.2. Testarea programului şi aplicaţiei	Neconformităţile şi erorile constatate în cursul testării unui program nu sunt analizate cu atenţie	0,5	2	0,3	2	0,2	2	2,00
			5.2.3. Asigurarea corectitudinii rezultatelor	Opţiunile şi parametrii de lucru ai programului/aplicaţiei nu sunt stabiliţi conform specificaţiilor din documentaţiile tehnice	0,5	3	0,3	1	0,2	2	2,20
			5.2.4. Implementarea unui program după realizarea testării acestuia	Programele sau aplicaţiile achiziţionate sunt implementate fără a fi testate	0,5	2	0,3	1	0,2	1	1,50
6.	Elaborarea şi implementarea	6.1. Dezvoltarea proiectelor IT	6.1.1. Metodologia pentru dezvoltarea şi achiziţia aplicaţiei	Lipsa proiectelor de dezvoltare a achiziţiilor	0,5	1	0,3	2	0,2	2	1,50

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Criterii de analiză a riscurilor						Punctaj total
					Aprecierea controlului intern		Aprecierea cantitativă		Aprecierea calitativă		
					P1 50%	N1	P2 30%	N2	P3 20%	N3	
	proiectelor IT	(programe şi aplicaţii)	6.1.2. Iniţierea şi elaborarea proiectelor IT	Obiectivele generale ale proiectului nu sunt stabilite cu respectarea strategiei generale a organizaţiei	0,5	3	0,3	2	0,2	2	2,50
			6.1.3. Monitorizarea performanţelor soluţiilor IT implementate	Parametri de referinţă şi valorile etalon ale programelor elaborate nu respectă specificaţiile şi nu se încadrează în standarde	0,5	3	0,3	2	0,2	2	2,50
		6.2. Implementarea şi funcţionarea programelor şi aplicaţiilor	6.2.1. Reproiectarea soluţiilor IT pentru programe şi aplicaţii	Soluţiile privind îmbunătăţirea programelor şi aplicaţiilor nu ţin cont de punctele slabe şi critice, precum şi evoluţiile tehnologice	0,5	2	0,3	2	0,2	2	2,00
			6.2.2. Implementarea adecvată a aplicaţiilor	Rapoartele nu corespund cerinţelor	0,5	2	0,3	1	0,2	2	1,70
			6.2.3. Întreţinerea aplicaţiilor garantează funcţionarea proceselor la parametrii optimi	Supravegherea proceselor aflate în execuţie şi a performanţelor aplicaţiilor, sistemelor sau programelor nu respectă procedurile şi instrucţiunile	0,5	3	0,3	2	0,2	2	2,50
7.	Proiectarea şi menţinerea în funcţiune a unei reţele	7.1. Proiectarea, instalarea şi administrarea reţelei de calculatoare	7.1.1. Asigurarea bunei funcţionări a sistemelor bazate pe existenţa şi funcţionarea reţelei de calculatoare	Subsistemele existente nu sunt configurate şi supravegheate individual	0,5	3	0,3	2	0,2	2	2,50
			7.1.2. Monitorizarea performanţelor reţelelor	Scăderea performanţelor reţelelor	0,5	1	0,3	2	0,2	2	1,50
			7.1.3. Administrarea serverelor	Accesul şi utilizarea datelor şi informaţiilor stocate pe server nu respectă strategia de securitate a reţelei	0,5	2	0,3	2	0,2	2	2,00
			7.1.4. Reţeaua de calculatoare corespunde cerinţelor funcţionale	Reţeaua de calculatoare nu asigură integrarea informaţiilor şi elaborarea rapoartelor	0,5	2	0,3	1	0,2	1	1,50
		7.2. Interconectarea şi securitatea	7.2.1. Interconectarea reţelelor	Conexiunile dintre reţele nu sunt conforme cu arhitectura prevăzută de instrucţiuni şi nu respectă standardele	0,5	3	0,3	1	0,2	3	2,40

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Criterii de analiză a riscurilor						Punctaj total
					Aprecierea controlului intern		Aprecierea cantitativă		Aprecierea calitativă		
					P1 50%	N1	P2 30%	N2	P3 20%	N3	
		reţelei	7.2.2. Proiectarea şi asigurarea securităţii reţelei	Vulnerabilităţile şi ameninţările nu sunt identificate şi prioritizate	0,5	2	0,3	2	0,2	2	2,00
			7.2.3. Urmărirea adecvării performanţelor unei reţele	Conceperea unei reţele nu asigură integrarea programelor	0,5	2	0,3	1	0,2	2	1,70

Auditori,
Popescu Sorin
Radu George

Notă:

Stabilirea nivelului riscului şi determinarea punctajului total al riscurilor este documentul din procedura Analiza riscurilor în care auditorii apreciază nivelul riscului pe factorii de risc şi determină punctajul total al riscurilor pe baza documentelor în posesia cărora au intrat până în acel moment, dar şi pe baza expertizei personale în domeniu.

Elaborarea documentului **Stabilirea nivelului riscului şi a punctajului total al riscului** comportă două etape: în prima fază se realizează evaluarea nivelelor riscurilor asociate operaţiilor audiabile, iar în a doua fază se determină punctajul total pe baza formulei din Normele metodologice privind auditul intern, respectiv:

$$T = \sum_{i=1} P_i \times N_i$$

unde: P_i = ponderea riscului pentru fiecare criteriu
N_i = nivelul riscurilor pentru fiecare criteriu utilizat

Evaluarea riscurilor asociate operaţiilor audiabile pe baza informaţiilor în posesia cărora a intrat auditorul intern, până în acest moment, din documentele primite de la entitate şi/sau din rapoarte anterioare, dar şi din propria expertiza în domeniu are un oarecare grad de subiectivitate.

Procedura PO5 :	ANALIZA RISCULUI

Entitatea Publică
Serviciul de Audit Intern

CLASAREA OPERAŢIILOR ÎN FUNCŢIE DE ANALIZA RISCURILOR

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 07.09.2009
Avizat: Dumitru Daniel Data: 07.09.2009

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Pct. total	Clasare	Obs.
1.	Strategia şi planificarea sistemelor informatice	1.1. Strategia IT este concordantă cu scopurile organizaţiei	1.1.1. Strategia IT defineşte necesităţile şi priorităţile	Achiziţia şi implementarea programelor şi aplicaţiilor nu este corelată cu obiectivele propuse;	2,20	Mare	
			1.1.2. Strategia IT face trimitere la nevoile viitoare ale organizaţiei	Sistemele nu sunt dezvoltate într-o manieră planificată şi controlată	1,90	Mediu	
			1.1.3. Strategia defineşte direcţiile şi obiectivele de dezvoltare a IT	Strategia IT nu are o viziune orientată spre viitor, fiind o extrapolare a tendinţelor trecute	1,00	Mic	
		1.2. Planurile IT se adresează întregii organizaţii	1.2.1. Strategia IT este transpusă în planuri IT	Dezvoltarea IT nu acoperă toate procesele;	1,50	Mic	
			1.2.2. Planurile IT ajută la îndeplinirea misiunii organizaţiei	Planurile IT nu contribuie la realizarea scopului entităţii în domeniul IT;	2,00	Mediu	
			1.2.3. Planurile IT oferă asigurare cu privire la faptul că resursele IT sunt alocate în concordanţă cu necesităţile	Resursele IT nu sunt identificate pentru fiecare element al planului;	2,00	Mediu	
		1.3. Obiectivele IT îndeplinesc obiectivele organizaţiei	1.3.1. Strategia IT este concordantă cu scopurile organizaţiei	Utilizatorii şi IT nu au aceleaşi opinii cu privire la responsabilităţile şi autoritatea lor	2,10	Mare	
			1.3.2. Planurile IT se adresează întregii organizaţii	Planul IT nu acoperă cerinţele pe termen mediu;	1,50	Mic	
			1.3.3. Obiectivele IT îndeplinesc obiectivele organizaţiei	Obiectivele în domeniul IT nu derivă şi nu contribuie la realizarea obiectivelor entităţii;	1,70	Mic	
		1.4. Comitetul IT determină strategia IT	1.4.1. Strategia IT este stabilită de un comitet IT	Strategia IT este definită de departamentul IT;	2,00	Mediu	
			1.4.2. Comitetul IT transpune strategia în planuri pe termen scurt şi pe termen mediu	Comitetul IT nu contribuie la dezvoltarea şi implementarea strategiei în domeniu;	2,70	Mare	
			1.4.3. Comitetul IT stabileşte priorităţile proiectelor de dezvoltare a sistemelor IT	Stabilirea dezvoltării IT de către departamentul IT;	2,50	Mare	
		1.5. Organizarea IT corespunde	1.5.1. Organizarea adecvată a funcţiei IT	Responsabilităţile nu sunt definite clar în cadrul compartimentelor şi posturilor;	2,00	Mediu	

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Pct. total	Clasare	Obs.
		necesităţilor organizaţiei	1.5.2. Personalul IT are calificarea şi competenţele adecvate	Lipsa calificărilor necesare;	1,70	Mic	
			1.5.3. Adecvarea practicilor şi procedurilor IT la procesele existente	Programele şi aplicaţiile nu sunt integrate şi nu răspund cerinţelor activităţilor;	2,50	Mare	
		1.6. Elaborarea strategiei IT corespunde strategiei entităţii	1.6.1. Dotarea actuală cu tehnică de calcul a stat la baza elaborării strategiei IT	Infrastructura IT existentă nu asigură implementarea strategiei IT;	3,00	Mare	
			1.6.2. Realizarea strategiei IT pe baza evaluării sistemelor existente	Elaborarea strategiei nu are la bază şi o evaluare şi identificare a posibilităţilor financiare;	1,50	Mic	
2	Organizarea şi funcţionarea departamentului IT	2.1. Definirea atribuţiilor şi activităţilor	2.1.1. Definirea atribuţiilor şi responsabilităţilor în cadrul departamentului IT	Lipsa ariei de competenţă pentru realizarea activităţilor stabilite structurii funcţionale	2,40	Mare	
			2.1.2. Atribuţiile specifice departamentului sunt stabilite în cadrul atribuţiilor generale ale entităţii	Definirea de atribuţii care nu se regăsesc in ROF	1,50	Mic	
			2.1.3. Atribuţiile stabilite asigură realizarea activităţilor necesare implementării obiectivelor	Definirea atribuţiilor sub formă de sarcini	1,80	Mic	
			2.1.4. Identificarea tuturor activităţilor care concură la realizarea obiectivelor	Activităţi stabilite incorect pentru realizarea obiectivelor	1,80	Mic	
			2.1.5. Corelaţia între atribuţiile postului şi competenţele ocupantului postului	Stabilirea de sarcini diferite pentru aceleaşi funcţii sau aceleaşi sarcini pentru funcţii diferite	1,50	Mic	
			2.1.6. Definirea activităţilor în cadrul structurii organizatorice	Activităţile realizate la nivelul structurii funcţionale nu se regăsesc în totalitate în cadrul sarcinilor stabilite posturilor	2,40	Mare	
		2.2. Stabilirea structurii organizatorice	2.2.1. Organizarea funcţională a departamentului IT	Structura funcţională nu este adaptată complexităţii activităţilor derulate	1,90	Mediu	
			2.2.2. Definirea relaţiilor organizatorice între compartimente	Repartizarea activităţilor şi relaţiilor organizatorice fără a se ţine cont de natura organizării compartimentului	1,50	Mic	
			2.2.3. Examinarea sistemului de gestionare a riscurilor generale la nivelul departamentului IT	Riscurile nu sunt identificate şi gestionate la nivelul structurii funcţionale	2,50	Mare	
			2.2.4. Riscurile legate de securitatea datelor, programelor şi echipamentelor sunt identificate şi evaluate cât mai corect şi complet	Gestionarea slabă a riscurilor privind securitatea informaţiilor	2,40	Mare	
		2.3. Stabilirea responsabilităţilor	2.3.1. Definirea limitelor de competenţă	Autoritatea formală în realizarea activităţilor este insuficient stabilită postului	1,60	Mic	
			2.3.2. Definirea responsabilităţilor în realizarea activităţilor	Definirea doar a atribuţiilor, nu şi a limitei până unde răspunde ocupantul postului în realizarea activităţilor	1,80	Mic	
			2.3.3. Definirea sarcinilor prin fişa postului	Sarcinile stabilite postului potrivit fişei postului nu corespund cu acţiunile efectiv realizate de ocupantul postului	2,50	Mare	

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Pct. total	Clasare	Obs.
3.	Operaţii ale sistemului informatic	3.1 Managementul operaţiunilor	3.1.1. Existenţa listei operaţiunilor zilnice de realizat	Activităţile se realizează fără o prioritizare a operaţiilor	1,50	Mic	
			3.1.2. Performanţa, capacitatea şi disponibilitatea sistemelor informatice este monitorizată de administratori	Lipsa analizelor privind scopul şi cerinţele de realizare a activităţilor şi calitatea aplicaţiilor sau programelor utilizate	2.20	Mare	
			3.1.3. Responsabilitatea pentru supravegherea sarcinilor pe seturi de programe revine administratorilor	Responsabilităţile operatorilor nu sunt delimitate şi stabilite în funcţie de specializarea fiecăruia şi tipurile de aplicaţii şi programe utilizate	2,50	Mare	
			3.1.4. Elaborarea Planului anual de activitate	Activităţile sunt derulate în cadrul departamentului fără a exista o planificare anuală sau periodică	2,20	Mare	
		3.2. Managementul problemelor	3.2.1. Incidentele privind funcţionarea normală a serviciilor IT sunt rezolvate sau prevenite în termen	Soluţionarea cu întârziere a problemelor apărute în utilizarea aplicaţiilor şi programelor	1,00	Mic	
			3.2.2. Programele antivirus asigură protecţia aplicaţiilor	Utilizarea neadecvată a programelor antivirus	2,50	Mare	
			3.2.3. Problemele apărute sunt prioritizate şi luate în calcul pentru remediere	Soluţionarea problemelor apărute nu este realizată potrivit gravităţii şi asigurând eficienţa realizării activităţilor entităţii	1,40	Mic	
			3.2.4. Implementarea subsistemelor IT	Programele şi aplicaţiile derulate la nivelul organizaţiei nu sunt actualizate potrivit noilor necesităţi ca urmare a modificării acţiunilor de realizare a activităţilor	2,20	Mare	
			3.2.5. Activităţile operaţionale sunt conforme cu instrucţiunile din manualele de utilizare	Neconcordanţe între utilizarea unei aplicaţii sau program şi precizările din caietul tehnic, privind execuţia acelei operaţii	1,80	Mic	
		3.3. Funcţionalitatea activităţilor în cadrul departamentului IT	3.3.1. Activităţile sunt bine organizate pentru asigurarea bunei funcţionării a departamentului	Lipsa revizuirii şi urmării contractelor la nivel de service şi a celor la nivel operativ	1,50	Mic	
			3.3.2. Organizarea funcţională a activităţilor în cadrul departamentului IT	Activităţile şi acţiunile necesare realizării acestora nu sunt repartizate eficient şi omogen pe compartimente în cadrul departamentului IT	2,50	Mare	
			3.3.3. Activităţile în cadrul departamentului sunt definite respectând criteriile de calitate	Activităţi şi acţiuni neresponsabilizate	1,40	Mic	
			3.3.4. Evidenţa datelor aflate pe mediile de stocare	Acces nerestricţionat la date şi informaţii	1,70	Mic	
			3.3.5. Distribuirea cu precizie a informaţiei către utilizatori şi mediile de stocare	Dependenţa de terţe părţi în centralizarea informaţiei şi oferirea rapoartelor	1,80	Mic	
			3.3.6. Asigurarea caracterului secret al datelor	Accesul la datele şi informaţiile organizaţiei nu este limitat doar pentru persoanele îndreptăţite	2,30	Mare	

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Pct. total	Clasare	Obs.
			3.3.7. Soluţionarea problemelor presupune parcurgerea etapelor: iniţierea, planificarea, execuţia, monitorizarea şi analiza, încheierea	Soluţionarea unei probleme prin luarea în calcul doar a execuţiei acesteia	1,50	Mic	
		3.4. Mentenanţa echipamentelor	3.4.1. Obţinerea de rapoarte de activitate utile	Rapoartele obţinute nu oferă informaţii suficiente pentru luarea deciziilor	2,00	Mediu	
			3.4.2. Întreţinerea calculatorului şi a echipamentelor	Disfuncţiile identificate nu sunt analizate şi înlăturate în conformitate cu instrucţiunile şi manualele de întreţinere	2,20	Mare	
			3.4.3. Instalarea şi configurarea calculatorului	Echipamentele periferice nu sunt instalate şi conectate conform documentaţiei	2,80	Mare	
			3.1.1. Sistemul este întreţinut pentru a se asigura că este conform cu nevoile organizaţiei	Întreţinerea sistemului doar la solicitările utilizatorilor	1,20	Mic	
		3.5. Utilizarea echipamentelor	3.5.1. Realizarea eficientă a operaţiilor în cadrul departamentului IT	Suportul tehnic cu privire la utilizarea programului nu este acordat în mod corespunzător utilizatorilor	2,30	Mare	
			3.5.2. Identificarea şi raportarea pericolelor	Costuri ridicate cu remedierea defecţiunilor, frecvenţă mare a acestora, timpi mari până la reluarea lucrului	1,40	Mic	
			3.5.3. Administrarea eficientă a aplicaţiilor şi programelor	Controlul intern asupra datelor de intrare nu este asigurat corespunzător	2,70	Mare	
			3.5.4. Evaluarea problemelor şi soluţionarea acestora	Lipsa revizuirii şi urmării măsurilor privind corectarea erorilor conduce la persistenţa unora dintre acestea	1,90	Mediu	
			3.5.5. Programele corespund cerinţelor stabilite	Neadaptarea la schimbările rapide ale tehnologiei informaţiei	1,40	Mic	
			3.5.6. Echipamentele sunt utilizate adecvat asigurând un confort în exploatare	Lipsa cunoştinţelor privind exploatarea echipamentelor la potenţialul maxim	1,50	Mic	
4.	Securitatea informaţiilor	4.1. Organizarea securităţii informaţiilor	4.1.1. Crearea politicii de securitate a informaţiei	Organizarea şi responsabilităţile privind securitatea informaţiilor nu constituie o prioritate a politicii de securitate	1,50	Mic	
			4.1.2. Crearea standardelor şi practicilor pentru securitatea informaţiei	Standardele privind securitatea informaţiei nu sunt definite formal	2,50	Mare	
			4.1.3. Stabilirea responsabilităţilor privind securitatea informaţiei	Responsabilităţile nu sunt separate clar între cele ale administratorilor şi cele ale operatorilor	1,50	Mic	
			4.1.4. Elaborarea politicii privind securitatea informaţiei	Datele şi informaţiile prelucrate şi stocate nu sunt asigurate în condiţii de confidenţialitate, integritate şi disponibilitate	2,50	Mare	
			4.1.5. Stabilirea responsabilităţilor în cadrul politicii de securitate	Politica de securitate nu defineşte responsabilităţile cu privire la securitatea datelor şi informaţiilor	2,00	Mediu	

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Pct. total	Clasare	Obs.
			4.1.6. Securitatea informaţiilor asigură integritatea acestora	Datele şi informaţiile nu sunt stocate în condiţii de securitate	1,50	Mic	
			4.1.7. Securitatea datelor asigură disponibilitatea acestora doar pentru utilizatori autorizaţi	Accesul la informaţii şi pentru persoanele neautorizate	2,50	Mare	
		4.2. Disponibilitatea datelor	4.2.1. Protejarea împotriva atacurilor informatice	Lipsa programelor de protecţie adecvate pentru aplicaţii şi programe;	1,80	Mic	
			4.2.2. Protejarea datelor împotriva viruşilor	Vulnerabilitate sporită în faţa viruşilor	2,70	Mare	
			4.2.3. Asigurarea continuităţii activităţilor	Planurile privind continuitatea activităţilor nu stabilesc măsuri concrete pentru reluarea activităţii	1,50	Mic	
			4.2.4. Recuperarea datelor în caz de dezastru	Lipsa planurilor de recuperare a datelor şi informaţiilor	1,50	Mic	
			4.2.5. Protejarea împotriva asumării unei identităţii false	Sustragerea informaţiilor sau echipamentelor, fără autorizare	1,70	Mic	
		4.3. Asigurarea funcţionării programelor şi aplicaţiilor	4.3.1. Asigurarea introducerii corecte a datelor şi informaţiilor pentru prelucrare	Aplicaţiile informatice nu sunt utilizate în conformitate cu instrucţiunile de exploatare	2,30	Mare	
			4.3.2. Existenţa licenţelor pentru programele utilizate	Plata unor despăgubiri urmare implementării unor programe fără licenţă	1,50	Mic	
			4.3.3. Prelucrarea datelor	Introducerea incorectă a datelor şi informaţiilor în cadrul programelor şi aplicaţiilor	2,50	Mare	
			4.3.4. Asigurarea securităţii datelor şi informaţiilor	Accesul la datele şi informaţiile stocate nu este restricţionat şi autorizat pe niveluri ierarhice	2,00	Mediu	
		4.4. Implementarea instrumentelor de control	4.4.1. Accesul la aplicaţie este oferit pe baza necesităţilor utilizatorului	Accesul la program, aplicaţie este oferit pentru întregul personal ce posedă o parolă	2,40	Mare	
			4.4.2. Mecanismele de securitate configurate şi implementate verifică şi limitează accesul la aplicaţii	Pentru vulnerabilităţile sistemelor nu sunt stabilite şi implementate instrumente de control	1,50	Mic	
			4.4.3. Introducerea instrumentelor de control fizic asupra echipamentelor IT	Accesul fizic la echipamente şi aplicaţii este restricţionat	2,50	Mare	
			4.4.4. Stabilirea de chei de control pentru fiecare program sau aplicaţie	Posibilitatea de a obţine şi utiliza rezultate nesigure, neverificate	1,20	Mic	
		4.5. Securitatea reţelei	4.5.1. Mecanismele de securitate configurate şi implementate asigură securitatea informaţiilor în cadrul reţelei	Metodele de criptare nu asigură protecţia integrităţii şi confidenţialităţii datelor sensibile	1,50	Mic	
			4.5.2. Monitorizarea securităţii reţelelor	Comunicarea în reţea nu este monitorizată	1,80	Mic	
		4.6. Gestionarea parolelor	4.6.1. Utilizatorii au parole de acces individuale	Accesul la aplicaţii se realizează direct, fără a fi permis doar pentru personalul îndreptăţit	2,00	Mediu	
			4.6.2. Schimbarea periodică a parolelor	Risc crescut de spargere a parolei	2,10	Mare	

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Pct. total	Clasare	Obs.
			4.6.3. Conturile şi parolele generice sunt folosite pentru accesul la sisteme şi aplicaţii	Conturile şi parolele generice iniţiale nu sunt personalizate după începerea prelucrărilor de către utilizatori	1,50	Mic	
			4.6.4. Protejarea parolelor	Descărcarea ilegală a unor informaţii	2,50	Mare	
			4.6.5. Persoanele autorizate au acces la sistemul de operare	Accesul la servere este permis întregului personal, nefiind înregistrat şi monitorizat	2.30	Mare	
		4.7. Securitatea logică	4.7.1. Asigurarea securităţii funcţionării programelor şi aplicaţiilor	Lipsa controalelor sau controale slabe de acces	2,50	Mare	
			4.7.2.Protejarea sistemelor informatice împotriva factorilor de mediu	Lipsa controalelor de mediu, respectiv detectoare de foc, incendiu etc.	1,50	Mic	
			4.7.3. Protejarea informaţiei din reţea	Funcţii de siguranţă sau control nu sunt prevăzute în cadrul sistemelor de aplicaţii	1,80	Mic	
5	Proiectarea şi testarea programelor şi aplicaţiilor	5.1. Proiectarea şi elaborarea programelor şi aplicaţiilor	5.1.1. Proiectarea programului informatic	În proiectarea programului/aplicaţiei, fluxul de date nu este stabilit adecvat rezultatelor aşteptate	2,00	Mediu	
			5.1.2. Elaborarea programului informatic	Graficul de realizare a programului şi bugetul aprobat nu sunt respectate	2,50	Mare	
			5.1.3. Proiectarea unui program sau aplicaţie tine cont de necesităţile organizaţiei	Elaborarea de programe şi aplicaţii fără o analiză strategică la nivelul utilizatorilor	1,80	Mic	
			5.1.4. Proiectarea unui program sau aplicaţie pe baza existenţei resurselor financiare	Lipsa resurselor financiare în elaborarea şi implementarea unui program sau aplicaţie	1,80	Mic	
			5.1.5. Respectarea cerinţelor şi programelor în achiziţia unei aplicaţii	Costuri suplimentare în achiziţia unui program sau aplicaţie	1,40	Mic	
		5.2. Testarea şi implementarea programelor şi aplicaţiilor	5.2.1. Utilizarea de date ipotetice în testarea unui program	Efectuarea de prelucrări asupra datelor reale în cadrul testării programelor	2,50	Mare	
			5.2.2. Testarea programului şi aplicaţiei	Neconformităţile şi erorile constatate în cursul testării unui program nu sunt analizate cu atenţie	2,00	Mediu	
			5.2.3. Asigurarea corectitudinii rezultatelor	Opţiunile şi parametrii de lucru ai programului/aplicaţiei nu sunt stabiliţi conform specificaţiilor din documentaţiile tehnice	2,20	Mare	
			5.2.4. Implementarea unui program după realizarea testării acestuia	Programele sau aplicaţiile achiziţionate sunt implementate fără a fi testate	1,50	Mic	
6.	Elaborarea şi implementarea proiectelor IT	6.1. Dezvoltarea proiectelor IT (programe şi aplicaţii)	6.1.1. Metodologia pentru dezvoltarea şi achiziţia aplicaţiei	Lipsa proiectelor de dezvoltare a achiziţiilor	1,50	Mic	
			6.1.2. Iniţierea şi elaborarea proiectelor IT	Obiectivele generale ale proiectului nu sunt stabilite cu respectarea strategiei generale a organizaţiei	2,50	Mare	
			6.1.3. Monitorizarea performanţelor soluţiilor IT implementate	Parametri de referinţă şi valorile etalon ale programelor elaborate nu respectă specificaţiile şi nu se încadrează în standarde	2,50	Mare	

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	Pct. total	Clasare	Obs.
		6.2. Implementarea şi funcţionarea programelor şi aplicaţiilor	6.2.1. Reproiectarea soluţiilor IT pentru programe şi aplicaţii	Soluţiile privind îmbunătăţirea programelor şi aplicaţiilor nu ţin cont de punctele slabe şi critice, precum şi evoluţiile tehnologice	2,00	Mediu	
			6.2.2. Implementarea adecvată a aplicaţiilor	Rapoartele nu corespund cerinţelor	1,70	Mic	
			6.2.3. Întreţinerea aplicaţiilor garantează funcţionarea proceselor la parametrii optimi	Supravegherea proceselor aflate în execuţie şi a performanţelor aplicaţiilor, sistemelor sau programelor nu respectă procedurile şi instrucţiunile	2,50	Mare	
7.	Proiectarea şi menţinerea în funcţiune a unei reţele	7.1. Proiectarea, instalarea şi administrarea reţelei de calculatoare	7.1.1. Asigurarea bunei funcţionări a sistemelor bazate pe existenţa şi funcţionarea reţelei de calculatoare	Subsistemele existente nu sunt configurate şi supravegheate individual	2,50	Mare	
			7.1.2. Monitorizarea performanţelor reţelelor	Scăderea performanţelor reţelelor	1,50	Mic	
			7.1.3. Administrarea serverelor	Accesul şi utilizarea datelor şi informaţiilor stocate pe server nu respectă strategia de securitate a reţelei	2,00	Mediu	
			7.1.4. Reţeaua de calculatoare corespunde cerinţelor funcţionale	Reţeaua de calculatoare nu asigură integrarea informaţiilor şi elaborarea rapoartelor	1,50	Mic	
		7.2. Interconectarea şi securitatea reţelei	7.2.1. Interconectarea reţelelor	Conexiunile dintre reţele nu sunt conforme cu arhitectura prevăzută de instrucţiuni şi nu respectă standardele	2,40	Mare	
			7.2.2. Proiectarea şi asigurarea securităţii reţelei	Vulnerabilităţile şi ameninţările nu sunt identificate şi prioritizate	2,00	Mediu	
			7.2.2. Urmărirea adecvării performanţelor unei reţele	Proiectarea reţelei de calculatoare nu asigură integrarea programelor	1,70	Mic	

Auditori,
Popescu Sorin
Radu George

Notă:

Clasarea activităţilor sau operaţiilor în funcţie de punctajul riscurilor este a şasea fază a procedurii *Analiza riscurilor*, în care riscurile se împart în mari, medii şi mici.

Împărţirea riscurilor în cele trei categorii se realizează ţinând cont de importanţa riscurilor şi de resursele de audit de care dispunem, respectiv numărul de auditori intern si numărul de ore efectuate pentru desfăşurarea misiunii de audit.

În mod special, activitatea de împărţire a riscurilor pe cele trei categorii trebuie să ţină cont de resursele alocate misiunii (număr de persoane, timpul aferent ş.a.), respectiv să aibă în vedere volumul riscurilor pe care le poate auditat şi să renunţe pentru moment la riscurile care pot fi neglijate. Numărul riscurilor medii se recomandă să fie foarte redus (5-10%), pentru că acesta demonstrează o nehotărâre din partea auditorilor interni. În general, riscurile medii se acordă pentru operaţiile pe care auditorii interni nu le cunosc bine din practic şi care vor fi cuprinse în auditare.

Pentru continuarea analizei, auditorii interni au împărţit in cele trei categorii (mari, medii si mici) riscurile din documentul *Stabilirea nivelului riscului şi a punctajului total*, ţinând cont şi de resursele alocate misiunii (număr de persoane, timpul aferent ş.a.), astfel:

- Riscuri mici 1,0 - 1,7
- Riscuri medii 1,8 - 2,3
- Riscuri mari 2,4 - 3,0

Pentru moment, riscurile mici vor fi ignorate, in sensul ca nu vor fi auditate, iar riscurile semnificative (mari şi medii) vor intra în faza de ierarhizare, ocazie cu care se va elabora documentul *Tabelul puncte tari şi puncte slabe*.

Procedura PO5 :	ANALIZA RISCULUI

Entitatea Publică
Serviciul de Audit Intern

TABELUL PUNCTE TARI ŞI PUNCTE SLABE

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 07.09.2009
Avizat: Dumitru Daniel Data: 07.09.2009

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	T/ S	Consecinţa funcţionarii/ nefuncţionării controlului intern	Grad încredere in control intern	Obs.
1.	Strategia şi planificarea sistemelor informatice	1.1. Strategia IT este concordantă cu scopurile organizaţiei	1.1.1. Strategia IT defineşte necesităţile şi priorităţile	Achiziţia şi implementarea programelor şi aplicaţiilor nu este corelată cu obiectivele propuse;	S		Scăzut	
		1.2. Planurile IT se adresează întregii organizaţii	1.2.2. Planurile IT ajută la îndeplinirea misiunii organizaţiei	Planurile IT nu contribuie la realizarea scopului entităţii în domeniul IT;	S		Scăzut	
			1.2.3. Planurile IT oferă asigurare cu privire la faptul că resursele IT sunt alocate în concordanţă cu necesităţile	Resursele IT nu sunt identificate pentru fiecare element al planului;	S		Scăzut	
		1.3. Obiectivele IT îndeplinesc obiectivele organizaţiei	1.3.1. Strategia IT este concordantă cu scopurile organizaţiei	Utilizatorii şi IT nu au aceleaşi opinii cu privire la responsabilităţile şi autoritatea lor	S		Scăzut	
		1.4. Comitetul IT determină strategia IT	1.4.1. Strategia IT este stabilită de un comitet IT	Strategia IT este definită de departamentul IT;	T		Ridicat	
			1.4.2. Comitetul IT transpune strategia în planuri pe termen scurt şi pe termen mediu	Comitetul IT nu contribuie la dezvoltarea şi implementarea strategiei în domeniu;	S		Scăzut	

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	T/ S	Consecinţa funcţionarii/ nefuncţionării controlului intern	Grad încredere in control intern	Obs.
			1.4.3. Comitetul IT stabileşte prioritătile proiectelor de dezvoltare a sistemelor IT	Stabilirea dezvoltării IT de către departamentul IT;	S		Scăzut	
		1.5. Organizarea IT corespunde necesităţilor organizaţiei	1.5.1. Organizarea adecvată a funcţiei IT	Responsabilităţile nu sunt definite clar în cadrul compartimentelor şi posturilor;	S		Scăzut	
			1.5.3. Adecvarea practicilor şi procedurilor IT la procesele existente	Programele şi aplicaţiile nu sunt integrate şi nu răspund cerinţelor activităţilor;	S		Scăzut	
		1.6. Elaborarea strategiei IT corespunde strategiei entităţii	1.6.1. Dotarea actuală cu tehnică de calcul a stat la baza elaborării strategiei IT	Infrastructura IT existentă nu asigură implementarea strategiei IT;	S		Scăzut	
2.	Organizarea şi funcţionarea departamentului IT	2.1. Definirea atribuţiilor şi activităţilor	2.1.1. Definirea atribuţiilor şi responsabilităţilor în cadrul departamentului IT	Lipsa ariei de competenţă pentru realizarea activităţilor stabilite structurii funcţionale	S		Scăzut	
			2.1.6. Definirea activităţilor în cadrul structurii organizatorice	Activităţile realizate la nivelul structurii funcţionale nu se regăsesc în totalitate în cadrul sarcinilor stabilite posturilor	S		Scăzut	
		2.2. Stabilirea structurii organizatorice	2.2.1. Organizarea funcţională a departamentului IT	Structura funcţională nu este adaptată complexităţii activităţilor derulate	S		Scăzut	
			2.2.3. Examinarea sistemului de gestionare a riscurilor generale la nivelul departamentului IT	Riscurile nu sunt identificate şi gestionate la nivelul structurii funcţionale	S		Scăzut	
			2.2.4. Riscurile legate de securitatea datelor, programelor şi echipamentelor sunt identificate şi evaluate cât mai corect şi complet.	Gestionarea slabă a riscurilor privind securitatea informaţiilor	T		Ridicat	

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	T/ S	Consecinţa funcţionarii/ nefuncţionării controlului intern	Grad încredere in control intern	Obs.
		2.3. Stabilirea responsabilităţilor	2.3.3. Definirea sarcinilor prin fişa postului	Sarcinile stabilite postului potrivit fişei postului nu corespund cu acţiunile efectiv realizate de ocupantul postului	S		Scăzut	
3.	Operaţii ale sistemului informatic	3.1 Managementul operaţiunilor	3.1.2. Performanţa, capacitatea si disponibilitatea sistemelor informatice este monitorizată de administratori	Lipsa analizelor privind scopul şi cerinţele de realizare a activităţilor şi calitatea aplicaţiilor sau programelor utilizate	S		Scăzut	
			3.1.3. Responsabilitatea pentru supravegherea sarcinilor pe seturi de programe revine administratorilor	Responsabilităţile operatorilor nu sunt delimitate şi stabilite în funcţie de specializarea fiecăruia şi tipurile de aplicaţii şi programe utilizate	S		Scăzut	
			3.1.4. Elaborarea Planului anual de activitate	Activităţile sunt derulate în cadrul departamentului fără a exista o planificare anuală sau periodică	S		Scăzut	
		3.2. Managementul problemelor	3.2.2. Programele antivirus asigură protecţia aplicaţiilor	Utilizarea neadecvată a programelor antivirus	S		Scăzut	
			3.2.4. Implementarea subsistemelor IT	Programele şi aplicaţiile derulate la nivelul organizaţiei nu sunt actualizate potrivit noilor necesităţi ca urmare a modificării acţiunilor de realizare a activităţilor	S		Scăzut	
		3.3. Funcţionalitatea activităţilor în cadrul departamentului IT	3.3.2. Organizarea funcţională a activităţilor în cadrul departamentului IT	Activităţile şi acţiunile necesare realizării acestora nu sunt repartizate eficient şi omogen pe compartimente în cadrul departamentului IT	S		Scăzut	

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	T/ S	Consecinţa funcţionarii/ nefuncţionării controlului intern	Grad încredere in control intern	Obs.
			3.3.6. Asigurarea caracterului secret al datelor	Accesul la datele şi informaţiile organizaţiei nu este limitat doar pentru persoanele îndreptăţite	S		Scăzut	
		3.4. Mentenanţa echipamentelor	3.4.1. Obţinerea de rapoarte de activitate utile	Rapoartele obţinute nu oferă informaţii suficiente pentru luarea deciziilor	T		Ridicat	
			3.4.2. Întreţinerea calculatorului şi a echipamentelor	Disfuncţiunile identificate nu sunt analizate şi înlăturate în conformitate cu instrucţiunile şi manualele de întreţinere	S		Scăzut	
			3.4.3. Instalarea şi configurarea calculatorului	Echipamentele periferice nu sunt instalate şi conectate conform documentaţiei	S		Scăzut	
		3.5. Utilizarea echipamentelor	3.5.1. Realizarea eficientă a operaţiilor în cadrul departamentului IT	Suportul tehnic cu privire la utilizarea programelor nu este furnizat în mod corespunzător utilizatorilor	S		Scăzut	
			3.5.3. Administrarea eficientă a aplicaţiilor şi programelor	Controlul intern asupra datelor de intrare nu este asigurat corespunzător	S		Scăzut	
			3.5.4. Evaluarea problemelor şi soluţionarea acestora	Lipsa revizuirii şi urmăririi măsurilor privind corectarea erorilor conduce la persistenţa unora dintre acestea	S		Scăzut	
4.	Securitatea informaţiilor	4.1. Organizarea securităţii informaţiilor	4.1.2. Crearea standardelor şi practicilor pentru securitatea informaţiei	Standardele privind securitatea informaţiei nu sunt definite formal	T		Ridicat	
			4.1.4. Elaborarea politicii privind securitatea informaţiei	Datele şi informaţiile prelucrate şi stocate nu sunt asigurate în condiţii de confidenţialitate, integritate şi disponibilitate;	S		Scăzut	

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	T/ S	Consecinţa funcţionarii/ nefuncţionării controlului intern	Grad încredere in control intern	Obs.
			4.1.5. Stabilirea responsabilităţilor în cadrul politicii de securitate	Politica de securitate nu defineşte responsabilităţile cu privire la securitatea datelor şi informaţiilor	S		Scăzut	
			4.1.7. Securitatea datelor asigură disponibilitatea acestora doar pentru utilizatori autorizaţi	Accesul la informaţii şi pentru persoanele neautorizate	S		Scăzut	
		4.2. Disponibilitatea datelor	4.2.2. Protejarea datelor împotriva viruşilor	Vulnerabilitate sporită în faţa viruşilor	S		Scăzut	
			4.2.3. Asigurarea continuităţii activităţilor	Planurile privind continuitatea activităţilor nu stabilesc măsuri concrete pentru reluarea activităţii	S		Scăzut	
			4.2.4. Recuperarea datelor în caz de dezastru	Lipsa planurilor de recuperare a datelor şi informaţiilor	S		Scăzut	
		4.3. Asigurarea funcţionării programelor şi aplicaţiilor	4.3.1. Asigurarea introducerii corecte a datelor şi informaţiilor pentru prelucrare	Aplicaţiile informatice nu sunt utilizate în conformitate cu instrucţiunile de exploatare	S		Scăzut	
			4.3.3. Prelucrarea datelor	Introducerea incorectă a datelor şi informaţiilor în cadrul programelor şi aplicaţiilor	S		Scăzut	
			4.3.4. Asigurarea securităţii datelor şi documentelor	Accesul la datele şi informaţiile stocate nu este restricţionat şi autorizat pe niveluri ierarhice	S		Scăzut	
		4.4. Implementarea instrumentelor de control	4.4.1. Accesul la aplicaţie este oferit pe baza necesităţilor utilizatorului	Accesul la program, aplicaţie este oferit pentru întregul personal ce posedă o parolă	S		Scăzut	
			4.4.3. Introducerea instrumentelor de control fizic asupra echipamentelor IT	Accesul fizic la echipamente şi aplicaţii nu este restricţionat	S		Scăzut	

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	T/ S	Consecinţa funcţionarii/ nefuncţionării controlului intern	Grad încredere in control intern	Obs.
		4.5. Securitatea reţelei	4.5.2. Monitorizarea securităţii reţelelor	Comunicarea datelor în reţea nu este monitorizată	S		Scăzut	
		4.6. Gestionarea parolelor	4.61. Utilizatorii au parole de acces individuale	Accesul la aplicaţii se realizează direct, fără a fi permis doar pentru personalul îndreptăţit	S		Scăzut	
			4.6.2. Schimbarea periodică a parolelor	Risc crescut de spargere a parolei	S		Scăzut	
			4.6.4. Protejarea parolelor	Descărcarea ilegală a unor informaţii	S		Scăzut	
			4.6.5. Persoanele autorizate au acces la sistemul de operare	Accesul la servere este permis întregului personal, nefiind înregistrat şi monitorizat	S		Scăzut	
		4.7. Securitatea logică	4.7.1. Asigurarea securităţii funcţionării programelor şi aplicaţiilor	Lipsa controalelor sau controale slabe de acces	S		Scăzut	
5	Proiectarea şi testarea programelor şi aplicaţiilor	5.1. Proiectarea şi elaborarea programelor şi aplicaţiilor	5.1.1. Proiectarea programului informatic	În proiectarea programului/ aplicaţiei, fluxul de date nu este stabilit adecvat rezultatelor aşteptate	S		Scăzut	
			5.1.2. Elaborarea programului informatic	Graficul de realizare a programului şi bugetul aprobat nu sunt respectate	S		Scăzut	
		5.2. Testarea şi implementarea programelor şi aplicaţiilor	5.2.1. Utilizarea de date ipotetice în testarea unui program	Efectuarea de prelucrări asupra datelor în cadrul testării programelor	T		Ridicat	
			5.2.2. Testarea programului şi aplicaţiei	Neconformităţile şi erorile constatate în cursul testării unui program nu sunt analizate cu atenţie	S		Scăzut	

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	T/ S	Consecinţa funcţionarii/ nefuncţionării controlului intern	Grad încredere in control intern	Obs.
			5.2.3. Asigurarea corectitudinii rezultatelor	Opţiunile şi parametrii de lucru ai programului/aplicaţiei nu sunt stabiliţi conform specificaţiilor din documentaţiile tehnice	S		Scăzut	
6.	Elaborarea şi implementarea proiectelor IT	6.1. Dezvoltarea proiectelor IT (programe şi aplicaţii)	6.1.2. Iniţierea şi elaborarea proiectelor IT	Obiectivele generale ale proiectului nu sunt stabilite cu respectarea strategiei generale a organizaţiei	S		Scăzut	
			6.1.3. Monitorizarea performanţelor soluţiilor IT implementate	Parametri de referinţă şi valorile etalon ale programelor elaborate nu respectă specificaţiile şi nu se încadrează în standarde	S		Scăzut	
		6.2. Implementarea şi funcţionarea programelor şi aplicaţiilor	6.2.1. Reproiectarea soluţiilor IT pentru programe şi aplicaţii	Soluţiile privind îmbunătăţirea programelor şi aplicaţiilor nu ţin cont de punctele slabe şi critice, precum şi evoluţiile tehnologice	S		Scăzut	
			6.2.3. Întreţinerea aplicaţiilor garantează funcţionarea proceselor la parametrii optimi	Supravegherea proceselor aflate în execuţie şi a performanţelor aplicaţiilor, sistemelor sau programelor nu respectă procedurile şi instrucţiunile	S		Scăzut	
7.	Proiectarea şi menţinerea în funcţiune a unei reţele	7.1. Proiectarea, instalarea şi administrarea reţelei de	7.1.1. Asigurarea bunei funcţionări a sistemelor bazate pe existenţa şi funcţionarea reţelei de calculatoare	Subsistemele existente nu sunt configurate şi supravegheate individual,	S		Scăzut	

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Riscuri semnificative	T/ S	Consecinţa funcţionarii/ nefuncţionării controlului intern	Grad încredere in control intern	Obs.
		calculatoare	7.1.3. Administrarea serverelor	Accesul şi utilizarea datelor şi informaţiilor stocate pe server nu respectă strategia de securitate a reţelei	S		Scăzut	
		7.2. Interconectarea şi securitatea reţelei	7.2.1. Interconectarea reţelelor	Conexiunile dintre reţele nu sunt conforme cu arhitectura prevăzută de instrucţiuni şi nu respectă standardele;	S		Scăzut	
			7.2.2. Proiectarea şi asigurarea securităţii reţelei	Vulnerabilităţile şi ameninţările nu sunt identificate şi prioritizate	S		Scăzut	

Auditori,

Popescu Sorin
Radu George

Notă:

În faza de ierarhizare se elaborează documentul *Tabelul puncte tari şi puncte slabe*, prin preluarea operaţiilor auditabile cu riscuri semnificative (mari şi medii) din documentul *Clasarea operaţiilor*, respectiv un număr de 70 obiecte audiabile şi 70 de riscuri asociate acestora.

Ierarhizarea obiectelor audiabile constă în evaluarea funcţionalităţii sistemelor de control intern care limitează efectele riscurilor şi care dau posibilitatea auditorilor interni să aprecieze acele obiecte audiabile ca fiind „*puncte tari",* celelalte riscuri pentru care nu exista activităţi de control sau acestea sunt nefuncţionale sunt in continuare considerate „*puncte slabe*". Astfel, în urma analizei au rezultat 6 riscuri asociate obiectelor audiabile care au fost evaluate ca fiind "puncte tari" şi care vor fi eliminate din auditare.

Pornind de la documentul Tabelul puncte tari şi puncte slabe se va elabora documentul *Tematica în detaliu* a misiunii de audit în care vor fi preluate numai operaţiile considerate ca fiind puncte slabe, ocazie cu care vor fi renumerotate si stabilita corespondenta cu paragrafele din Raportul de audit intern..

„*Un punct tare*" sau „*un punct slab*" trebuie să fie exprimat în funcţie de un obiectiv de control intern sau de o caracteristică urmărită, pentru a asigura buna funcţionare a structurii auditate.

Documentul *Tabelul puncte tari şi puncte slabe* conţine atât gradul de încredere al auditorului intern în funcţionarea controlului intern, cât şi consecinţele funcţionării/nefuncţionării acestuia, care va conduce la minimizarea riscului, atunci când gradul de încredere este mare (punct tare), şi la maximizarea apariţiei riscului, atunci când gradul de încredere este mic (punct slab).

Procedura PO5 :	ANALIZA RISCULUI

Entitatea Publică
Serviciul de Audit Intern

TEMATICA ÎN DETALIU

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 07.09.2009
Avizat: Dumitru Daniel Data: 07.09.2009

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Paragraful corespunzător din RAI
1.	Strategia şi planificarea sistemelor informatice	Strategia IT este concordantă cu scopurile organizaţiei	Strategia IT defineşte necesităţile şi priorităţile	II 1.1.1.
		Planurile IT se adresează întregii organizaţii	Planurile IT ajută la îndeplinirea misiunii organizaţiei	II 1.2.1
			Planurile IT oferă asigurare cu privire la faptul că resursele IT sunt alocate în concordanţă cu necesităţile	II 1.2.2
		Obiectivele IT îndeplinesc obiectivele organizaţiei	Strategia IT este concordantă cu scopurile organizaţiei	II 1.3.1
		Comitetul IT determină strategia IT	Comitetul IT transpune strategia în planuri pe termen scurt şi pe termen mediu	II 1.4.1.
			Comitetul IT stabileşte priorităţile proiectelor între dezvoltarea sistemelor şi activităţile realizate	II 1.4.2.
		Organizarea IT corespunde necesităţilor organizaţiei	Organizarea adecvată a funcţiei IT	II 1.5.1.
			Adecvarea practicilor şi procedurilor IT la procesele existente	II 1.5.2.
		Elaborarea strategiei IT corespunde strategiei entităţii	Dotarea actuală cu tehnică de calcul a stat la baza strategiei IT	II 1.6.1.
2	Organizarea şi funcţionarea departamentului IT	Definirea atribuţiilor şi activităţilor	Definirea atribuţiilor şi responsabilităţilor în cadrul departamentului IT	II 2.1.1.
			Definirea activităţilor în cadrul structurii organizatorice	II 2.1.2.
		Stabilirea structurii organizatorice	Organizarea funcţională a departamentului IT	II 2.2.1.
			Examinarea sistemului de gestionare a riscurilor generale la nivelul departamentului IT	II 2.2.2.
		Stabilirea responsabilităţilor	Definirea sarcinilor prin fişa postului	II 2.3.1.
3.	Operaţii ale sistemului informatic	Managementul operaţiunilor	Performanţa, capacitatea si disponibilitatea sistemelor informatice este monitorizată de administratori	II 3.1.1.
			Responsabilitatea pentru supravegherea sarcinilor pe seturi de programe revine administratorilor	II 3.1.2.
			Elaborarea planului anual de activitate	II 3.1.3.
		Managementul problemelor	Programele antivirus asigură protecţia aplicaţiilor	II 3.2.1.
			Implementarea subsistemelor IT	II 3.2.2.
		Funcţionalitatea activităţilor în cadrul departamentului IT	Organizarea funcţională a activităţilor în cadrul departamentului IT	II 3.3.1.
			Asigurarea caracterului secret al datelor	II 3.3.2.
		Mentenanţa echipamentelor	Întreţinerea calculatorului şi a echipamentelor	II 3.4.21
			Instalarea şi configurarea calculatorului	II 3.4.2.

Nr crt	Domeniul	Activităţi/ obiective	Obiecte auditabile	Paragraful corespunzător din RAI
		Utilizarea echipamentelor	Realizarea eficientă a operaţiilor în cadrul departamentului IT	II 3.5.1.
			Administrarea eficientă a aplicaţiilor şi programelor	II 3.5.2.
			Evaluarea problemelor şi soluţionarea acestora	II 3.5.3.
4.	Securitatea informaţiilor	Organizarea securităţii informaţiilor	Elaborarea politicii privind securitatea informaţiei	II 4.1.1.
			Stabilirea responsabilităţilor în cadrul politicii de securitate	II 4.1.2.
			Securitatea datelor asigură disponibilitatea acestora doar pentru utilizatori autorizaţi	II 4.1.3.
		Disponibilitatea datelor	Protejarea datelor împotriva viruşilor	II 4.2.1.
			Asigurarea continuităţii activităţilor	II 4.2.2.
			Recuperarea datelor în caz de dezastru	II 4.2.3.
		Asigurarea funcţionării programelor şi aplicaţiilor	Asigurarea introducerii corecte a datelor şi informaţiilor pentru prelucrare	II 4.3.1.
			Prelucrarea datelor	II 4.3.2.
			Asigurarea securităţii datelor şi documentelor	II 4.3.3.
		Implementarea instrumentelor de control	Accesul la aplicaţie este oferit pe baza necesităţilor utilizatorului	II 4.4.1.
			Introducerea instrumentelor de control fizic asupra echipamentelor IT	II 4.4.2.
		Securitatea reţelei	Monitorizarea securităţii reţelelor	II 4.5.1.
		Gestionarea parolelor	Utilizatorii au parole de acces individuale	II 4.6.1.
			Schimbarea periodică a parolelor	II 4.6.2.
			Protejarea parolelor	II 4.6.3.
			Persoanele autorizate au acces la sistemul de operare	II 4.6.4.
		Securitatea logică	Asigurarea securităţii funcţionării programelor şi aplicaţiilor	II 4.7.1.
5	Proiectarea şi testarea programelor şi aplicaţiilor	Proiectarea şi elaborarea programelor şi aplicaţiilor	Proiectarea programului informatic	II 5.1.1.
			Elaborarea programului informatic	II 5.1.2.
		Testarea şi implementarea programelor şi aplicaţiilor	Testarea programului şi aplicaţiei	II 5.2.1.
			Asigurarea corectitudinii rezultatelor	II 5.2.2.
6.	Elaborarea şi implementarea proiectelor IT	Dezvoltarea proiectelor IT (programe şi aplicaţii)	Iniţierea şi elaborarea proiectelor IT	II 6.1.1.
			Monitorizarea performanţelor soluţiilor IT implementate	II 6.1.22.
		Implementarea şi funcţionarea programelor şi aplicaţiilor	Reproiectarea soluţiilor IT pentru programe şi aplicaţii	II 6.2.1.
			Întreţinerea aplicaţiilor garantează funcţionarea proceselor la parametrii optimi	II 6.2.2.
7.	Proiectarea şi menţinerea în funcţiune a unei reţele	Proiectarea, instalarea şi administrarea reţelei de calculatoare	Asigurarea bunei funcţionări a sistemelor bazate pe existenţa şi funcţionarea reţelei de calculatoare	II 7.1.1.
			Administrarea serverelor	II 7.1.2.
		Interconectarea şi securitatea reţelei	Interconectarea reţelelor	II 7.2.1.
			Proiectarea şi asigurarea securităţii reţelei	II 7.2.2

Auditori,

Popescu Sorin
Radu George

Notă:

Procedura Analiza riscurilor a început cu elaborarea documentului Lista centralizatoare a obiectelor audiabile şi se finalizează cu Tematica în detaliu a misiunii de audit.

Tematica în detaliu a misiunii de audit, este acea fază din procedura Analizei riscurilor, care se realizează prin selectarea obiectelor audiabile, pornind de la documentul Tabelul puncte tari şi puncte slabe, care au fost evaluate ca fiind puncte slabe si care vor fi avute in vedere, in continuare, pentru auditare.

Documentul, semnat de echipa de auditori şi de supervizorul misiunii, respectiv de şeful compartimentului de audit intern, va fi adus la cunoştinţă principalilor responsabili ai entităţii auditate în cadrul Şedinţei de deschidere.

În continuare, operaţii/obiecte audiabile, vor fi avute în vedere în activitatea de auditare, deoarece reprezintă riscuri semnificative pentru domeniul auditat şi vor fi supuse diferitelor testări, stabilite pe baza Programului intervenţiei la faţa locului, care se vor materializa în FIAP-uri şi FCRI-uri, acolo unde este cazul, şi în final vor fi transferate şi comentate în Raportul de audit intern, în ordinea din Tematica în detaliu a misiunii de audit.

Procedura PO6:	ELABORAREA PROGRAMULUI DE AUDIT

Entitatea Publică
Serviciul de Audit Intern

PROGRAMUL DE AUDIT

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 08.09.2009
Avizat: Dumitru Daniel Data: 08.09.2009

OBIECTIVELE AUDITULUI	ACTIVITĂŢILE PROGRAMATE	DURATA (H)	PERSOANELE IMPLICATE	LOCUL DESFĂŞURĂRII
Tema generală: **Activitatea IT**		**388**		
1. Pregătirea misiunii de audit		**54**		
	1. Tipărirea şi procesarea Ordinului de serviciu	2	Dumitru Daniel	SAI
	2. Tipărirea şi procesarea Declaraţiei de independenţa	2	Popescu Sorin	SAI
	3. Pregătirea şi transmiterea Notificării privind declanşarea misiunii de audit intern către părţile interesate	4	Radu George	SAI
	4. Colectarea şi prelucrarea informaţiilor	8	Popescu Sorin Radu George	SAI AUDITAT
	5. Întocmirea Listei centralizatoare a obiectelor audiabile	8	Popescu Sorin Radu George	SAI
	6. Elaborarea Tabelului puncte tari şi puncte slabe	8	Radu George Popescu Sorin	SAI
	7. Întocmirea Programului de audit intern	8	Radu George	SAI
	8. Întocmirea Notei şi a Programului intervenţiei la faţa locului	8	Popescu Sorin	SAI
	9. Obţinerea aprobării Notei şi a anexelor acesteia: Colectarea şi prelucrarea datelor, „Tabelul - Puncte tari şi puncte slabe“ şi Programul intervenţiei la faţa locului.	2	Popescu Sorin	SAI
	10. Planificarea şi organizarea Şedinţei de deschidere cu Departamentul IT	2	Popescu Sorin	SAI AUDITAT
	11. Redactarea Minutei şedinţei de deschidere. Obţinerea numelui persoanelor de contact şi stabilirea unui loc pentru desfăşurarea activităţii de audit.	2	Radu George	AUDITAT
2. Intervenţia la faţa locului		**272**		
Obiectivul I.	1.1 Efectuarea testărilor	22	Popescu Sorin	

OBIECTIVELE AUDITULUI	ACTIVITĂŢILE PROGRAMATE	DURATA (H)	PERSOANELE IMPLICATE	LOCUL DESFĂŞURĂRII
Strategia şi planificarea sistemelor informatice	1.2 Discutarea constatărilor cu şeful de serviciu	2		AUDITAT SAI
	1.3 Elaborare FIAP - urilor	8		
	1.4 Colectarea dovezilor	4		
	1.5 Revizuirea documentelor de lucru din punct de vedere al conţinutului şi al formei şi întocmirea Notei centralizatoare a documentelor de lucru	4		
Obiectivul II. **Organizarea şi funcţionarea departamentului IT**	2.1 Efectuarea testărilor	22	Radu George	AUDITAT SAI
	2.2 Discutarea constatărilor cu şeful de serviciu	2		
	2.3 Elaborarea FIAP - urilor	8		
	2.4 Colectarea dovezilor	4		
	2.5 Revizuirea documentelor de lucru din punct de vedere al conţinutului şi al formei şi întocmirea Notei centralizatoare a documentelor de lucru	4		
Obiectivul III. **Operaţii ale sistemului informatic**	3.1 Efectuarea testărilor	22	Popescu Sorin	AUDITAT SAI
	3.2 Discutarea constatărilor cu şeful de serviciu	2		
	3.3 Elaborarea FIAP - urilor	8		
	3.4 Colectarea dovezilor	4		
	3.5 Revizuirea documentelor de lucru din punct de vedere al conţinutului şi al formei şi întocmirea Notei centralizatoare a documentelor de lucru	4		
Obiectivul IV. **Securitatea informaţiilor**	4.1 Efectuarea testărilor	22	Radu George	AUDITAT SAI
	4.2 Discutarea constatărilor cu şeful de serviciu	2		
	4.3 Elaborarea FIAP - urilor	8		
	4.4 Colectarea dovezilor	4		
	4.5 Revizuirea documentelor de lucru din punct de vedere al conţinutului şi al formei şi întocmirea Notei centralizatoare a documentelor de lucru	4		
Obiectivul V. **Achiziţionarea şi testarea aplicaţiilor**	5.1 Efectuarea testărilor	20	Popescu Sorin	AUDITAT SAI
	5.2 Discutarea constatărilor cu şeful de serviciu	2		
	5.3 Elaborarea FIAP - urilor	8		
	5.4 Colectarea dovezilor	4		
	5.5 Revizuirea documentelor de lucru din punct de vedere al conţinutului şi al formei şi întocmirea Notei centralizatoare a documentelor de lucru	4		
Obiectivul VI. **Elaborarea şi implementarea**	6.1 Efectuarea testărilor	20	Radu George	AUDITAT
	6.2 Discutarea constatărilor cu şeful de serviciu	2		
	6.3 Elaborarea FIAP - urilor	8		

OBIECTIVELE AUDITULUI	ACTIVITĂŢILE PROGRAMATE	DURATA (H)	PERSOANELE IMPLICATE	LOCUL DESFĂŞURĂRII
proiectelor IT	6.4 Colectarea dovezilor	4		SAI
	6.5 Revizuirea documentelor de lucru din punct de vedere al conţinutului şi al formei şi întocmirea Notei centralizatoare a documentelor de lucru	4		
Obiectivul VII. **Proiectarea şi menţinerea în funcţiune a unei reţele**	6.1 Efectuarea testărilor	18	Popescu Sorin	
	6.2 Discutarea constatărilor cu şeful de serviciu	2		
	6.3 Elaborarea FIAP - urilor	8		
	6.4 Colectarea dovezilor	4		
	6.5 Revizuirea documentelor de lucru din punct de vedere al conţinutului şi al formei şi întocmirea Notei centralizatoare a documentelor de lucru	4		
	12. Planificarea si organizarea Şedinţei de închidere		Radu George	AUDITAT
	13. Discutarea constatărilor cu Departamentul IT	4	Radu George Popescu Sorin	AUDITAT
	14. Concluzii	4	Radu George	SAI
III. ***Raportul de audit intern***		**58**		
	15. Redactarea proiectului de Raport de audit intern	16	Radu George Popescu Sorin	SAI
	16. Revizuirea Raportului de audit intern	8	Radu George Popescu Sorin	SAI
	17. Obţinerea proiectului de Raport de audit intern aprobat de conducere	8	Popescu Sorin	SAI
	18. Transmiterea proiectului de Raport de audit intern la auditat şi solicitarea de răspuns în 15 zile	2	Popescu Sorin	SAI
	19. Planificarea şi organizarea Reuniunii de conciliere, dacă este cazul	4	Popescu Sorin	AUDITAT
	20. Includerea în Raportul de audit intern a aspectelor reţinute din punct de vedere al auditatului	4	Radu George Popescu Sorin	SAI
	21. Finalizarea Raportului de audit intern	4	Radu George Popescu Sorin	SAI
	22. Obţinerea Raportului de audit intern aprobat de conducerea instituţiei	8	Popescu Sorin	SAI
	23. Transmiterea recomandărilor aprobate către auditat	4	Popescu Sorin	SAI
IV. Urmărirea recomandărilor	24. Întocmirea Fisei de urmărire a recomandărilor	**4**	Popescu Sorin	SAI

Data: 08.09.2009

Auditori,
Popescu Sorin
Radu George

Şef compartiment audit intern,
Dumitru Daniel

Notă:

Programul de audit intern este documentul prin care repartizăm resursele de audit în vederea realizării misiunii de audit intern respectiv, stabilim între membri echipei de auditori activităţile pe care le vor desfăşura în vederea atingerii obiectivelor stabilite si timpul necesar pentru parcurgerea etapelor si procedurilor specifice in vederea încadrării in perioadele afectate prin Planul de audit intern.

Programul de audit este un document intern de lucru al compartimentului de audit intern, care se întocmeşte pe baza Tematicii în detaliu a misiunii de audit prin care se realizează ordinea de parcurgere a procedurilor misiunii de audit pe timpul derulării acesteia. De fapt, Programul de audit presupune un plan detaliat al activităţii ce trebuie realizat în etapa de Intervenţie la faţa locului şi care trebuie să cuprindă procedurile necesare atingerii obiectivelor misiunii de audit.

Procedura PO6 :	ELABORAREA PROGRAMULUI DE AUDIT

Entitatea Publică
Serviciul de Audit Intern

PROGRAMUL INTERVENŢIEI LA FAŢA LOCULUI

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 09.09.2009
Avizat: Dumitru Daniel Data: 09.09.2009

Nr. crt.	Obiecte audiabile	Tipul testării	Locul testării	Durata testării (h)	Nr. lista de verificare	Nr. test	Auditori
OBIECTIVUL NR. 1 – STRATEGIA ŞI PLANIFICAREA SISTEMELOR INFORMATICE							
A	**1.1. Strategia IT este concordantă cu scopurile organizaţiei**						
1	1.1.1. Strategia IT defineşte necesităţile şi priorităţile;	*Analiza sistemului de elaborarea a strategiei* *Compararea obiectivelor strategie ale IT cu cele ale organizaţiei* *Examinarea direcţiilor strategice în domeniul IT* *Analiza responsabilităţilor în elaborarea strategiei* *Analiza politicilor privind implementarea strategiei* *Analiza obiectivelor IT strategice* *Analiza managementului IT*	*Structura auditată*	*6*	*I*	*T1*	Popescu Sorin
B	**1.2. Planurile IT se adresează întregii organizaţii**						
1	1.2.2. Planurile IT ajută îndeplinirea misiunii organizaţiei	*Analiza planurilor de activitate* *Examinarea cunoaşterii obiectivelor planului de activitate* *Analiza echilibrului îndeplinirii planului de activitate cu resursele alocate* *Analiza adaptabilităţii planului la necesităţi* *Analiza corelării planului de activitate cu politica şi strategia*	*Structura auditată*	*4*	*I*	*T2*	Popescu Sorin
2	1.2.3. Planurile IT oferă asigurare cu privire la faptul că resursele IT sunt alocate în concordanţă cu necesităţile	*Analiza monitorizării obiectivelor şi direcţiilor de activitate* *Analiza implicaţiei strategiei IT asupra organizaţiei*	*Structura auditată*	*4*	*I*	*T3*	Popescu Sorin

Nr. crt.	Obiecte audiabile	Tipul testării	Locul testării	Durata testării (h)	Nr. lista de verificare	Nr. test	Auditori
C	**1.3. Obiectivele IT îndeplinesc obiectivele organizaţiei**						
1	1.3.1. Strategia IT este concordantă cu scopurile organizaţiei	*Observarea modului de cunoaştere şi implementare a strategiei* *Analiza organizării funcţionale a departamentului IT* *Analiza impactului obiectivelor strategice* *Examinarea misiunii organizaţiei în comparaţie cu scopurile strategice* *Analiza modalităţilor de implementare a strategiei* *Analiza fundamentării necesarului de resurse în fundamentarea strategiei*	*Structura auditată*	*4*	*I*	*T4*	Popescu Sorin
D	**1.4. Comitetul IT determină strategia IT**						
1	1.4.2. Comitetul IT transpune strategia în planuri pe termen scurt şi mediu	*Examinarea constituirii Comitetului de dezvoltare IT* *Examinarea atribuţiilor Comitetului IT* *Analiza responsabilităţilor Comitetului IT* *Analiza activităţilor realizate de Comitetul IT*	*Structura auditată*	*4*	*I*	*T5*	Popescu Sorin
2	1.4.3. Comitetul IT stabileşte priorităţile proiectelor între dezvoltarea sistemelor şi operaţiile realizate	*Examinarea programului de dezvoltare IT a organizaţiei* *Analiza modului de fundamentare a programului de dezvoltare IT a organizaţiei* *Analiza calitativă a echipamentelor si aplicaţiilor achiziţionate*	*Structura auditată*	*4*	*I*	*T6*	Popescu Sorin
E	**1.5. Organizarea IT corespunde necesităţilor organizaţiei**						
1	1.5.1. Organizarea adecvată a funcţiei IT	*Examinarea deciziilor IT şi transformările mediului organizaţional* *Analiza adecvării şi conformităţii procedurilor* *Analiza performanţelor activităţii IT* *Analiza competenţelor şi responsabilităţilor IT*	*Structura auditată*	*4*	*I*	*T7*	Popescu Sorin
2	1.5.3. Adecvarea practicilor şi procedurilor IT la procesele existente	*Examinarea modului de instruire a utilizatorilor* *Analiza dacă sistemele şi aplicaţiile IT acoperă nevoile şi necesităţile organizaţiei* *Examinarea adecvării practicii IT la procesele din organizaţie* *Examinarea suficienţei procedurilor în domeniul IT*		*4*	*I*		Popescu Sorin
F	**1.6. Elaborarea strategiei IT corespunde strategiei entităţii**						
1	1.6.1. Infrastructura IT a stat la baza elaborării strategiei IT	*Analiza existentei controlului asupra echipamentelor* *Examinarea realizării achiziţiilor în concordanţă cu*	*Structura auditată*	*8*	*I*	*T8*	Popescu Sorin

Nr. crt.	Obiecte audiabile	Tipul testării	Locul testării	Durata testării (h)	Nr. lista de verificare	Nr. test	Auditori
		realizarea obiectivelor strategice					
OBIECTIVUL NR. 2 – ORGANIZAREA ŞI FUNCŢIONAREA DEPARTAMENTULUI IT							
A	**2.1. Definirea atribuţiilor şi activităţilor**						
1	2.1.1. Definirea atribuţiilor şi responsabilităţilor în cadrul departamentului IT	*Analiza activităţilor stabilite* *Analiza gradului de procedurare a activităţilor* *Analiza atribuţiilor stabilite* *Compararea atribuţiilor cu aria de competenţă necesară pentru realizarea activităţilor*	*Structura auditată*	*10*	*II*	*T9*	Radu George
2	2.1.6. Definirea activităţilor în cadrul structurii organizatorice	*Examinarea stabilirii omogene a activităţilor în cadrul compartimentelor funcţionale ale departamentului IT* *Analiza acţiunilor stabilite pentru realizarea activităţilor* *Examinarea repartizării activităţilor pe compartimente în funcţie de rolul acestora*	*Structura auditată*	*10*	*II*	*T10*	Radu George
B	**2.2. Stabilirea structurii organizatorice**						
1	2.2.1. Organizarea funcţională a departamentului IT	*Analiza organigramei departamentului* *Analiza ROF-ului departamentului* *Analiza ocupării posturilor* *Analiza specializării posturilor* *Analiza dotării tehnice a posturilor* *Analiza limitelor decizionale la nivelul posturilor de conducere şi execuţie* *Analiza modului de proiectare a sistemului informaţional*	*Structura auditată*	*5*	*II*	*T11*	Radu George
2	2.2.3. Examinarea sistemului de gestionare a riscurilor generale la nivelul Departamentului IT	*Analiza politicii de gestionare a riscurilor* *Analiza modului de control şi gestiune a riscurilor* *Analiza modului de conducere a Registrului riscurilor* *Analiza nivelului decizional privind implementarea instrumentelor de control* *Analiza modului de identificare şi gestionare a riscurilor pe activităţi şi obiective* *Analiza modului revizuire a riscurilor*	*Structura auditată*	*5*	*II*	*T12*	Radu George
C	**2.3. Stabilirea responsabilităţilor**						
1	2.3.3. Definirea sarcinilor prin fişa postului	*Analiza elaborării fişei postului in raport cu cerinţele potului* *Analiza modului de delegare a activităţilor* *Analiza capacităţii titularului postului de a realiza*	*Structura auditată*	*10*	*II*	*T13*	Radu George

Nr. crt.	Obiecte audiabile	Tipul testării	Locul testării	Durata testării (h)	Nr. lista de verificare	Nr. test	Auditori
		atribuţiile alocate *Analiza stabilirii atribuţiilor în raport cu nivelul postului*					
OBIECTIVUL NR. 3 – OPERAŢII ALE SISTEMULUI INFORMATIC							
A	**3.1. Managementul operaţiunilor**						
1	3.1.2. Performanţa, capacitatea si disponibilitatea sistemelor informatice este monitorizată de operatori	*Verificarea dacă mesajele de eroare sunt abordate în conformitate cu manualele de operare* *Verificarea dacă informatizarea organizaţiei ia în considerare toate departamentele din cadrul acesteia* *Verificarea dacă este estimat timpul maxim de nefuncţionare care poate fi acceptat, şi costurile asociate acestuia.*	*Structura auditată*	*3*	*III*	*T14*	Popescu Sorin
2	3.1.3. Responsabilitatea pentru supravegherea sarcinilor pe seturi de programe revine operatorilor	*Verificarea dacă utilizatorii sunt instruiţi pentru însuşirea modului de lucru cu aplicaţiile noi* *Verificarea dacă utilizatorii primesc asistenţă în rularea aplicaţiilor* *Verificarea dacă responsabilitatea funcţionării fiecărui program este în sarcina unui administrator* *Verificarea dacă există o supraveghere permanentă în cadrul sistemului asupra derulării unui program sau aplicaţie*	*Structura auditată*	*3*	*III*	*T15*	Popescu Sorin
3	3.1.4. Elaborarea planului anual de activitate	*Verificarea dacă politica în domeniul IT se reflectă în planul anual de activitate în domeniul IT* *Examinarea dacă managerii cu responsabilităţi în monitorizarea implementării politicii IT, au fost consultaţi la elaborarea planului anual de activitate în domeniul IT* *Examinarea dacă responsabilităţile sunt clar definite pentru realizarea activităţilor IT* *Identificarea deciziilor luate în vederea elaborării şi actualizării planului şi analiza dacă acestea sunt în conformitate cu activităţile stabilite*	*Structura auditată*	*2*	*III*	*T16*	Popescu Sorin
B	**3.2. Managementul problemelor**						
1	3.2.2. Programele antivirus asigură protecţia aplicaţiilor	*Verificarea dacă există proceduri pentru protecţia împotriva viruşilor, care să specifice modul de configurare al programului antivirus* *Verificarea dacă sunt alese cele mai potrivite soluţii antivirus;* *Verificarea dacă se realizează scanarea antivirus pe*	*Structura auditată*	*4*	*III*	*T17*	Popescu Sorin

Nr. crt.	Obiecte audiabile	Tipul testării	Locul testării	Durata testării (h)	Nr. lista de verificare	Nr. test	Auditori
		servere, staţii de lucru sau poşta electronică *Verificarea configurării programului antivirus*					
2	3.2.4. Implementarea subsistemelor IT	*Analiza criteriilor avute în vedere la elaborarea subsistemelor IT pentru funcţiile principale* *Verificarea dacă departamentele nou înfiinţate au fost solicitate să-şi exprime cerinţele specifice privind realizarea unor subsisteme IT specifice activităţii lor* *Verificarea stabilirii de responsabilităţi personalului de specialitate, pe linia implementării sistemului IT* *Examinarea cunoaşterii reglementărilor specifice privind implementarea sistemului IT de către responsabilii cu realizarea acestei activităţi* *Examinarea modului de alocare a resurselor necesare realizării subsistemelor IT* *Verificarea activităţii de monitorizare a implementării subsistemelor IT*	*Structura auditată*	*4*	*III*	*T18*	Popescu Sorin
C	**3.3.** Funcţionalitatea activităţilor în cadrul departamentului IT						
1	3.3.2. Organizarea funcţională a activităţilor în cadrul departamentului IT	*Analiza dacă departamentul IT este subordonat unui nivel managerial corespunzător* *Verificarea dacă organigrama departamentului IT corespunde organizării actuale a departamentului;* *Verificarea dacă numărul de posturi existent în cadrul departamentului IT asigură realizarea activităţilor şi atribuţiilor* *Analiza dacă atribuţiile departamentului sunt definite corect şi în totalitate în cadrul ROF-ului* *Analiza modului de asigurare a continuităţii activităţilor în funcţie de pregătirea salariaţilor şi vechimea în muncă* *Analizaţi dacă pregătirea şi calificarea salariaţilor departamentului IT asigură utilizarea optimă a programelor, aplicaţiilor, echipamentelor şi dezvoltarea informaţională a entităţii*	*Structura auditată*	*4*	*III*	*T19*	Popescu Sorin
2	3.3.6. Asigurarea caracterului secret al datelor	*Verificarea dacă aplicaţiile respectă schemele privind nivele de secretizare în conformitate cu standardele organizaţiei;* *Verificarea dacă secretizarea informaţiilor ia în considerare impactul pierderii confidenţialităţii, integrităţii sau disponibilităţilor informaţiei asupra activităţii*	*Structura auditată*	*4*	*III*	*T20*	Popescu Sorin

Nr. crt.	Obiecte audiabile	Tipul testării	Locul testării	Durata testării (h)	Nr. lista de verificare	Nr. test	Auditori
		Verificarea dacă monitorizarea sistemelor se concentrează pe punctele vulnerabile *Verificarea dacă sunt înregistrate toate evenimentele cheie în cadrul unui sistem*					
D	**3.4.** Mentenanţa echipamentelor						
1	3.4.2. Întreţinerea calculatorului şi a echipamentelor	*Verificarea dacă operaţiunile de mentenanţă se efectuează conform planificării, folosindu-se procedurile standard de testare* *Verificarea dacă disfuncţionalităţile hardware sunt identificate corect şi în timp util şi sunt înlăturate în conformitate cu instrucţiunile şi manualele de întreţinere* *Verificarea dacă produsele software sunt instalate şi configurate conform documentaţiilor şi indicaţiilor furnizorilor* *Verificaţi dacă corecţia erorilor se realizează în limita competenţelor*	*Structura auditată*	*4*	*III*	*T21*	Popescu Sorin
2	3.4.3. Instalarea şi configurarea calculatorului	*Verificarea dacă sursele de alimentare sunt alese şi verificate în conformitate cu cerinţele tehnice;* *Verificarea dacă sistemul de operare, componentele software, componentele de acces în reţea sunt instalate şi configurate corect;* *Verificarea dacă partajarea resurselor se face verificând tipul de acces permis utilizatorilor;*	*Structura auditată*	*4*	*III*	*T22*	Popescu Sorin
E	**3.5. Utilizarea echipamentelor**						
1	3.5.1. Realizarea eficientă a operaţiilor în cadrul departamentului IT	*Verificarea dacă este analizat impactul produs de funcţionarea incorectă a unei operaţii asupra întregului sistem;* *Verificarea dacă operaţiile IT sunt realizate într-o manieră eficientă, în timp util şi la intervale bine stabilite* *Identificarea proceselor care utilizează o cantitate mai mare de resurse şi alocarea optimă a acestora.*	*Structura auditată*	*3*	*III*	*T23*	Popescu Sorin
2	3.5.3. Administrarea eficientă a aplicaţiilor şi programelor	*Verificarea dacă se utilizează funcţii de verificare prin totaluri, chei şi algoritmi;* *Verificarea dacă utilizatorii finali pot obţine rapoarte diverse fără a afecta tranzacţiile curente;* *Verificaţi dacă utilizatorilor li se acordă suport tehnic corespunzător pentru aplicaţiile existente;*	*Structura auditată*	*2*	*III*	*T24*	Popescu Sorin

Nr. crt.	Obiecte audiabile	Tipul testării	Locul testării	Durata testării (h)	Nr. lista de verificare	Nr. test	Auditori
		Verificaţi dacă administrarea aplicaţiilor se realizează de către administratori autorizaţi, care au ca atribuţii protejarea aplicaţiilor împotriva distrugerilor, a accesului neautorizat sau utilizării incorecte.					
3	3.5.4. Evaluarea problemelor şi soluţionarea acestora	*Verificarea modului de prevenire şi rezolvare a incidentelor care afectează funcţionarea normală a serviciilor IT;* *Verificarea dacă măsurile de corectare a erorilor asigură prevenirea reapariţiei acestora;* *Verificarea respectării etapelor în soluţionarea unei probleme.*	*Structura auditată*	*3*	*III*	*T25*	Popescu Sorin
OBIECTIVUL NR. 4 – SECURITATEA INFORMAŢIILOR							
A	**4.1. Organizarea securităţii informaţiilor**						
1	4.1.4. Elaborarea politicii privind securitatea informaţiei	*Verificarea dacă politica privind securitatea informaţiei stabileşte responsabilităţile asociate şi principiile de securitate care trebuie urmate de către personal;* *Verificarea dacă politica de securitate a informaţiei supune informaţiile şi sistemele importante unei analize de risc în mod regulat;* *Verificarea dacă politica de securitate este revizuită periodic şi dacă este concordantă cu cultura organizaţiei.*	*Structura auditată*	*3*	*IV*	*T26*	Radu George
2	4.1.5. Stabilirea responsabilităţilor în cadrul politicii de securitate	*Verificarea dacă există un comitet însărcinat cu coordonarea activităţii de securitate a informaţiei;* *Verificaţi dacă comitetul însărcinat cu coordonarea activităţii de securitate a informaţiei este responsabil pentru integrarea informaţiei pentru toate sectoarele organizaţiei;* *Verificaţi dacă comitetul însărcinat cu coordonarea activităţii de securitate a informaţiei asigură coordonarea implementării instrumentelor de control aferente securităţii informaţiei.*	*Structura auditată*	*3*	*IV*	*T27*	Radu George
3	4.1.7. Securitatea datelor asigură disponibilitatea acestora doar pentru utilizatori autorizaţi	*Verificarea dacă dispozitivele de stocare sunt păstrate în condiţii de securitate pentru a evita distrugerea fizică, pierderea sau modificarea conţinutului;* *Verificarea dacă salvările de date sunt efectuate cu periodicitatea impusă de importanţa datelor şi de regulile prestabilite;*	*Structura auditată*	*2*	*IV*	*T28*	Radu George

Nr. crt.	Obiecte audiabile	Tipul testării	Locul testării	Durata testării (h)	Nr. lista de verificare	Nr. test	Auditori
		Verificarea dacă permisiunile curente de acces la resursele partajate sunt verificate, în vederea conformităţii cu regulile de securitate impuse.					
B	**4.2. Disponibilitatea datelor**						
1	4.2.2. Protejarea datelor împotriva viruşilor	*Verificarea dacă actualizarea produselor antivirus se realizează cu regularitate;* *Verificarea dacă programele anti-virus sunt adecvate necesităţilor utilizatorilor staţiilor de lucru* *Verificaţi dacă este realizată o monitorizarea sistematică a funcţionalităţii programelor anti-virus.*	*Structura auditată*	*2*	*IV*	*T29*	Radu George
2	4.2.3. Asigurarea continuităţii activităţilor	*Verificarea dacă resursele umane, precum şi cele hardware/software implicate în procesul de aplicare a planului de asigurare a continuităţii sunt prestabilite şi sunt disponibile;* *Verificarea dacă planul privind asigurarea continuităţii activităţilor stabileşte criteriile şi procedurile de recunoaştere a unei crize;* *Verificarea dacă planul defineşte procedurile tehnice de reluare sau continuare a proceselor critice;* *Verificarea dacă echipa de intervenţie în caz de dezastru este implicată în conceperea planului privind continuitatea activităţilor;* *Verificarea dacă planurile privind continuitatea activităţilor sunt conforme cu obiectivele generale şi cu strategia de administrare a riscurilor.*	*Structura auditată*	*2*	*IV*	*T30*	Radu George
3	4.2.4. Recuperarea datelor în caz de dezastru	*Verificarea modului de elaborare a planului de recuperare a datelor în caz de dezastru;* *Verificarea responsabilităţilor echipa însărcinate cu implementarea planului;* *Analiza modului de testare şi modificare periodică a planului;* *Verificarea modului de creare a salvărilor de siguranţă;* *Stabilirea dacă locaţia în care sunt stocate datele pentru a fi recuperate în caz de dezastru este adecvată.*	*Structura auditată*	*2*	*IV*	*T30*	Radu George
C	**4.3.** Asigurarea funcţionării programelor şi aplicaţiilor						
1	4.3.1. Asigurarea introducerii corecte a datelor şi	*Verificarea procedurilor de introducere a datelor;* *Verificarea monitorizării prelucrării electronice a datelor;*	*Structura auditată*	*3*	*IV*	*T31*	Radu George

Nr. crt.	Obiecte audiabile	Tipul testării	Locul testării	Durata testării (h)	Nr. lista de verificare	Nr. test	Auditori
	informaţiilor pentru prelucrare	*Verificarea rapoartelor de erori înregistrate de sistemul informatic şi a modului de efectuare a testelor pentru identificarea cauzelor apariţiei acestora;* *Verificarea modului de întocmire a jurnalului intervenţiilor operatorilor, jurnalul utilizării bibliotecii de programe şi a arhivelor de date şi aplicaţii;* *Verificarea conformităţii datelor introduse cu documentele primare.*					
2	4.3.3. Prelucrarea datelor	*Verificarea modului de depistare şi corectare a erorilor apărute în timpul rulărilor aplicaţiilor informatice;* *Verificarea modului de funcţionare a programelor, folosind ca date de test fie înregistrări originale, fie înregistrări mostră şi corectarea eventualelor erori apărute în procesul de introducere a datelor;* *Verificarea în mod regulat a drepturilor de acces*	*Structura auditată*	*3*	*IV*	*T32*	Radu George
3	4.3.4. Asigurarea securităţii datelor şi documentelor	*Verificarea modului de realizare a copiilor de siguranţă pe suporturi de stocare adecvate;* *Verificarea condiţiilor de păstrare a datelor şi documentelor;* *Verificarea dacă accesul utilizatorilor la echipamente şi la suporturi de date este realizat numai în limita permisiunilor cerute de efectuarea sarcinilor curente;* *Verificarea dacă regulile de securitate referitoare la accesul la echipamente sunt respectate;* *Definirea şi comunicarea corespunzătoare a descrierilor şi responsabilităţilor posturilor în raport cu securitatea informaţiei.*	*Structura auditată*	*4*	*IV*	*T33*	Radu George
D	**4.4.** Implementarea instrumentelor de control						
1	4.4.1. Accesul la aplicaţie este oferit pe baza necesităţilor utilizatorului	*Verificarea dacă drepturile de acces sunt acordate conform regulilor specifice;* *Verificarea dacă responsabilitatea pentru administrarea şi operarea aplicaţiei este definită clar;* *Verificarea dacă utilizatorii sunt instruiţi cu privire la utilizarea reţelei şi securitatea acesteia;* *Verificarea dacă activitatea în reţea este monitorizată, asigurându-se că securitatea acesteia este adecvată;* *Verificarea proiectării reţelelor astfel încât să asigure eficienţa traficului de date.*	*Structura auditată*	*4*	*IV*	*T34*	Radu George
2	4.4.3. Introducerea	*Verificarea restricţiilor asupra accesului fizic la sistemele*	*Structura*	*2*	*IV*	*T35*	Radu

Nr. crt.	Obiecte audiabile	Tipul testării	Locul testării	Durata testării (h)	Nr. lista de verificare	Nr. test	Auditori
	instrumentelor de control fizic asupra echipamentelor IT	*de calculatoare;* *Verificarea dacă echipamentele şi documentaţia de importanţă critică sunt asigurate suplimentar;* *Verificarea modului de supraveghere a camerelor în care sunt adăpostite echipamente şi facilităţi critice;* *Verificaţi dacă măsurile de protecţie sunt în acord cu politica de securitate a organizaţiei.*	*auditată*				George
E	**4.5.** Securitatea reţelei						
1	4.5.2. Monitorizarea securităţii reţelelor	*Verificarea existenţei unui program de management al vulnerabilităţilor reţelei;* *Verificarea grupării şi clasificării dispozitivelor din reţea în funcţie de priorităţi, de la sisteme de importanţă redusă la sisteme de importanţă vitală;* *Verificarea dacă expunerea la risc este monitorizată prin reprezentarea stării de ansamblu a reţelei;* *Verificarea dacă panoul de afişare privind expunerea la risc este actualizat permanent;* *Verificarea dacă este urmărită permanent reducerea timpilor necesari pentru identificarea, remedierea şi validarea soluţiilor aplicate.*	*Structura auditată*	*2*	*IV*	*T36*	Radu George
F	**4.6. Gestionarea parolelor**						
1	4.61. Utilizatorii au parole de acces individuale	*Verificarea dacă programele şi aplicaţiile au nivele de acces în funcţie de nivelul postului;* *Verificaţi dacă parolele sunt schimbate periodic, respectând regulile de complexitate impuse.*	*Structura auditată*	*2*	*IV*	*T37*	Radu George
2	4.6.2. Schimbarea periodică a parolelor	*Verificarea dacă permisiunile sau drepturile utilizatorilor sunt verificate periodic, pentru a corespunde strict sarcinilor acestora;* *Verificarea dacă administratorul sistemului creează şi configurează corespunzător conturile fiecărui utilizator;* *Verificarea dacă parolele generice iniţiale sunt schimbate de către fiecare utilizator în parte.*	*Structura auditată*	*2*	*IV*	*T38*	Radu George
3	4.6.4. Persoanele autorizate au acces la sistemul de operare	*Verificarea dacă accesul la sistem se realizează numai pe baza conturilor de utilizatori în funcţie de tipurile specifice şi de atribuţiile specifice fiecărui angajat;* *Verificarea modului de instruire a utilizatorilor în legătură cu regulile de securitate logică.*	*Structura auditată*	*2*	*IV*	*T39*	Radu George
G	**4.7. Securitatea logică**						

Nr. crt.	Obiecte audiabile	Tipul testării	Locul testării	Durata testării (h)	Nr. lista de verificare	Nr. test	Auditori
1	4.7.1. Asigurarea securităţii funcţionării programelor şi aplicaţiilor	*Verificarea modului de identificare a ameninţărilor aferente sistemelor informatice;* *Verificarea protecţiilor în cazul accesului de la distanţă;* *Verificarea modului de utilizare a algoritmilor de criptare a datelor;* *Verificarea modului de administrare a securităţii sistemelor de către persoane specializate;*	*Structura auditată*	*2*	*IV*	*T40*	Radu George
OBIECTIVUL NR. 5 – PROIECTAREA ŞI TESTAREA PROGRAMELOR ŞI APLICAŢIILOR							
A	**5.1.** Proiectarea şi elaborarea programelor şi aplicaţiilor						
1	5.1.1. Proiectarea programului informatic	Verificarea procedurilor utilizate în proiectarea programelor, din punct de vedere al corectitudinii şi completitudinii prelucrările care se vor efectua asupra datelor; Verificarea dacă instrumentele de dezvoltare a programului/aplicaţiei sunt stabilite cu respectarea specificaţiilor; Verificarea dacă pentru fiecare aplicaţie în parte sunt stabilite următoarele: numărul de utilizatori, rolurile acestora, privilegiile şi restricţiile aplicabile fiecărui rol in parte, accesul restricţionat; Verificarea dacă proiectarea aplicaţiei este monitorizată; Verificarea dacă versiunile aplicaţiilor instalate ulterior sunt compatibile şi utilizează toate resursele versiunilor anterioare; Verificarea dacă comunicarea cu echipa de specialişti este permanentă pe timpul proiectării şi utilizării aplicaţiei.	*Structura auditată*	*10*	*V*	*T41*	Popescu Sorin
2	5.1.2. Elaborarea programului informatic	*Verificarea algoritmului programului/aplicaţiei din punct de vedere al conformităţii cu logica operaţiilor;* *Verificarea dacă algoritmul respectă cerinţele de integrare ale aplicaţiei;* *Verificarea performanţei soluţiilor de programare;* *Verificarea integrării componentelor unui program în funcţie de cerinţele utilizatorilor.*	*Structura auditată*	*10*	*V*	*T42*	Popescu Sorin
B	**5.2.** Testarea şi implementarea programelor şi aplicaţiilor						
1	5.2.2. Testarea programului şi aplicaţiei	*Verificarea dacă datele de test sunt definite corespunzător prelucrărilor programului pe toate ramurile acestuia;* *Evaluarea rezultatelor testării în funcţie de documentaţia programului/aplicaţiei;*	*Structura auditată*	*10*	*V*	*T43*	Popescu Sorin

Nr. crt.	Obiecte audiabile	Tipul testării	Locul testării	Durata testării (h)	Nr. lista de verificare	Nr. test	Auditori
		Verificarea conformităţii datelor de testare cu manualele de operare şi utilizare; *Verificarea dacă simulările se realizează conform manualului de utilizare.*					
2	5.2.3. Asigurarea corectitudinii rezultatelor	*Verificarea dacă opţiunile şi parametrii de lucru ai programului/aplicaţiei sunt stabiliţi conform specificaţiilor din documentaţii;* *Verificarea condiţiilor de funcţionare a programului/aplicaţiei, în funcţie de solicitările utilizatorului;* *Verificarea opţiunilor şi a parametrilor de operare ai programului/aplicaţiei, în funcţie de specificaţiilor din documentaţii;* *Analiza modului de însuşire de către utilizatori a specificaţiilor programului/aplicaţiei.*	*Structura auditată*	*10*	*V*	*T44*	Popescu Sorin
OBIECTIV NR. 6 ELABORAREA ŞI IMPLEMENTAREA PROIECTELOR IT							
A	**6.1.** Dezvoltarea proiectelor IT (programe şi aplicaţii)						
1	6.1.2. Iniţierea şi elaborarea proiectelor IT	*Verificarea oportunităţii soluţiile propuse pentru implementarea proiectelor IT;* *Verificarea compatibilităţii proiectului cu proiectele aflate în derulare;* *Verificarea necesităţii asistenţei tehnice;* *Verificarea competitivităţii proiectelor.*	*Structura auditată*	*10*	*VI*	*T45*	Radu George
2	6.1.3. Monitorizarea performanţelor soluţiilor IT implementate	*Verificarea parametrilor de referinţă şi a valorilor etalon ale programelor elaborate;* *Verificarea regulilor şi procedurilor stabilite pentru supravegherea şi colectarea valorilor parametrilor de referinţă;* *Analiza rapoartelor privind implementarea proiectelor IT propuse din punct de vedere al rigurozităţii.*	*Structura auditată*	*10*	*VI*	*T46*	Radu George
B	**6.2.** Implementarea şi funcţionarea programelor şi aplicaţiilor						
1	6.2.1. Reproiectarea soluţiilor IT pentru programe şi aplicaţii	*Verificarea modului de identificare a punctelor slabe şi a limitărilor unui program/aplicaţie;* *Verificarea dacă documentaţia cu fluxul de date şi prelucrările necesare este elaborată adecvat situaţiei reale;* *Verificarea dacă soluţiile IT sunt proiectate pornind de la punctele slabe, critice detectate, de la evoluţiile tehnologice*	*Structura auditată*	*10*	*VI*	*T47*	Radu George

Nr. crt.	Obiecte audiabile	Tipul testării	Locul testării	Durata testării (h)	Nr. lista de verificare	Nr. test	Auditori
		existente şi cele prefigurate de dezvoltare a entităţii.					
2	6.2.3. Întreţinerea aplicaţiilor garantează funcţionarea proceselor la parametrii optimi	*Verificarea monitorizării mesajelor de eroare;* *Verificarea dacă sistemele de operare şi aplicaţiile sunt instalate, actualizate sau configurate corespunzător, folosind proceduri standardizate;* *Verificarea dacă utilizatorii beneficiază permanent de asistenţă tehnică;* *Verificarea modului de întreţinere a aplicaţiilor şi dacă asigură funcţionarea proceselor.*	*Structura auditată*	*10*	*VI*	*T48*	Radu George
OBIECTIV NR. 7 PROIECTAREA ŞI MENŢINEREA ÎN FUNCŢIUNE A UNEI REŢELE							
A	**7.1.** Proiectarea, instalarea şi administrarea reţelei de calculatoare						
1	7.1.1. Asigurarea bunei funcţionări a sistemelor bazate pe existenţa şi funcţionarea reţelei de calculatoare	*Verificarea dacă echipamentele din reţea sunt administrate centralizat;* *Verificarea dacă configurarea reţelei, conectarea componentelor în reţea, distribuirea serviciilor contribuie la creşterea productivităţii muncii în organizaţie;* *Verificarea dacă serverele şi staţiile client sunt amplasate în reţea şi configurate conform regulilor impuse prin strategia de securitate;* *Verificarea dacă regulile stabilite şi implementate asigură accesul controlat şi sigur al utilizatorilor numai la acele resurse de care au nevoie pentru îndeplinirea sarcinilor de serviciu conform fişei postului.*	*Structura auditată*	*10*	*VII*	*T49*	Radu George
2	7.1.3. Administrarea serverelor	*Verificarea dacă accesul şi utilizarea resurselor serverului respectă strategia de securitate a reţelei;* *Verificarea dacă permisiunea de administrare a unui program este acordată numai personalului calificat;* *Verificaţi dacă jurnalele identifică utilizatorii care au avut acces la program, în limita permisiunilor ce le-au fost acordate.*	*Structura auditată*	*10*	*VII*	*T50*	Radu George
B	**7.2.** Interconectarea şi securitatea reţelei						
1	7.2.1. Interconectarea reţelelor	*Verificarea dacă conexiunile dintre reţele sunt conforme cu arhitectura generală şi respectă standardele de interconectare;* *Verificarea dacă componentele hardware şi software ale echipamentelor de legătură sunt configurate respectând regulile de securitate a transmisiilor de date din strategia de securitate a organizaţiei;*	*Structura auditată*	*10*	*VII*	*T51*	Radu George

Nr. crt.	Obiecte audiabile	Tipul testării	Locul testării	Durata testării (h)	Nr. lista de verificare	Nr. test	Auditori
		Verificarea dacă tabelele de rutare sunt corect configurate şi indică adresele reţelelor accesibile.					
2	7.2.2. Proiectarea şi asigurarea securităţii reţelei	*Verificarea dacă vulnerabilităţile şi ameninţările sunt corect identificate şi prioritizate;* *Verificarea dacă procedurile de securitate ce trebuie implementate sunt aduse operativ la cunoştinţa personalului;* *Analiza siguranţei accesului la reţea şi a comunicării datelor în reţea.* *Analiza rapoartelor de monitorizare a traficului datelor în reţea.*	*Structura auditată*	*10*	*VII*	*T52*	Radu George

Data: 09.09.2009

Auditori,
Popescu Sorin
Radu George

Notă:

Programul de intervenţie la faţa locului sau ***Programul preliminar*** se elaborează pe baza *Programului de audit* şi prezintă detaliat lucrările pe care auditorii interni îşi propun să le efectueze, tipurile de teste şi eşantioanele pe baza cărora se vor realiza acestea, locul şi durata testării.

În practica, se recomandă realizarea unui grad mai mare de detaliere a testărilor, care se vor efectua în etapa de *Intervenţie la faţa locului***,** prin completarea *Programului preliminar* cu modalităţile concrete de determinare a eşantioanelor, în conformitate cu regulile statisticii, dar şi prin diversificarea tipurilor testărilor ce se vor realiza de către auditorii interni.

ENTITATEA PUBLICA
Serviciul Audit Intern

MINUTA ŞEDINŢEI DE DESCHIDERE

Misiunea de audit: Tehnologia informaţiei
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 10.09.2009
Avizat: Dumitru Daniel Data: 10.09.2009

A. Lista participanţilor:

Numele	Funcţia	Direcţia/ Serviciul	Nr. telefon	E-mail	Semnătura
Dumitru Daniel	Coordonator	CAPI			
Popescu Sorin	Auditor	SAPI			
Radu George	Auditor	SAPI			
Pătrulescu George	Director	DIT			
Voiculescu Alin	Sef	STDAM			
Boerescu Ilie	Sef	SCD			
Teodorescu Rodica	Sef	SEE			
Eleodor Darius	Sef	SAPP			
Iordache Camelia	Sef	SRC			
Păun Elena	Sef	SSD			
Badea Ştefan	Sef	SAT			

B. Stenograma şedinţei

În cadrul şedinţei de deschidere s-a procedat la:

- prezentarea echipei de auditori care urmează să efectueze misiunea de audit;
- prezentarea funcţiei de audit intern de către şeful Serviciului Audit Public Intern, în special a obiectivelor generale ale auditului intern şi semnificaţia auditului intern;
- Prezentarea *Programului intervenţiei la faţa locului*, obiectivele auditabile care se intenţionează a fi realizate, după analizele de risc efectuate. A fost cerută părerea audiaţilor cu privire la aceste obiective, unde s-au făcut remarci că acestea în general reprezintă zone cu risc, dar s-au făcut şi unele comentarii cu privire la complexitatea activităţii Direcţiei IT; resursele umane insuficiente şi neatractivitatea nivelului salariului pentru atragerea unor specialişti; fluctuaţia mare a personalului implicat in activitatea IT.

De asemenea, s-au stabilit:

- persoanele pe care auditorii le pot contacta în vederea colectării informaţiilor, modul de efectuare a testelor, chestionarelor şi interviurilor, programul întâlnirilor şi timpul necesar pentru realizarea acestor proceduri;
- condiţiile minime pe care auditatul trebuie să le asigure în vederea realizării misiunii de audit (spaţiu de lucru, calculatoare, posibilitate de editare etc.)

- aspectele procedurale, respectiv eventualitatea unor şedinţe intermediare în cursul misiunii, informarea sistematică asupra constatărilor;

- data şedinţei de închidere, inclusiv a participanţilor;

- convenirea unor aspecte procedurale, respectiv eventualitatea unor şedinţe intermediare în cursul auditului, informarea sistematică asupra constatărilor.

- stabilirea modalităţii de redactare a Raportului de audit intern (când, cum şi cui va fi distribuit). Recomandările formulate, ca urmare a eventualelor disfuncţionalităţi constatate, vor fi discutate şi analizate cu structura auditată, inclusiv calendarul implementării şi persoanele răspunzătoare cu implementarea recomandărilor.

ENTITATEA PUBLICĂ
Serviciul Audit Intern

LISTA DE VERIFICARE nr. 1

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 13.09.2009
Avizat: Dumitru Daniel Data: 13.09.2009

Obiectivul I.

STRATEGIA ŞI PLANIFICAREA SISTEMELOR INFORMATICE

Nr. crt.	Activitatea de audit	Da	Nu	Observaţii
1.	***Examinarea procedurilor privind planul strategic***			
1.1.	Examinarea procedurilor privind definirea şi elaborarea strategiei	X		
1.2.	Verificaţi dacă procedurile sunt aprobate de către persoanele competente;	X		
1.3.	Verificaţi dacă sunt stabilite posturile de lucru responsabile de elaborarea strategiei;	X		
1.4.	Verificaţi dacă sunt stabilite competentele în elaborarea procedurilor;	X		
1.5.	Verificaţi dacă se realizează actualizarea sistematică a procedurilor;	X		
1.6.	Verificaţi dacă sunt înglobate activităţi de control intern în punctele cheie ale proceselor;	X		
1.7.	Verificaţi dacă se respectă principiul dublei semnături;	X		
1.8.	Verificaţi dacă procedurile sunt cunoscute şi aplicate;	X		
A	**Strategia IT este concordantă cu scopurile organizaţiei**			
1.	**Strategia IT defineşte necesităţile şi priorităţile**			
1.1	Examinarea dacă există strategie elaborată la nivelul structurii funcţionale;	X		
1.2.	Analiza sistemului de fundamentare a strategiei	X		
1.3	Analiza corelării strategiei cu planurile anuale	X		
1.4.	Examinarea priorităţilor strategice in domeniul IT în corelare cu direcţiile de dezvoltare;	X		
1.5.	Verificarea dacă strategia elaborată la nivelul structurii funcţionale este în concordanţă cu strategia organizaţiei;	X		
1.6.	Verificarea dacă strategia elaborată la nivelul structurii funcţionale a avut în vedere:	X		Test nr. 1.2. Nota de relaţii 1.1. Interviu nr. 1.1. FIAP nr. 1.2.
	a. evaluarea situaţiei actuale pe baza analizei diagnostic;			
	b. identificarea punctelor tari şi a punctelor slabe ale entităţii;			
	c. formularea misiunii structurii organizatorice;			
	d. fundamentarea variantelor strategice;			
	e. identificarea şi provenienţa resurselor;			
	f. implementarea strategiei ;			
1.7.	Analiza dacă identificarea punctelor tari şi a punctelor slabe s-a realizat pe baza analizei ameninţărilor şi oportunităţilor;	X		
1.8.	Verificarea dacă strategia definită la nivelul structurii funcţionale defineşte clar obiectivele;	X		
1.9.	Analizaţi dacă direcţiile de activitate din cadrul strategiei sunt monitorizate şi evaluate, respectiv:		X	
	a) există concordanţă cu strategia elaborată la nivelul entităţii;			

	b) responsabilităţile stabilite Comisiei de dezvoltare IT conduc la implementarea IT şi asigură o decizie eficientă			Test nr. 1.1 FIAP nr. 1.1
	c) analiza proceselor verbale ale Comisiei numită la nivelul entităţii în domeniul dezvoltării IT şi urmărirea dacă politica de dezvoltare IT are ca obiectiv implementarea strategiei entităţii cu privire la domeniul IT;			
	d) urmărirea dacă toate activităţile de implementare a strategiei sunt monitorizate şi evaluate;			
1.10.	Stabilirea obiectivelor strategice a ţinut cont de mediul intern şi de mediul extern			Test nr.. 1.3. Interviu nr. 1.2. Notă de relaţii nr. 1.2. FIAP nr. 1.3.
1.11.	Obiectivele definite în cadrul strategiei asigură:			
	a) definirea realistă a acestora;			
	b) asigurarea factorului de mobilizare			
	c) definirea lor astfel încât să fie înţelese de către salariaţi			
	d) definirea lor în formă stimulatoare			
	e) asigurarea necesarului de resurse în vederea implementării obiectivelor			
1.12.	Obiectivele generale sunt definite în termeni de impact		X	
1.13.	Obiectivele generale derivă din obiectivele strategice			
1.14.	Obiectivele generale acoperă strategia definită în cadrul domeniului de activitate			
1.15.	Obiectivele generale în domeniul resurselor umane oferă direcţia şi ţinta finală ce urmează a fi atinsă			
1.16.	Obiectivele sunt formulate de o manieră precisă, riguroasă fără interpretări			
1.17.	Verificarea dacă strategia dezvoltă funcţiile esenţiale ale structurii funcţionale;	X		
1.18.	Verificarea dacă există persoană responsabilă cu actualizarea strategiei;	X		
1.19.	Analiza dacă la elaborarea strategiei s-a urmărit:			
	a. definirea obiectivelor strategice în consens cu direcţiile de acţiune ale organizaţiei			
	b. dezvoltarea strategiei este asigurată pe baza unui management funcţional	X		
	c. analiza domeniului de activitate şi definirea mandatului şi misiunii structurii organizaţionale			
	d. definirea şi analiza tuturor domeniilor şi activităţilor specifice			
1.20.	Verificarea dacă există planul de activitate pentru implementarea strategiei;	X		
1.21.	Analiza politicilor entităţii publice în domeniul IT şi stabilirea dacă asigură atingerea obiectivelor entităţii publice	X		
1.22.	Verificarea dacă politicile entităţii publice în domeniul IT se reflectă în planul strategic şi în planurile anuale	X		
1.23.	Examinarea dacă managerii cu responsabilităţi în monitorizarea implementării politicilor IT, au fost consultaţi la elaborarea planului strategic	X		
1.24.	Analiza activităţii de actualizare a planului strategic	X		
B.	**Planurile IT se adresează întregii organizaţii**			
1.	**Planurile IT ajută la îndeplinirea misiunii organizaţiei**			
1.1.	Verificarea dacă exista planuri de activitate elaborate la nivelul departamentului IT	X		
1.2.	Examinarea dacă planurile de activitate sunt elaborate anual	X		
1.3.	Verificarea dacă obiectivele sunt clar definite în cadrul planurilor	X		
1.4.	Verificarea dacă planul de activitate anual este comunicat şi cunoscut de personalul implicat în realizarea acestuia;	X		Test nr. 1.4. Interviu nr. 1.3. FIAP nr. 1.4.
1.5.	Analiza dacă planul este fundamentat, iar resursele necesare implementării acestuia sunt dimensionate corect;	X		
1.6.	Examinarea dacă la realizarea activităţilor planificate sunt asigurate competenţele necesare;	X		
1.7.	Verificarea dacă salariaţii cunosc metodologia de realizare şi de implementare a activităţilor planificate;	X		

1.8.	Verificarea dacă planul de activitate este alcătuit în concordanţă cu bugetul anual de venituri şi cheltuieli;	X		
1.9.	Analiza dacă pentru realizarea planului anual de activitate managementul a luat în considerare şi cunoaşterea nevoilor salariaţilor;	X		
1.10.	Verificarea dacă planul anual de activitate corelează obiectivele individuale cu cele organizaţionale;	X		
1.11.	Examinarea dacă planul anual de activitate permite încadrarea în resursele financiare planificate;	X		
1.12.	Examinarea dacă managementul organizaţiei acţionează consecvent pentru implementarea planului de activitate;	X		
1.13.	Analiza dacă managementul a elaborat strategii, politici, programe etc. pentru orientarea unitară a activităţii organizaţiei în vederea realizării scopurilor fundamentale;	X		
1.14.	Verificarea dacă planurile de activitate sunt adaptate la condiţiile externe organizaţiei;	X		
1.15	Identificarea proiectelor în derulare şi examinarea planurilor de proiecte în raport cu Standardele IT aprobate pentru gestionarea proiectului.	X		
1.16.	Analizaţi dacă planul aprobat este în conformitate cu politicile entităţii publice în domeniul IT;	X		
1.17.	Analiza dacă elaborarea planurilor de activitate au avut în vedere:			
	a) cunoaşterea de către salariaţi;			
	b) motivarea salariaţilor şi cointeresarea lor în realizarea obiectivelor;			
	c) necesarul de resurse este fundamentat şi dimensionat potrivit necesităţilor;			Test nr. 1.4. Interviu nr. 1.3. FIAP nr. 1.4.
	d) realizarea obiectivelor planurilor sunt asigurate competenţele necesare;			
	e) metodologia de implementare este cunoscută;			
	f) bugetele de venituri şi cheltuieli;			
1.18	Verificarea dacă planul anual de activitate ia în considerare necesităţile salariaţilor;		X	
1.19.	Evaluarea dacă planul anual de activitate corelează obiectivele departamentului IT cu obiectivele individuale ale salariaţilor;			
1.20.	Examinarea dacă realizarea planului se încadrează în limitele resurselor financiare alocate;			
1.21.	Analiza dacă tendinţele viitoare de dezvoltare sunt luate în calcul la elaborarea planurilor de activitate			
1.22.	Analizaţi realizarea subsistemelor IT pentru funcţiile principale din cadrul entităţii publice;	X		
2.	**Planurile IT oferă asigurare cu privire la faptul că resursele IT sunt alocate în concordanţă cu necesităţile**			
2.1.	Examinarea dacă proiectele sunt monitorizate permanent, urmărindu-se dacă sunt realizate în termen, în vederea sincronizării realizării obiectivelor strategice;	X		
2.2.	Examinarea procesului-verbal al grupului de strategie pentru a se garanta examinarea şi luarea de măsuri cu privire la îndeplinirea obiectivelor;	X		
2.3.	Obţinerea de exemplare ale unor analize referitoare la proiectele IT care au fost realizate, pentru a se garanta că sunt luate în considerare de grupul de strategie şi de conducerea superioară.	X		
2.4.	Obţinerea unui exemplar al documentului de politică strategică şi identificarea principalelor obiective;	X		
2.5.	Verificarea dacă strategia IT ia în considerare obiectivele de afaceri în totalitate şi sprijină atingerea acestora.	X		
2.6.	Verificarea dacă strategia IT ia în considerare organigrama organizaţiei, pentru a se asigura că toate departamentele au fost luate în considerare la elaborarea strategiei;	X		
2.7.	Examinarea dacă subsistemele IT acoperă în totalitate nevoile pentru funcţiile principale ale entităţii			
2.8.	Analiza dacă nevoile de subsisteme IT pentru funcţiile principale nou create au fost acoperite		X	Test nr. 1.5. Interviu nr. 1.4. FIAP nr. 1.5.
2.9.	Verificarea dacă departamentele înfiinţate ca urmare a funcţiilor principale nou create au fost solicitate să-şi exprime cerinţele specifice privind realizarea unor subsisteme IT proprii activităţii lor			
2.10.	Analiza procedurilor pe baza cărora se realizează subsistemele IT şi			

	stabilirea dacă acestea sunt suficiente pentru implementarea acestor subsisteme în condiţii optime			
2.11.	Verificaţi dacă strategia IT este distribuită tuturor părţilor interesate.	X		
2.12.	Examinaţi dacă angajaţii şi conducerea superioară au cunoştinţă de conţinutul strategiei şi de implicaţiile acesteia pentru dezvoltarea IT în domeniul lor de activitate.	X		
C.	**Obiectivele IT îndeplinesc obiectivele organizaţiei**			
1.	**Strategia IT este concordantă cu scopurile organizaţiei**			
1.1.	Analiza Planului strategic în domeniul IT în raport cu obiectivele strategice stabilite pentru domeniul IT;	X		
1.2.	Verificaţi dacă planului strategic şi documentele de politică strategică sunt cunoscute de către părţile interesate şi implicate în implementarea lui;	X		
1.3.	Examinaţi dacă dezvoltarea IT este asigurată prin obiectivele strategice;	X		
1.4.	Examinarea concordanţei dintre direcţiile de dezvoltare stabilite prin Planul strategic în domeniul IT şi organizarea funcţională actuală a departamentului IT.	X		
1.5	Analizaţi dacă la stabilirea obiectivelor strategice s-a ţinut cont de mediul intern şi de mediul extern;	X		
1.6.	Analizaţi dacă obiectivele definite reprezintă o componentă importantă în cadrul sistemului de management al organizaţiei.	X		
1.7.	Examinaţi dacă strategia acoperă mandatul cu care a fost investită structura funcţională;	X		
1.8.	Verificaţi dacă există o fundamentare detaliată a strategiei;	X		
1.9.	Verificaţi dacă planul de acţiune pentru implementarea strategiei este dezvoltat suficient;	X		
1.10.	Verificaţi dacă există persoană responsabilă cu actualizarea strategiei;	X		
1.11.	Examinaţi dacă definirea priorităţilor strategice este realizată în concordanţă cu scopul entităţii, în cadrul domeniului de activitate	X		
1.12.	Analizaţi dacă strategia elaborată defineşte	X		
	a) misiunea structurii organizaţionale	X		
	b) stabilirea scopurilor fundamentale	X		
	c) precizarea modalităţilor de acţiune	X		
	d) fundamentarea necesarului de resurse	X		
	e) eşalonarea termenelor	X		
D.	**Comitetul IT determină strategia IT**			
1.	**Comitetul IT transpune strategia în planuri pe termen scurt şi pe termen mediu**			
1.1.	Verificaţi dacă Comitetul de dezvoltare IT este constituit în mod adecvat;	X		
1.2.	Analizaţi dacă planul este examinat periodic pentru a se verifica îndeplinirea acestuia.	X		
1.3.	Examinaţi procesul-verbal al grupului de strategie şi urmăriţi dacă garantează examinarea şi luarea de măsuri cu privire la îndeplinirea obiectivelor strategice.	X		
1.4.	Obţinerea de exemplare ale unor analize referitoare la proiectele de suport IT care au fost realizate, pentru a se garanta că sunt luate în considerare de grupul de strategie şi de conducerea superioară.	X		
1.5.	Verificaţi dacă sunt definite termenele şi etapele de realizare a activităţilor;	X		
1.6.	Verificaţi dacă planul este alcătuit în concordanţă cu bugetul anual de venituri şi cheltuieli;	X		
1.7.	Analizaţi dacă priorităţile sunt judicios ierarhizate în cadrul planului;	X		
1.8.	Analizaţi dacă gradul de adecvare al priorităţilor este raportat la misiunea organizaţiei;	X		
1.9.	Analizaţi dacă indicatorii ataşaţi obiectivelor converg spre economicitate, eficienţă şi eficacitate;	X		
1.10.	Analizaţi dacă planurile sunt adaptate la condiţiile externe organizaţiei;	X		
1.11.	Verificaţi dacă resursele sunt delimitate pentru implementarea planurilor de activitate;			
	a) cunoaşterea de către toţi salariaţii a panului anual de activitate;			
	b) interesul salariaţilor în realizarea obiectivelor planului anual;			
	c) asigurarea competenţelor necesare pentru realizarea activităţilor;			
	d) cunoaşterea metodologiei de realizare şi implementare a activităţilor în			

	rândul salariaţilor;	X		
	e) cunoaşterea nevoilor salariaţilor;			
	f) corelarea obiectivelor individuale cu obiectivele organizaţiei;			
	g) încadrarea în resursele financiare planificate;			
1.12.	Analizaţi dacă impactul planurilor este raportat la performanţa organizaţiei;	X		
1.13.	Analizaţi dacă nivelul cunoştinţelor personalului asigură realizarea programelor;	X		
1.14.	Analizaţi dacă instrumentele de implementare a programelor sunt bine definite;	X		
1.15.	Verificaţi dacă posturile care vor apărea sau se vor schimba sunt luate în calcul la definirea strategiei;	X		
1.16.	Analizaţi dacă competenţele necesare în viitor sunt definite în cadrul strategiei;	X		
1.17.	Verificaţi dacă posibilitatea reorientării şi recalificării profesionale este luată în calcul la stabilirea resurselor necesare implementării strategiei;	X		
1.18.	Verificaţi dacă strategia ţine cont de schimbările la nivel managerial;	X		
1.19	Verificaţi dacă nevoile de instruire sunt definite în cadrul strategiei;	X		
2.	**1.4.3. Comitetul IT stabileşte prioritățile proiectelor între dezvoltarea sistemelor şi activitățile realizate**			
2.1.	Verificaţi dacă există un program de dezvoltare IT	X		
2.2.	Verificaţi dacă programul de dezvoltare IT conţine achiziţii de aplicaţii şi echipamente;	X		
2.3.	Verificaţi dacă există o fundamentare a necesităţii achiziţiilor de echipamente;	X		
2.4.	Verificaţi dacă există o fundamentare a necesităţii achiziţiilor de aplicaţii şi programe;	X		
2.5.	Verificaţi dacă achiziţiile de echipamente sunt prioritizate în funcţie de necesităţi	X		
2.6.	Verificaţi dacă achiziţiile de programe şi aplicaţii sunt prioritizate în funcţie de necesităţi şi de dezvoltarea strategică a organizaţiei în domeniul IT;	X		
2.7.	Verificaţi dacă programele de achiziţii de echipamente şi aplicaţii sunt evaluate de către Comitetul IT;	X		
2.8.	Verificaţi dacă Comitetul IT a realizat şi o evaluare calitativă şi tehnică a echipamentelor şi aplicaţiilor planificate a fi achiziţionate	X		
2.9.	Verificaţi dacă achiziţiile de echipamente şi aplicaţii sunt realizate cu respectarea criteriilor planificate;	X		
2.10.	Verificaţi dacă procesul de achiziţii IT este monitorizat de Comitetul IT;	X		
2.11.	Verificaţi dacă Comitetul IT raportează periodic managementului necesităţile apărute şi stadiul derulării programelor în domeniul IT.	X		
E.	**Organizarea IT corespunde necesităţilor organizaţiei**			
1.	**Organizarea adecvată a funcţiei IT**			
1.1.	Verificaţi dacă deciziile sunt în corelaţie cu transformările din mediul organizaţional;	X		
1.2.	Verificaţi dacă persoana care emite decizia deţine sarcinile, competenţele şi responsabilităţile necesare;	X		
1.3.	Examinarea dacă subsistemele IT acoperă nevoile pentru funcţiile principale ale entităţii;		X	Test nr. 1.5 Interviu nr. 1.5 FIAP nr. 1.5
1.4.	Analiza dacă nevoile pentru funcţiile principale nou-create sunt acoperite;		X	
1.5.	Analiza dacă structurile din cadrul IT si-au definit clar propriile activităţi;		X	
1.6.	Examinarea dacă procedurile elaborate acoperă toate activităţile derulate;		X	
1.7.	Verificaţi dacă responsabilităţile sunt stabilite clar şi precis în sarcina utilizatorilor;	X		
1.8.	Verificaţi dacă competenţele asigură realizarea activităţilor;	X		
1.9.	Verificaţi dacă este realizată evaluarea performanţelor actuale ale activităţilor desfăşurate;	X		
1.10.	Verificaţi dacă este realizată analiza sistemului actual de organizare şi conducere a activităţii;	X		
1.11.	Verificaţi dacă mediul şi factorii externi de influenţă sunt examinaţi şi analizaţi la stabilirea proceselor organizaţionale;	X		
1.12.	Verificaţi dacă mediul intern şi factorii interni de influenţă sunt analizaţi	X		

	şi evaluaţi la stabilirea proceselor organizaţionale;			
1.13.	Verificaţi dacă au fost elaborate instrumentele şi procedurile de implementare a strategiei;	X		
1.14.	Analizaţi dacă s-a determinat volumul şi structura resurselor necesare pentru realizarea obiectivelor;	X		
1.15	Analizaţi dacă au fost elaborate instrumentele şi procedurile de control;	X		
2.	**Adecvarea practicii şi procedurilor IT la procesele existente**			
2.1.	Analizaţi sistemul de elaborare a subsistemelor IT pentru funcţiile principale.	X		
2.2.	Existenţa programului pentru instruirea utilizatorilor subsistemului IT	X		
2.3.	Examinaţi dacă subsistemele IT acoperă în totalitate nevoile pentru funcţiile principale ale entităţii publice	X		
2.4.	Analizaţi dacă nevoile de subsisteme IT pentru funcţiile principale nou-create au fost acoperite.	X		
2.5.	Verificaţi dacă departamentele înfiinţate ca urmare a funcţiilor principale nou-create au fost solicitate să-şi exprime cerinţele specifice privind realizarea unor subsisteme IT proprii activităţii lor	X		
2.6.	Analizaţi existenţa corelării între termenele de realizare a subsistemelor.	X		
2.7.	Analizaţi procedurile pe baza cărora se realizează subsistemele IT şi stabiliţi dacă acestea sunt suficiente pentru implementarea acestor subsisteme în condiţii optime.	X		
2.8.	Stabiliţi dacă există studii de fezabilitate pentru subsistemele IT planificate.	X		
2.9.	Verificaţi dacă există proceduri pentru toate aplicaţiile derulate în cadrul organizaţiei;	X		
2.10.	Verificaţi dacă aplicaţiile derulate în cadrul posturilor de lucru sunt suficiente, necesare şi asigură eficientizarea activităţilor;	X		
2.11.	Verificaţi dacă aplicaţiile derulate sunt adecvate proceselor organizaţiei;	X		
2.12.	Verificaţi dacă aplicaţiile sunt cunoscute şi aplicate de utilizatori.	X		
F.	**Elaborarea strategiei IT corespunde strategiei organizaţiei**			
1.	**Dotarea actuală cu tehnică de calcul a stat la baza elaborării strategiei IT**			
1.1.	Verificarea dacă există un control asupra stării echipamentelor;	X		
1.2.	Verificarea dacă obiectivele strategice în domeniul IT sunt stabilite pe baza unei analize a stării actuale;	X		
1.3.	Verificarea dacă achiziţia aplicaţiilor şi programelor are în vederea dezvoltarea strategică a organizaţiei;	X		
1.4.	Verificarea dacă achiziţia echipamentelor şi tehnicii de calcul ţine cont de dotarea existentă;	X		
1.5.	Verificarea dacă achiziţiile de echipamente ţin cont de caracteristicile calitative şi de performante acestora;	X		
1.6.	Verificarea dacă achiziţiile de echipamente sunt adaptate nevoilor şi necesităţilor organizaţiei;	X		
1.7	Verificarea dacă aplicaţiile şi programele de achiziţionat sunt adecvate proceselor organizaţiei;	X		
1.8.	Verificarea dacă aplicaţiile şi programele achiziţionate conduc la integrarea datelor şi informaţiilor;	X		
1.9.	Verificarea dacă strategia IT conduce la informatizarea în totalitate a organizaţiei;	X		
1.10.	Verificarea dacă strategia asigură pregătirea personalului în concordanţă cu programele de dezvoltare IT.	X		

Auditori,

Popescu Sorin
Radu George

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 1.1

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 13.09.2009
Avizat: Dumitru Daniel Data: 13.09.2009

Obiectul testului	Strategia IT defineşte necesităţile şi priorităţile
Obiectivele testului	Analiza direcţiilor de acţiune stabilite în cadrul strategiei IT şi urmărirea dacă acestea contribuie la realizarea mandatului şi scopului entităţii şi dacă acestea au fost implementate, conform programelor aprobate.
Descrierea testului	1. ***Populaţia*** avută în vedere pentru constituirea eşantionului este formată din: - strategia elaborată în domeniul IT, direcţiile de acţiune definite şi obiectivele strategice stabilite cu privire la dezvoltarea entităţii în domeniul IT; - procesele verbale ale comisiei numite la nivelul entităţii cu responsabilităţi în domeniul planificării, elaborării şi urmăririi implementării strategiei; - programele şi aplicaţiile informatice, aprobate la nivelul entităţii, în perioada analizată, care corespund direcţiilor de implementare a strategiei. 2. ***Eşantionul*** a fost constituit astfel: - strategia entităţii în domeniul IT a fost analizată şi evaluată în totalitatea ei şi comparată cu strategia entităţii; - în perioada suspusă auditării, au fost aprobate în vederea implementării patru proiecte informatice, în acest sens toate acestea fiind evaluate cu privire condiţiile de implementare, termenele de implementate şi concordanţa cu direcţiile strategice aprobate. - în perioada supusă auditării, Comisia numită la nivelul entităţii cu responsabilităţi în domeniul dezvoltării IT s-a întrunit trimestrial, în acest sens au fost analizate şi evaluate toate procesele verbale întocmite după fiecare şedinţă de lucru organizată; 3. ***Prin testarea*** ce se va realiza se va urmări, dacă activităţile desfăşurate în realizarea direcţiilor de acţiune stabilite în cadrul Strategiei sunt monitorizate şi evaluate cu privire la modul de implementare, respectiv: - concordanţa strategiei elaborate în domeniul IT cu strategia entităţii; - responsabilităţile stabilite Comisiei numită la nivelul entităţii cu atribuţii în domeniul dezvoltării IT, contribuie la asigurarea unei decizii eficiente la nivelul entităţii. - analiza proceselor verbale ale Comisiei numită la nivelul entităţii cu atribuţii în domeniul dezvoltării IT - urmărirea dacă toate activităţile de implementare a strategiei sunt monitorizate şi evaluate;
Constatări	Potrivit deciziei de numire, Comisia de planificare strategică înfiinţată la nivelul entităţii are rolul de a stabili obiectivele strategice, relaţiile cu celelalte componente structurale din cadrul entităţii, fundamentarea modalităţilor de realizare a proiectelor, dimensionarea resurselor ce urmează a fi angajate, stabilirea termenelor intermediare şi finale de realizare a proiectelor, monitorizarea implementării proiectelor aprobate. 1. Cu privire la armonizarea strategiei în domeniul IT cu strategia entităţii, s-a constatat că aceasta derivă şi este elaborată în conformitate cu direcţiile şi principiile de dezvoltare ale entităţii, contribuie la dezvoltarea şi eficientizarea activităţilor entităţii şi prin implementare se urmăreşte realizarea unui sistem informatic integrat, care să asigure

	corelarea tuturor informaţiilor şi datelor la nivelul entităţii, respectiv juridice, economice, comerciale, tehnice, financiar-contabile, de personal, sociale şi patrimoniale. 2. Din analiza atribuţiilor stabilite Comisiei numită la nivelul entităţii cu responsabilităţi în domeniul dezvoltării IT, s-a constatat că acestea sunt, în general, de natură metodologică, respectiv planificarea şi elaborarea strategiei în domeniul IT şi armonizarea acesteia cu strategia şi mandatul entităţii. Totuşi, această comisie are şi atribuţii cu privire la monitorizarea activităţilor privind implementarea strategiei, însă analiza realizării acestor activităţi este rezumată doar la analiza raportărilor periodice realizate de departamentul IT, cu privire la stadiul implementării proiectelor IT. Limitarea exercitării acestor atribuţii, doar la analiza raportărilor efectuate de departamentul IT, fără o evaluare fizică, din partea comisiei, a modului de implementare a programelor informatice, conduce la formularea unor constatări şi concluzii insuficiente, care au influenţă în decizia managerială şi dezvoltarea strategică. 3. Analiza proceselor-verbale ale Comisiei numite la nivelul entităţii cu responsabilităţi în dezvoltarea IT, a direcţiilor de acţiune strategice şi a deciziilor luate în vederea implementării strategiei a pus în evidenţă unele disfuncţionalităţi, legate de faptul că anumite proiecte de dezvoltare IT, derulate în cadrul entităţii, nu au fost supuse analizei şi evaluării comisiei. Astfel, în cursul anului 2009, discuţiile în cadrul comisiei au privit, în general, analiza progreselor proiectelor IT stabilite şi aprobate la nivelul entităţii, însă potrivit proceselor verbale întocmite în urma şedinţelor, a rezultat că discuţiile s-au derulat doar cu privire la proiectele pentru care au fost înaintate de către departamentul IT, rapoarte privind stadiul implementării, astfel că propunerile formulate de comisie cu privire la dezvoltarea IT, inclusiv cu privire la asigurarea resursele financiare, au fost legate doar de acestea. În urma examinării şi analizelor efectuate, s-a constatat că anumite proiecte nu au fost implementate sau sunt întârzieri în implementarea acestora, respectiv: a) aplicaţia privind evidenţa documentelor intrate ieşite din cadrul organizaţiei, inclusiv stadiul soluţionării lor, a fost aprobată a fi implementată, inclusiv asigurarea resurselor financiare, încă din cursul anului anterior, dar până în prezent nu s-a realizat nici o procedură legată de stabilirea condiţiilor tehnice ale aplicaţiei, demararea acţiunilor de realizare a caietului de sarcini, sau procedurilor privind achiziţia, cu toate că în buget au fost alocate fondurile necesare. Din discuţiile purtate cu responsabilii IT în domeniul dezvoltării şi informatizării entităţii, a rezultat că acest program informatic nu a fost demarat, deoarece la nivelul departamentului IT nu existau specialişti în testarea şi implementarea lui, iar fondurile aprobate permiteau doar achiziţia aplicaţiei. În condiţiile în care atribuţiile comisiei permiteau şi o evaluare fizică a modului de implementare a proiectelor, greutăţile întâmpinate se puteau cunoaşte şi găsi soluţiile necesare, respectiv, în acest caz a condiţiilor de pregătire a personalului în vederea utilizării acestui program informatic. b) pentru proiectul „Implementarea unei infrastructuri IT care să asigure integrarea datelor la nivelul organizaţiei", a fost raportat stadiul de implementare la comisie, însă nu şi termenele de realizare. În urma evaluării, s-a constatat că au fost demarate procedurile pentru achiziţia acestuia, însă până în prezent acestea s-au limitat la studiul pieţei şi alocarea banilor în cadrul bugetului. Proiectul se află în întârziere şi nu va putea fi realizat în timp util. Aceasta va avea consecinţe negative în implementarea altor aplicaţii, care depind de acesta, în acest sens va trebui amânat termenul de începere a procedurilor privind implementarea proiectului „Crearea unei structuri IT care să permită urmărirea circuitului unui document, stadiul de realizare şi persoanele care au intervenit asupra acestuia, autorizarea pe niveluri ierarhice prestabilite". Întârzierea implementării acestui program a determinat nerealizarea în termenul planificat a obiectivului strategic „Modernizarea infrastructurii IT din cadrul entităţii".
Concluzii	Neatribuirea Comisiei numită la nivelul entităţii de responsabilităţi în domeniul

	dezvoltării IT, a unor atribuţii de urmărire fizică a modului de implementare a direcţiilor strategice, respectiv a proiectelor informatice de dezvoltare şi informatizare a entităţii, a condus la întârzieri în achiziţia, testarea şi implementarea programelor, neînceperea procedurilor de achiziţie şi implementare a altor programe sau aplicaţii informatice. Obiectivele strategice stabilite în domeniul IT nu au fost îndeplinite în termenele stabilite.

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 1.1

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2008
Întocmit: Popescu Sorin/ Radu George Data: 13.09.2009
Avizat: Dumitru Daniel Data: 13.09.2009

Problema	Nerealizarea în termen a procedurilor de achiziţie şi implementare a programelor şi aplicaţiilor informatice.
Constatarea	1. Cu privire la armonizarea strategiei în domeniul IT cu strategia entităţii, s-a constatat că aceasta derivă şi este elaborată în conformitate cu direcţiile şi principiile de dezvoltare ale entităţii, contribuie la dezvoltarea şi eficientizarea activităţilor entităţii şi prin implementare se urmăreşte realizarea unui sistem informatic integrat, care să asigure integrarea tuturor informaţiilor şi datelor la nivelul entităţii, respectiv juridice, economice, comerciale, tehnice, financiar-contabile, de personal, sociale şi patrimoniale. 2. Din analiza atribuţiilor stabilite Comisiei numită la nivelul entităţii cu responsabilităţi în domeniul dezvoltării IT, s-a constatat că acestea sunt, în general, de natură metodologică, respectiv planificarea şi elaborarea strategiei în domeniul IT şi armonizarea acesteia cu strategia şi mandatul entităţii. Totuşi, această comisie are şi atribuţii cu privire la monitorizarea activităţilor privind implementarea strategiei, însă analiza realizării acestor activităţi este rezumată doar la raportările periodice realizate de departamentul IT, cu privire la stadiul implementării proiectelor IT. Limitarea exercitării acestor atribuţii, doar la analiza raportărilor efectuate de departamentul IT, fără o evaluare fizică, din partea comisiei, a modului de implementare a programelor informatice, conduce la formularea unor constatări şi concluzii insuficiente, care au influenţă în decizia managerială şi dezvoltarea strategică. 3. Analiza proceselor-verbale ale Comisiei numite la nivelul entităţii cu responsabilităţi în dezvoltarea IT, a direcţiilor de acţiune strategice şi a deciziilor luate în vederea implementării strategiei a pus în evidenţă unele disfuncţionalităţi, legate de faptul că anumite proiecte de dezvoltare IT derulate în cadrul entităţii nu au fost supuse analizei şi evaluării comisiei. Astfel, în cursul anului 2009, discuţiile în cadrul comisiei au privit, în general, analiza progreselor proiectelor IT stabilite şi aprobate la nivelul entităţii, însă potrivit proceselor verbale întocmite în urma şedinţelor, a rezultat că discuţiile s-au derulat doar cu privire la proiectele pentru care au fost înaintate de către departamentul IT, rapoarte privind stadiul implementării, astfel că propunerile formulate de comisie cu privire la dezvoltarea IT, inclusiv cu privire la asigurarea resursele financiare, au fost legate doar de aceste aspecte. În urma examinării şi analizelor efectuate s-a constatat că anumite proiecte nu au fost implementate sau sunt întârzieri în implementarea acestora, respectiv: a) aplicaţia privind evidenţa documentelor intrate ieşite din cadrul organizaţiei, inclusiv stadiul soluţionării lor, a fost aprobată a fi implementată, inclusiv au fost asigurate resursele financiare încă din cursul anului anterior, dar până în prezent nu s-a realizat nici o procedură legată de stabilire a condiţiilor tehnice ale aplicaţiei, demararea acţiunilor de realizare a caietului de sarcini, sau a procedurilor de realizare a achiziţiei, cu toate că prin buget au fost alocate fondurile necesare. Din discuţiile purtate cu responsabilii IT în domeniul dezvoltării şi informatizării entităţii, a rezultat că acest program informatic nu a fost demarat, deoarece la nivelul departamentului IT nu existau specialişti în testarea şi implementarea programului, iar fondurile aprobate permiteau doar achiziţia aplicaţiei.

	În condiţiile în care atribuţiile comisiei permiteau şi o evaluare fizică a modului de implementare a proiectelor, greutăţile întâmpinate se puteau cunoaşte şi se puteau găsi soluţiile necesare, respectiv, în acest caz a condiţiilor de pregătire a personalului în vederea utilizării programului informatic. b) pentru proiectul „Implementarea unei infrastructuri IT care să asigure integrarea datelor la nivelul organizaţiei", a fost raportat stadiul de implementare la comisie, însă nu şi termenele de realizare. În urma evaluării s-a constatat că au fost demarate procedurile pentru achiziţia acestuia, însă până în prezent acestea s-au limitat la studiul pieţei şi alocarea banilor în cadrul bugetului. Proiectul se află în întârziere şi nu va putea fi realizat în timp util. Aceasta va avea consecinţe negative în implementarea altor aplicaţii, care au legătură cu acesta, în acest sens va trebui decalat termenul de începere a procedurilor privind implementarea proiectului „Crearea unei structuri IT care să permită urmărirea circuitului unui document, stadiul de realizare şi persoanele care au intervenit asupra acestuia, autorizarea pe niveluri ierarhice prestabilite". Întârzierea implementării acestui program a determinat decalarea termenul planificat a obiectivului strategic „Modernizarea infrastructurii IT din cadrul entităţii".
Cauza	Neatribuirea Comisiei numită la nivelul entităţii de responsabilităţi în domeniul dezvoltării IT, a unor atribuţii de urmărire fizică a modului de implementare a direcţiilor strategice, respectiv a proiectelor informatice de dezvoltare şi informatizare a entităţii. Potrivit deciziei de numire, Comisia de planificare strategică înfiinţată la nivelul entităţii are rolul de a stabili obiectivele strategice, relaţiile cu celelalte componente structurale din cadrul entităţii, fundamentarea modalităţilor de realizare a proiectelor, dimensionarea resurselor ce urmează a fi angajate, stabilirea termenelor intermediare şi finale de realizare a proiectelor, monitorizarea implementării proiectelor aprobate.
Consecinţa	Întârzieri în achiziţia, testarea şi implementarea programelor. Totodată, unele programe preconizate a fi achiziţionate ulterior şi care urmau a fi implementate după punerea în funcţiune a acestora nu s-au mai achiziţionat.
Recomandări	Reanalizarea atribuţiilor Comisiei de planificare strategică în domeniul IT şi redefinirea acestora astfel încât să poată realiza şi monitorizarea implementării proiectelor informatice şi informarea periodică a conducerii asupra realizării acestora. Analiza proiectelor informatice aprobate a fi implementate şi pentru care au fost alocate şi resursele financiare, stabilirea de termene de implementare şi respectarea acestora.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Popescu Sorin	Dumitru Daniel	Structura auditată

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 1.2

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 13.09.2009
Avizat: Dumitru Daniel Data: 13.09.2009

Obiectul testului	Strategia IT defineşte necesităţile şi priorităţile
Obiectivele testului	Analiza sistemului de fundamentare a necesarului de resurse pentru realizarea strategiei în domeniul IT.
Descrierea testului	Evaluarea condiţiilor privind elaborarea strategiei va urmări analiza modului în care au fost respectate şi analizate următoarele activităţi cuprinse în procedura de realizare a strategiei din *Lista de verificare nr. 1, poziţia 1.2.* Strategia elaborată la nivelul structurii funcţionale a avut în vedere următoarele: a) evaluarea situaţiei actuale pe baza analizei diagnostic; b) identificarea punctelor tari şi a punctelor slabe ale entităţii; c) formularea misiunii organizaţiei; d) fundamentarea variantelor strategice; e) identificarea şi provenienţa resurselor; f) implementarea strategiei . Testarea s-a realizat prin evaluarea sistemului de elaborare a strategiei şi a documentelor rezultate, dar şi în baza *Notei de relaţii nr. 1 privind modul de elaborare şi fundamentare a strategiei*, adresată domnului Georgescu Mihai – Şef serviciu.
Constatări	Din analiza sistemului de fundamentare a strategiei, rezultă că s-au realizat următoarele etape: *a) definirea rolului* IT în cadrul organizaţiei, fiind identificată şi definită importanţa departamentului IT; *b) definirea misiunii structurii funcţionale* în concordanţă cu obiectivele strategice şi direcţiile de acţiune stabilite la nivelul organizaţiei; *c) identificarea şi provenienţa resurselor financiare, materiale şi umane* necesare aplicării şi implementării strategiei; *d) implementarea strategiei,* fiind fixate termenele necesare atingerii obiectivelor în raport cu care se urmăresc asigurarea şi repartizarea resurselor precum şi concentrarea eforturilor umane şi materiale. Tot din analiză rezultă că la elaborarea strategiei, la nivelul structurii funcţionale, nu s-au avut în vedere următoarele etape: a) *Evaluarea situaţiei actuale pe baza analizei diagnostic*, respectiv orientarea activităţii pentru o anumită perioadă, prin strategie, presupune ca, în prealabil, să fie cunoscută situaţia actuală, pe baza unei analize diagnostic, pentru a avea o imagine cât mai completă asupra domeniului de activitate al organizaţiei. Analiza diagnostic trebuia elaborată în baza unor studii privind potenţialului intern, folosind metode statistice, matematice, analiza pe bază de bilanţ etc. care să surprindă evoluţia proceselor şi fenomenelor specifice domeniului de activitate. Informaţiile de intrare nu fac referire la aspecte cum sunt: dimensiunea structurii funcţionale, resursele umane, înzestrarea tehnic, managementul utilizat; b) *Identificarea punctelor tari şi a punctelor slabe ale entităţii* în vederea determinării ameninţărilor şi oportunităţilor cu care se confruntă entitatea; c) *Fundamentarea variantelor strategice* – obiectivele strategice stabilite nu au fost corelate cu posibilităţile efective ale organizaţiei, cu factorii interni şi factori externi. Realizarea strategiei implică fixarea şi respectarea termenelor necesare atingerii obiectivelor în raport cu care se urmăresc asigurarea şi repartizarea resurselor, precum şi

	concentrarea eforturilor umane şi materiale. Totodată, trebuie avută în vedere compatibilitatea variantei strategice elaborată teoretic cu realitatea şi modul în care s-a reuşit surprinderea acţiunii factorilor de influenţă. Strategia a fost elaborată fără a se evalua situata actuala, pe baza unei analize diagnostic, astfel încât să putem avea o imagine cât mai completa asupra organizaţiei, asupra rezultatelor pe care şi-a propus să le obţină, a potenţialului său financiar, cât şi a importanţei în cadrul realizării programului de guvernare. Totodată nu au fost identificate nici punctele tari şi punctele slabe în vederea determinării ameninţărilor şi oportunităţilor cu care se confruntă entitatea. De asemenea, obiectivele strategice ale structurii funcţionale, definite în cadrul strategiei, nu au fost corelate cu posibilităţile efective ale organizaţiei, cu factorii interni şi factori externi. Realizarea strategiei implica fixarea şi respectarea termenelor necesare atingerii obiectivelor în raport cu care se urmăresc asigurarea şi repartizarea resurselor precum şi concentrarea eforturilor umane şi materiale.
Concluzii	În activitatea de fundamentare a strategiei nu s-a respectat procedura operaţională de lucru aprobată de conducerea entităţii, astfel: a) Nerealizarea, pe baza analizei diagnostic, a evaluării situaţiei actuale în vederea elaborării strategiei. b) neidentificarea punctelor tari şi a punctelor slabe în vederea determinării ameninţărilor şi oportunităţilor. c) obiectivele strategice definite în cadrul strategiei nu au fost corelate cu posibilităţile efective ale organizaţiei, cu factorii interni şi factori externi.

Auditor intern,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

NOTĂ DE RELAŢII nr. 1.1
privind elaborarea şi fundamentarea strategiei
adresată
Domnului Georgescu Mihai, Şef serviciu

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Întrebarea nr. 1. Cine răspunde de elaborarea strategiei în domeniul IT*?*

Răspuns nr. 1. Compartimentul metodologie şi dezvoltare IT.

Întrebarea nr. 2. Cum au fost determinate necesităţile de achiziţii IT şi cuprinse în cadrul strategiei?
Răspuns nr. 2. Pe baza analizei importanţei activităţilor pe care le desfăşoară organizaţia şi a modului de satisfacere a cerinţelor colaboratorilor.

Întrebarea nr. 3. Definirea misiunii departamentului pe ce a fost fundamentată*?*
Răspuns nr. 3. Pe baza mandatului stabilit de Consiliul de Administraţie.

Întrebarea nr. 4. Strategia elaborată a fost implementată*?*
Răspuns nr. 4. Pe baza strategiei au fost elaborate politici pentru fiecare domeniu de activitate al departamentului, politici pe baza cărora au fost stabilite activităţile şi acţiunile necesare.

Întrebarea nr. 5. La elaborarea strategiei, evaluarea situaţiei actuale s-a realizat pe baza unei analize diagnostic*?*
Răspuns nr. 5. Nu.

Întrebarea nr. 6. Cum au fost analizate şi interpretate, la elaborarea strategiei punctele tari şi punctele slabe*?*
Răspuns nr. 6. Nu a fost realizată o analiza a punctelor tari şi punctelor slabe la elaborarea strategiei.

Întrebarea nr. 7. Fundamentarea strategiei s-a bazat pe elaborarea mai multor variante*?*
Răspuns nr. 7. Nu.

Întrebarea nr. 6. *Mai aveţi ceva de adăugat?*
Răspuns nr. 6. *Nu.*

Data: 13.09.2009

Dată în faţa noastră: Auditori
Popescu Sorin
Radu George

Şef serviciu,
Georgescu Mihai

Procedura P08:	**Colectarea dovezilor**

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

INTERVIU nr. 1.1
privind elaborarea şi fundamentarea planului strategic,
adresat domnului Ionescu Adrian, director general DGTI

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Nr. crt.	**Întrebări**	**Da**	**Nu**	**Observaţii**
1.	Există un sistem de fundamentare a planului strategic?	X		
2.	Planul strategic este corelat cu planurile anuale?	X		Planul strategic este defalcat în planurile anuale.
3.	Există un sistem de prioritizare a activităţilor cuprinse în plan?	X		Prin planul strategic aprobat se urmăreşte atingerea obiectivelor strategice stabilite prin politicile entităţii publice în domeniul IT.
4.	Strategia definită la nivelul entităţii publice defineşte clar obiectivele?	**X**		
5.	Obiectivele strategice sunt în concordanţă cu direcţiile de acţiune ale entităţii publice?	**X**		
6.	La elaborarea planului strategic aţi avut în vedere definirea mandatului şi a misiunii structurii organizaţionale?	**X**		
7.	Planul strategic are în vedere principalele domenii de interes în domeniul IT?	**X**		
8.	Planul strategic stabileşte politica în domeniul IT?	**X**		
9.	Planul strategic precizează modalităţile de acţiune?	**X**		
10.	Planul strategic conţine o eşalonare a termenelor de realizare a obiectivelor?	**X**		
11.	Au fost previzionate resursele necesare pentru îndeplinirea planului strategic?	X		
12.	Necesităţile de actualizare a planului strategic sunt analizate periodic?			
13.	Aţi desemnat persoane responsabile cu centralizarea noutăţilor în vederea actualizării planului strategic?	X		

Data: 13.09.2009

Formulat în prezenţa noastră: Auditori
Popescu Sorin
Radu George

Intervievat,
Director general, Ionescu Adrian

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 1.2

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 13.09.2009
Avizat: Dumitru Daniel Data: 13.09.2009

Problema	Nerespectarea procedurii de elaborare şi fundamentare a strategiei şi a politicilor de dezvoltare.
Constatarea	Din analiza sistemului de fundamentare a strategiei, rezultă că s-au realizat următoarele etape: *a) stabilirea rolului* IT în cadrul organizaţiei, fiind identificată şi definită importanţa acesteia; *b) definirea misiunii structurii funcţionale* în concordanţă cu obiectivele strategice şi direcţiile de acţiune stabilite la nivelul organizaţiei; *c) identificarea şi provenienţa resurselor financiare, materiale şi umane* necesare aplicării şi implementării strategiei; *d) implementarea strategiei,* fiind fixate termenele necesare atingerii obiectivelor în raport cu care se urmăresc asigurarea şi repartizarea resurselor precum şi concentrarea eforturilor umane şi materiale. Tot din analiză rezultă că la elaborarea strategiei, la nivelul structurii funcţionale, nu s-au avut în vedere următoarelor etape: *a) Evaluarea situaţiei actuale pe baza analizei diagnostic*, respectiv orientarea activităţii pentru o anumită perioadă, prin strategie, presupune ca, în prealabil, să fie cunoscută situaţia actuală, pe baza unei analize diagnostic, pentru a avea o imagine cât mai completă asupra domeniului de activitate al organizaţiei. Analiza diagnostic trebuia elaborată în baza unor studii privind potenţialului intern, folosind metode statistice, matematice, analiza pe bază de bilanţ etc. care să surprindă evoluţia proceselor şi fenomenelor specifice domeniului de activitate. Informaţiile de intrare nu fac referire la aspecte cum sunt: dimensiunea structurii funcţionale, resursele umane, înzestrarea tehnică, managementul utilizat; *b) Identificarea punctelor tari şi a punctelor slabe ale entităţii* în vederea determinării ameninţărilor şi oportunităţilor cu care se confruntă entitatea; ***c)*** *Fundamentarea variantelor strategice* – obiectivele strategice stabilite pentru IT nu au fost corelate cu posibilităţile efective ale organizaţiei, cu factorii interni şi factori externi. Realizarea strategiei implică fixarea şi respectarea termenelor necesare atingerii obiectivelor în raport cu care se urmăresc asigurarea şi repartizarea resurselor precum şi concentrarea eforturilor umane şi materiale. Totodată, trebuie avuta în vedere compatibilitatea variantei strategice elaborata teoretic cu realitatea şi modul în care s-a reuşit surprinderea acţiunii factorilor de influenta. Strategia a fost elaborată fără a se evalua situata actuala, pe baza unei analize diagnostic, astfel încât să putem avea o imagine cât mai completa asupra organizaţiei, asupra rezultatelor pe care şi-a propus să le obţină, a potenţialului său financiar, cât şi a importanţei în cadrul realizării programului de guvernare. Totodată nu au fost identificate nici punctele tari şi punctele slabe în vederea determinării ameninţărilor şi oportunităţilor cu care se confruntă entitatea. De asemenea, obiectivele strategice ale structurii funcţionale, definite în cadrul strategiei, nu au fost corelate cu posibilităţile efective ale organizaţiei, cu factorii interni şi factori externi. Realizarea strategiei implica fixarea şi respectarea

	termenelor necesare atingerii obiectivelor în raport cu care se urmăresc asigurarea şi repartizarea resurselor precum şi concentrarea eforturilor umane şi materiale.
Cauza	Personalul responsabil de elaborarea strategiei nu a avut pregătirea necesara în vederea realizării unei analize de ansamblu a organizaţiei şi a unei analize a domeniului de activitate, a identificării factorilor interni şi a factorilor externi care influenţează realizarea activităţilor specifice, cât şi a ameninţărilor şi oportunităţilor în îndeplinirea obiectivelor.
Consecinţa	Implementarea strategiei nu contribuie la realizarea mandatului cu care a fost investită organizaţia, la atingerea obiectivelor generale definite şi la realizarea direcţiilor de acţiune cu privire la dezvoltarea domeniului de activitate.
Recomandări	Pregătirea profesională anticipată a personalului implicat în elaborarea strategiei, de către managementul responsabil cu aceasta. Reanalizarea strategiei definite la nivelul structurii funcţionale în conformitate cu procedura operaţională aprobată. Actualizarea acesteia astfel încât implementarea sa să contribuie la realizarea unui management modern in domeniul de activitate şi la atingerea obiectivelor strategice ale organizaţiei. Îmbunătăţirea procedurilor operaţionale de lucru privind sistemul de fundamentare a necesarului de resurse pentru elaborarea strategiei.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Radu George	Dumitru Daniel	Structură auditată

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 1.3

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 13.09.2009
Avizat: Dumitru Daniel Data: 13.09.2009

Obiectul testului	Strategia IT defineşte necesităţile şi priorităţile
Obiectivele testului	Definirea obiectivelor generale derivate din obiectivele strategice.
Descrierea testului	Evaluarea condiţiilor privind elaborarea strategiei va urmări analiza modului în care au fost definite obiectivele generale, derivate din obiectivele strategice, în conformitate cu *Lista de verificare nr. 1, poziţia 1.3 respectiv:* *- Stabilirea obiectivelor strategice a ţinut cont de mediul intern şi de mediul extern;* *- Obiectivele definite în cadrul strategiei asigură:* *a. definirea realistă a acestora;* *b. asigurarea factorului de mobilizare;* *c. definirea lor astfel încât să fie înţelese de către salariaţi;* *d. definirea lor în formă stimulatoare;* *e. asigurarea necesarului de resurse în vederea implementării obiectivelor* *- Obiectivele generale sunt definite în termeni de impact;* *- Obiectivele generale derivă din obiectivele strategice;* *- Obiectivele generale acoperă strategia definită în cadrul domeniului de activitate;* *- Obiectivele generale în domeniul resurselor umane oferă direcţia şi ţinta finală ce urmează a fi atinsă;* *- Obiectivele sunt formulate de o manieră precisă, riguroasă fără interpretări.* Testarea a fost completată cu elaborarea unui *Interviu privind definirea în termeni de impact a obiectivelor strategice,* adresat domnului Stănescu Cristian - Şef serviciu.
Constatări	Obiectivele strategice reprezintă exprimările cantitative şi calitative ale scopului pentru care există şi funcţionează organizaţia. Din analiza modului de definire şi stabilire a obiectivelor strategice s-a constatat că acestea nu întrunesc următoarele caracteristici definitorii: - nu sunt realiste şi nu au fost luate în calcul capacităţile şi posibilităţile efective de realizare de care dispune organizaţia în condiţiile actuale; - nu sunt mobilizatoare şi nu implică eforturi de autodepăşire din partea salariaţilor; - nu sunt comprehensibile şi nu sunt formulate şi prezentate într-o manieră care să permită înţelegerea conţinutului lor de către salariaţi; - nu sunt stimulatoare şi nu asigură o abordare sistemică a intereselor organizaţiei şi componentelor sale organizatorice într-o viziune optimizantă pe termen mediu şi lung. Aceşti factori trebuie să se regăsească la orice obiectiv strategic, indiferent de natura sa (economică, tehnică), deoarece aceste obiective reprezintă punctul de plecare în conturarea unui sistem unitar de obiective ce vizează toate componentele procesuale şi structurale ale organizaţiei. Dimensiunea şi natura obiectivelor strategice generează direct sau indirect modalităţi şi opţiuni de realizare care condiţionează decisiv conţinutul şi funcţionalitatea strategiei, ceea ce impune ca la implementarea lor să se ia în considerare principalele variabile exogene ce influenţează comportamentul economic

	şi managerial al organizaţiei, cât şi capacitatea acesteia de adaptare la schimbare. La fundamentarea necesarului de resurse solicitate de atingerea obiectivelor nu s-a realizat o dimensionare corectă a fondurilor de investiţii şi a mijloacelor circulante pe baza unor indicatori specifici, cantitativi şi calitativi. De asemenea, personalului nu i-au fost asigurate în toate situaţiile, condiţiile de instruire pentru dobândirea aptitudinilor necesare realizării eficiente a obiectivelor individuale, pentru a contribui astfel, în condiţii de performanţă, la obţinerea impactului definit de obiectivele strategice.
Concluzii	Obiectivele strategice nu sunt definite, in toate cazurile, în mod realist, respectiv nu derivă din atribuţiile generale ce revin structurii funcţionale, ceea ce creează confuzii privind modul practic de realizare a acestora şi implicit de asigurare a impactului stabilit şi de asigurare a definirii corespunzătoare a obiectivelor specifice.

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern

Interviu nr. 1.2
privind definirea în termeni de impact a obiectivelor strategice, adresat domnului Stănescu Cristian - Şef serviciu

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2006 - 31.12.2008

Nr. crt.	ÎNTREBĂRI	DA	NU	OBSERVAŢII
1.	Există un responsabil cu elaborarea strategiei?	X		
2.	La definirea obiectivelor strategice a existat o analiză a domeniilor pentru care acestea au fost definite?		X	*Obiectivele strategice nu sunt realiste*
3.	La definirea obiectivelor strategice au fost luate în calcul capacităţile şi posibilităţile efective ale organizaţiei privind implementarea acestora?		X	*Obiectivele strategice nu sunt mobilizatoare pentru salariaţi*
4.	Obiectivele strategice sunt definite pentru nivelul de înţelegere al salariaţilor?		X	*Obiectivele strategice nu sunt înţelese de salariaţi*
5.	La stabilirea obiectivelor au fost dimensionate resursele pe baza unor indicatori calitativi şi cantitativi?	X		
6.	La definirea obiectivelor strategice s-a urmărit ca termenul de implementare al acestora să fie multianual?	X		
7.	Salariaţii au fost pregătiţi şi instruiţi astfel încât să asigure implementarea obiectivelor?	X		
8.	Obiectivele strategice sunt definite cu respectarea atribuţiilor şi funcţiilor generale ale organizaţiei?	X		
9.	Obiectivele generale sunt definite în cadrul strategiei elaborate la nivelul organizaţiei?	X		
10.	Obiectivele generale oferă pentru domeniile pe care sunt definite, direcţia şi ţinta finală ce urmează a fi atinse?	X		
11.	Obiectivele generale sunt definite într-o formă riguroasă, fără interpretări şi într-o manieră precisă?		X	Obiectivele generale definite nu sunt antrenante pentru salariaţi

Data:
13.09.2009

Şef Serviciu,
Stănescu Cristian

Elaborat în prezenţa noastră: Auditori
Popescu Sorin
Radu George

ENTITATEA PUBLICĂ
Serviciul Audit Intern

Notă de relaţii nr. 1.2
privind elaborarea planului strategic şi a planurilor anuale, adresată domnului Şef serviciu Dezvoltare aplicaţii

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Întrebarea nr. 1: Au fost elaborate planuri strategice şi planuri anuale?
Răspuns nr. 1: Planul strategic a fost elaborat pentru o perioadă de 5 ani în urmă cu doi ani. Planul strategic iniţial este defalcat în planuri anuale pentru a se asigura coordonarea implementării subsistemelor IT.

Întrebarea nr. 2: Elaborarea acestor planuri s-a realizat într-un cadru formalizat?
Răspuns nr. 2: Prin decizia managerului general a fost numită o comisie formată din conducătorii principalelor departamente din cadrul entităţii publice având responsabilitatea elaborării planului strategic şi a planurilor anuale. În calitate de conducător al departamentului IT fac parte din această comisie.

Întrebarea nr. 3: Există un sistem de fundamentare a planului strategic?
Răspuns nr. 3: Fundamentarea planului strategic s-a realizat pe baza analizei nevoilor de informatizare formulate de către departamentele ce asigură realizarea funcţiilor principale ale entităţii publice, pornindu-se de la sistemul IT existent şi urmărindu-se realizarea măsurilor necesare în vederea atingerii parametrilor stabiliţi prin politica IT.

Întrebarea nr. 4: Există un sistem de prioritizare a activităţilor cuprinse în plan?
Răspuns nr. 4: Da. Implementarea subsistemelor IT se va realiza conform planificării, pornind de la importanţa acestora pentru entitatea publică şi ţinându-se cont de resursele de care dispune organizaţia.

Întrebarea nr. 5: Mai aveţi ceva de adăugat?
Răspuns nr. 5: Nu.

Data: 13.09.2009

Intervievat,
Adrian Ionescu

Dată în faţa noastră: Auditori
Popescu Sorin
Radu George

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 1.3

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 13.09.2009
Avizat: Dumitru Daniel Data: 13.09.2009

Problema	Obiectivelor strategice nu asigură acoperirea domeniului de activitate al structurii funcţionale şi nu contribuie la asigurarea realizării mandatului organizaţiei.
Constatarea	Obiectivele strategice reprezintă exprimările cantitative şi calitative ale scopului pentru care există şi funcţionează organizaţia. Din analiza modului de definire şi stabilire a obiectivelor strategice s-a constatat că acestea nu întrunesc următoarele caracteristici definitorii: - nu sunt realiste şi nu au fost luate în calcul capacităţile şi posibilităţile efective de realizare de care dispune organizaţia în condiţiile actuale; - nu sunt mobilizatoare şi nu implică eforturi de autodepăşire din partea salariaţilor; - nu sunt comprehensibile şi nu sunt formulate şi prezentate într-o manieră care să permită înţelegerea conţinutului lor de către salariaţi; - nu sunt antrenante şi nu asigură o abordare sistemică a intereselor organizaţiei şi componentelor sale organizatorice într-o viziune optimizantă pe termen mediu şi lung. Aceşti factori trebuie să se regăsească la orice obiectiv strategic, indiferent de natura sa (economică, tehnică), deoarece aceste obiective reprezintă punctul de plecare în conturarea unui sistem unitar de obiective ce vizează toate componentele procesuale şi structurale ale organizaţiei. Dimensiunea şi natura obiectivelor strategice generează direct sau indirect modalităţi şi opţiuni de realizare care condiţionează decisiv conţinutul şi funcţionalitatea strategiei, ceea ce impune ca la implementarea lor să se ia în considerare principalele variabile exogene ce influenţează comportamentul economic şi managerial al organizaţiei, cât şi capacitatea acesteia de adaptare la schimbare. La fundamentarea necesarului de resurse solicitate de atingerea obiectivelor nu s-a realizat o dimensionare corectă a fondurilor de investiţii şi a mijloacelor circulante pe baza unor indicatori specifici, cantitativi şi calitativi. De asemenea, nu în toate situaţiile, personalului i-au fost asigurate condiţiile de instruire pentru dobândirea aptitudinilor necesare realizării eficiente a obiectivelor individuale pentru a contribui astfel, în condiţii de performanţă, la obţinerea impactului definit de obiectivele strategice.
Cauza	Personalul implicat în elaborarea strategiei nu a fost pregătit în cadrul organizaţiei şi nu a reuşit să înţeleagă obiectivele strategice şi să stabilească corect obiectivele generale, care vor sta la baza stabilirii obiectivelor specifice ale acesteia.
Consecinţa	În forma în care au fost identificate şi stabilite obiectivele strategice şi generale, departamentul nu poate pune la dispoziţia organizaţiei o strategie care să asigure posibilitatea de a-şi dezvolta un management eficient şi eficace al domeniului de activitate în consens cu mandatul său.
Recomandarea	Evaluarea performanţelor actuale ale sistemului de organizare şi conducere a activităţilor desfăşurate în cadrul structurii funcţionale, ţinând cont de influenţa factorilor de mediu, interni şi externi, în vederea redefinirii obiectivelor strategice.

	Implicarea managementului pentru ca obiectivele strategice redefinite să întrunească caracteristicile de a fi realiste, mobilizatoare, stimulative şi să poată fi înţelese de salariaţi, stabilite de metodologie. Totodată, la redefinirea acestora se va urmări asigurarea resurselor necesare (materiale, financiare şi umane) implementării lor.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Popescu Sorin	Dumitru Daniel	Structură auditată

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 1.4

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 13.09.2009
Avizat: Dumitru Daniel Data: 13.09.2009

Obiectul testului	Planurile IT ajută la îndeplinirea misiunii organizaţiei
Obiectivele testului	Fundamentarea resurselor în vederea elaborării planului anual de activitate.
Descrierea testului	Evaluarea resurselor în vederea elaborării planului anual de activitate a pornit de la analiza fundamentării planului, pe baza elementelor prezentate în *Lista de verificare elaborată.* La elaborarea planului de activitate au fost avute în vedere următoarele: - *planul de activitate anual a fost comunicat şi este cunoscut de personalul implicat în realizarea acestuia;* - *salariaţii sunt motivaţi şi cointeresaţi în realizarea obiectivelor planului de activitate;* - *este fundamentat şi dimensionat necesarul de resurse;* - *pentru realizarea activităţilor planificate sunt asigurate competenţele necesare;* - *salariaţii cunosc metodologia de realizare şi implementare a activităţilor planificate;* - *planul este alcătuit în concordanţă cu bugetul anual de venituri şi cheltuieli;* - *pentru realizarea planului anual de activitate, managementul a luat în considerare şi cunoaşterea nevoilor salariaţilor;* - *planul anual de activitate corelează obiectivele individuale cu cele organizaţionale;* - *stabilirea planului anual de activitate permite încadrarea în resursele financiare planificate.* - *sunt anticipate condiţiile viitoare în care va funcţiona organizaţia.* Testarea a fost completată cu un *Interviu privind fundamentarea resurselor pentru asigurarea implementării planului de activitate*, adresat domnului Popescu Valentin - Şef serviciu Dezvoltare Aplicaţii.
Constatări	Din analiză s-a constatat că eforturile pentru elaborarea planului anual de activitate implică alocarea de costuri şi resurse ridicate din partea organizaţiei, care, în cele mai multe din cazuri, nu au ca referinţă atingerea scopului fundamental al acesteia. În acelaşi timp, activităţile considerate prioritare ale planului anual nu au fost realizate sau implementate în mod corespunzător, deoarece nu au fost repartizate atribuţiile în cadrul compartimentelor în corelaţie cu noile obiective stabilite în cadrul planului. Aceasta a însemnat că, în unele cazuri, obiectivele şi activităţile, deşi erau cunoscute de personal, acesta nu avea competenţa necesară, în special a celor care erau realizate în colaborare cu alte structuri funcţionale, ceea ce a necesitat solicitarea unor competenţe pentru realizarea acestora, proces care a îngreunat implementarea obiectivelor şi realizarea activităţilor. În alte cazuri, activităţile de realizat nu au fost comunicate obiectiv salariaţilor, respectiv obiectivele individuale au rămas aceleaşi, în condiţiile în care obiectivele cuprinse în planul compartimentului au fost cu totul altele. Aceasta a însemnat stabilirea măsurilor în cursul anului, instruirea, sub diferite forme, a personalului pentru înţelegerea acestora şi stabilirea priorităţilor de implementare, ceea ce a condus la întârzieri în atingerea unor obiective ale planului. Nevoia de îmbunătăţire a nivelului de competenţă în raport cu progresele tehnico-

	informaţionale şi organizatorice, pentru creşterea eficienţei şi reducerea costurilor, a presupus definirea în cadrul planului anual, a unor asemenea obiective şi activităţi, însă pentru implementarea acestora nu a fost corelat necesarul de mijloace şi echipamente cu necesităţile pentru atingerea obiectivelor planului. În cadrul planului, reducerea costurilor a fost definită şi prin reducerea personalului, prin care s-au pierdut o serie de competenţe care, din motive financiare, nu au mai putut fi înlocuite, ceea ce a condus la realizarea activităţilor, fără a fi îndeplinite condiţiile de performanţă stabilite. Monitorizarea resurselor financiare utilizate în derularea obiectivelor planului anual a fost de multe ori deficitară, ceea ce a contribuit la majorarea costurilor . În cadrul entităţii nu a fost comunicată eficient şi nu a fost conştientizată nevoia de cunoaştere a normelor, legislaţiei şi metodologiei în domeniile de activitate, importanţa obiectivelor stabilite spre îndeplinire şi modul cum acestea contribuie la atingerea obiectivelor generale şi a obiectivelor strategice. Activităţile considerate prioritare ale planului anual nu au fost realizate sau implementate corespunzător, deoarece nu s-au reanalizat şi repartizat atribuţiile compartimentelor pentru a asigura competenţa necesară realizării obiectivelor şi activităţilor stabilite în cadrul planului. De asemenea, nu au fost stabilite şi comunicate salariaţilor obiectivele individuale care să derive din noile obiective stabilite în cadrul planului de activitate şi care se aflau în competenţa compartimentului funcţional. În cadrul planului anual nu au fost definite obiective şi activităţi care să asigure nevoia de îmbunătăţire a nivelului de competenţă în raport cu progresele tehnico-informaţionale şi organizatorice, creşterea eficienţei şi reducerea costurilor, prin corelarea necesarului de echipamente cu necesităţile de atingere a obiectivelor planului. S-a constatat monitorizarea deficitară a resurselor financiare utilizate în derularea obiectivelor planului anual, ceea ce a dus la costuri suplimentare faţă de cele planificate pentru implementarea obiectivelor stabilite.
Concluzii	Necorelarea atribuţiilor compartimentelor în vederea organizării şi asigurării competenţelor necesare realizării noilor obiective şi activităţi stabilite. Necunoaşterea de către toţi salariaţii a structurii planului anual de activitate, ceea ce nu a asigurat implicarea acestora în implementarea obiectivelor. Neasigurarea în totalitate a necesarului de mijloace pentru realizarea planului, respectiv nu a existat un echilibru între necesităţile de realizare a planului şi necesarul de echipamente. Depăşirea costurilor planificate în realizarea şi implementarea obiectivelor. Performanţele stabilite în realizarea activităţilor nu au fost atinse în toate cazurile.

Auditor intern,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern

INTERVIU nr. 1.3
privind fundamentarea resurselor pentru asigurarea implementării planului de activitate, adresat Domnului Popescu Valentin – Şef serviciu Dezvoltare Aplicaţii

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Nr. crt.	ÎNTREBĂRI	DA	NU	OBSERVAŢII
1.	Există un plan de activitate elaborat?	X		
2.	Planul de activitate este elaborat pe domenii de activitate?	X		
3.	La elaborarea planului de activitate s-a realizat o analiză SWOT a domeniilor de activitate?	X		
4.	Planul de activitate este corelat cu posibilităţile materiale, financiare şi umane existente în cadrul organizaţiei?	X		
5.	Planul de activitate a fost adus la cunoştinţa şi este cunoscut de salariaţii implicaţi în realizarea lui?	X		
6.	Politicile şi strategiile elaborate în cadrul organizaţiei şi care asigură implementarea şi realizarea planului de activitate, inclusiv metodologiile interne de lucru sunt cunoscute de salariaţi?	X	X x	*Nu este realizată o analiză a comportamentului salariaţilor cu privire la ţintele şi indicatorii planului*
7.	Atribuţiile definite compartimentelor s-a realizat în corelaţie cu activităţile şi sarcinile repartizate acestora?		X	*Unele activităţi nu au fost implementate corespunzător*
8.	Pentru realizarea activităţilor în cadrul compartimentelor au existat competenţele necesare?	X		
9.	Activităţile au fost comunicate corespunzător salariaţilor prin atribuirea de obiective individuale corespunzătoare?		X	Realizarea cu întârziere a activităţilor
10.	Monitorizarea realizării activităţilor planificate s-a realizat corespunzător, pe niveluri de responsabilităţi?	X		
11.	Personalul implicat în realizarea obiectivelor şi activităţile planificate a deţinut cunoştinţele necesare realizării acestora ?		X	Depăşirea costurilor planificate în realizarea obiectivelor
12.	Pentru realizarea activităţilor au fost asigurate echipamentele şi tehnologiile necesare ?		X	Nu a existat echilibru între necesităţile planului şi necesarul de echipamente

Data: 13.09.2009

Şef serviciu Dezvoltare aplicaţii,
Popescu Valentin

Elaborat în prezenţa noastră: Auditori
Popescu Sorin
Radu George

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 1.4

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 13.09.2009
Avizat: Dumitru Daniel Data: 13.09.2009

Problema	Resursele nu sunt fundamentate corect în vederea implementării planului anual de activitate;
Constatarea	Din analiză s-a constatat că eforturile pentru elaborarea planului anual de activitate implică alocarea de fonduri şi resurse ridicate din partea organizaţiei care, în cele mai multe din cazuri, nu au ca referinţă atingerea scopului fundamental al acesteia. În acelaşi timp, activităţile considerate prioritare ale planului anual nu au fost realizate sau implementate în totalitate, în mod corespunzător, deoarece nu au fost reanalizate şi repartizate atribuţiile în cadrul compartimentelor în corelaţie cu noile obiective şi activităţi stabilite în cadrul planului. Aceasta a însemnat că, în unele cazuri, obiectivele şi activităţile deşi erau cunoscute de personal, acesta nu avea competenţa necesară, în special a celor care erau realizate în colaborare cu alte structuri funcţionale, ceea ce a necesitat solicitarea unor competenţe pentru realizarea acestora, proces care a îngreunat implementarea obiectivelor şi realizarea activităţilor. În alte cazuri, activităţile nu au fost comunicate salariaţilor, respectiv obiectivele individuale au rămas aceleaşi, în condiţiile în care obiectivele cuprinse în planul compartimentului au fost cu totul altele. Aceasta a însemnat stabilirea măsurilor în cursul anului, instruirea, sub diferite forme, a personalului pentru înţelegerea acestora şi stabilirea priorităţilor de implementare, ceea ce a condus la întârzieri în atingerea unor obiective ale planului. Nevoia de îmbunătăţire a nivelului de competenţă în raport cu progresele tehnico-informaţionale şi organizatorice, pentru creşterea eficienţei şi reducerea costurilor, a presupus definirea în cadrul planului anual a unor asemenea obiective şi activităţi, însă pentru implementarea acestora nu a fost corelat necesarul de mijloace şi echipamente cu necesităţile pentru atingerea obiectivelor planului. În cadrul planului reducerea costurilor a fost definită şi prin reducerea personalului, prin care s-au pierdut o serie de competenţe care, din motive financiare, nu au fost înlocuite, prin dezvoltarea altor angajaţi, ceea ce a condus la realizarea activităţilor, dar nu au fost atinse condiţiile de performanţă stabilite. Monitorizarea resursele financiare utilizate în derulare obiectivelor planului anual a fost de multe ori deficitară, ceea ce a contribuit la realizarea de costuri suplimentare faţă de cele planificate pentru implementarea obiectivelor stabilite. În cadrul entităţii nu a fost comunicată eficient şi nu a fost conştientizată nevoia de cunoaştere a normelor, legislaţiei şi metodologiei în domeniile de activitate, a diferitelor culturi din cadrul organizaţiei, importanţa obiectivelor stabilite spre îndeplinire şi modul cum acestea contribuie la atingerea obiectivelor generale şi a obiectivelor strategice, şi înţelegerea comportamentului competitiv ca un sistem în care oamenii şi resursele interacţionează continuu. Activităţile considerate prioritare ale planului anual nu au fost realizate sau implementate corespunzător deoarece nu s-au reanalizat şi repartizat atribuţiile compartimentelor pentru a asigura competenţa necesară realizării obiectivelor şi activităţilor stabilite în cadrul planului. De asemenea, nu au fost stabilite şi comunicate salariaţilor obiectivele individuale care derivă din noile obiective stabilite în cadrul planului de activitate şi care se aflau în

	competenţa compartimentului funcţional. Definirea în cadrul planului anual a obiectivelor şi activităţilor s-a realizat fără să se asigure: nevoia de îmbunătăţire a nivelului de competenţă în raport cu progresele tehnico-informaţionale şi organizatorice;creşterea eficienţei şi reducerea costurilor; corelarea necesarul de echipamente cu necesităţile de atingere a obiectivelor planului.
Cauza	Inexistenţa unui sistem de reglementare şi monitorizare a instruirii personalului, la nivelul structurilor funcţionale, prin care să se asigure comunicarea clară a sarcinilor de realizat, a instrumentelor de aplicat şi urmărirea utilizării acestora. Inexistenţa programelor de formare care se bazează pe dezvoltarea aptitudinilor de cercetare-analiză-diagnoză, pe cultivarea capacităţii de asumare a responsabilităţilor de a decide sau de a conduce activitatea unui grup. Atitudinea faţă de sarcini şi responsabilităţi nu este întotdeauna pozitivă, iar politica de cointeresare este slabă.
Consecinţa	Planurile anuale de activitate nu sunt îndeplinite în condiţii de performanţă, iar indicatorii de impact sau rezultat ataşaţi obiectivelor nu sunt realizaţi în condiţii de eficienţă, economicitate şi eficacitate.
Recomandarea	Dezvoltarea unui sistem de instruire şi pregătire a salariaţilor astfel încât metodologia specifică domeniului de activitate, normativă şi procedurală, să fie aplicată corespunzător pentru dezvoltarea şi implementarea planurilor anuale. În baza planurilor elaborate să se identifice toate atribuţiile necesare pentru atingerea obiectivelor stabilite, iar acestea să fie repartizate corespunzător în cadrul compartimentelor. Promovarea dezvoltării resurselor umane pentru a obţine competenţele necesare creşterii economice în condiţiile în care au loc reduceri de personal. Evaluarea cuprinzătoare a resurselor (financiare, instituţionale, programe, personal) necesare implementării planurilor anuale de activitate şi monitorizarea eficientă pentru a se asigura încadrarea în limitele stabilite.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Radu George	Dumitru Daniel	Structură auditată

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 1.5

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 13.09.2009
Avizat: Dumitru Daniel Data: 13.09.2009

Obiectul testului	Planurile IT oferă asigurare cu privire la faptul că nevoile IT sunt alocate în concordanţă cu necesităţile
Obiectivele testului	Implementarea subsistemele IT pentru funcţii principale stabilite urmare direcţiilor de dezvoltare ale organizaţiei.
Descrierea testului	Populaţia statistică a fost constituită din cele trei de funcţii principale nou-create la nivelul entităţii publice în baza recomandărilor Comisiei Europene, identificate ca urmare a analizei modificărilor operate în organigramă la data elaborării planului strategic. Eşantionul pentru realizarea testării situaţiei subsistemelor IT pentru funcţiile principale a fost constituit din cele trei funcţii identificate. Testarea a constat în examinarea următoarelor elemente: - examinarea dacă subsistemele IT acoperă în totalitate nevoile pentru funcţiile principale ale entităţii publice - analiza dacă nevoile de subsisteme IT pentru funcţiile principale nou-create au fost acoperite - verificarea dacă departamentele înfiinţate ca urmare a funcţiilor principale nou-create au fost solicitate să-şi exprime cerinţele specifice privind realizarea unor subsisteme IT proprii activităţii lor - analiza procedurile pe baza cărora se realizează subsistemele IT şi stabilirea dacă acestea sunt suficiente pentru implementarea acestor subsisteme în condiţii optime Testarea s-a concretizat în elaborarea unei *Liste de control privind analiza subsistemelor IT pentru funcţiile principale nou-create*.
Constatări	Din analiza efectuată s-a constatat că în cadrul entităţii publice există structuri nou-înfiinţate, ca urmare a schimbărilor legislative apărute, pentru care nu s-au realizat aplicaţii informatice specifice, respectiv *Autoritatea de Management a Fondurilor Structurale, Autoritatea de Management a Fondurilor de Coeziune, Autoritatea competentă pentru acreditarea agenţiilor de plată*. În acelaşi timp, există şi o structură nou înfiinţată – *Autoritatea de Management a Fondurilor de Coeziune* – care a notificat departamentul IT, dar implementarea nu s-a realizat în termen.
Concluzii	Nu există aplicaţii informatice implementate la nivelul tuturor structurilor funcţionale din cadrul entităţii

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern

INTERVIU nr. 1.4
privind subsistemele IT pentru funcţiile principale
adresat
domnului Ionescu Adrian, Director General

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Nr. crt.	Întrebări	Da	Nu	Observaţii
1.	Planul strategic prevede elaborarea de subsisteme IT pentru funcţiile principale?	X		
2.	Au fost elaborate subsisteme IT pentru toate funcţiile principale?		X	Procesul de elaborare a subsistemelor IT este încă în derulare.
3.	Procesul de elaborare a subsistemelor IT pentru funcţiile principale este procedurat?	X		Prin planul strategic au fost stabilite termene de realizare a subsistemelor IT.
4.	Au fost elaborate subsisteme IT pentru funcţii principale apărute la solicitarea Comisiei Europene sau ca urmare a schimbărilor legislative apărute în România?		X	Resursele umane de care dispunem sunt implicate în elaborarea subsistemelor IT prevăzute prin planul strategic defalcat în planuri anuale. Până în prezent planul strategic iniţial nu a fost modificat.
5.	A fost efectuată periodic (trimestrial, anual) o analiză a nevoilor de subsisteme IT la nivelul funcţiilor principale nou-create?		X	Realizarea acestei analize nu este în sfera de competenţe a conducătorului departamentului IT
6.	Sunt corelate termenelor de realizare a subsistemelor IT?	X		Da, prin planul strategic.
7.	Au fost realizate subsistemele IT la termenele prevăzute?		X	S-au înregistrat întârzieri în realizarea subsistemelor IT
8.	Au fost previzionate resursele necesare pentru elaborarea subsistemelor IT?	X		Departamentul IT asigură resursele umane necesare pentru elaborarea subsistemelor IT.

Data: 13.09.2009

Intervievat,
Director general, Ionescu Adrian

Elaborat în prezenţa noastră: Auditori
Popescu Sorin
Radu George

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 1.5

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 13.09.2009
Avizat: Dumitru Daniel Data: 13.09.2009

Problema	Unele departamente din cadrul entităţii nu dispun de subsisteme IT specifice activităţilor care se desfăşoară în cadrul acestora.
Constatarea	Din analiză s-a constatat că în cadrul entităţii publice există structuri nou-înfiinţate ca urmare a recomandărilor Comisiei Europene şi a schimbărilor legislative, care nu au notificat departamentul IT în privinţa nevoilor lor de aplicaţii informatice specifice. În acelaşi timp, s-au constatat şi departamente nou înfiinţate care şi-au exprimat nevoile pentru realizarea subsistemelor IT specifice activităţii lor, dar care nu au beneficiat de implementarea acestora, conform planificării, datorită întârzierilor în realizarea achiziţiilor.
Cauza	Inexistenţa la nivelul entităţii publice a unor proceduri complete de elaborare a strategiei IT care să permită actualizarea sistematica, funcţie de schimbările legislative; Insuficienţa personalului de specialitate.
Consecinţa	Domenii importante de activitate ale entităţii publice pentru care nu s-a realizat implementarea subsistemelor IT necesare pentru desfăşurarea activităţii au randamente scăzute, ceea ce afectează pe ansamblul realizarea activităţilor entităţii publice
Recomandarea	Coroborarea atribuţiilor prezentate prin proceduri cu cele stabilite prin fişele posturilor; Inventarierea stadiului implementării subsistemelor IT la nivelul departamentelor entităţii publice şi stabilirea necesităţilor IT care trebuie incluse în strategia IT.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Popescu Sorin	Dumitru Daniel	Structură auditată

ENTITATEA PUBLICĂ
Serviciul Audit Intern

LISTA DE VERIFICARE nr. 2

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Obiectivul I.
ORGANIZAREA ŞI FUNCŢIONAREA DEPARTAMENTULUI IT

Nr. crt.	Activitatea de audit	Da	Nu	Observaţii
A	**Definirea atribuţiilor şi activităţilor**			
1.	**Definirea atribuţiilor şi responsabilităţilor în cadrul departamentului IT**			
1.1.	Funcţionalitatea procedurilor de lucru în corelaţie cu activităţile derulate	X		
1.2.	Verificarea gradului de acoperire prin procedură a activităţilor privind organizarea şi definirea structurilor organizatorice.	X		
1.3.	Verificarea concordanţei atribuţiilor stabilite Departamentului IT cu cele ale organizaţiei			
1.4.	Verificarea definirii clare a atribuţiilor pe compartimentele funcţionale ale Departamentului IT			
1.5.	Verificarea definirii activităţilor ce trebuie realizate în cadrul Departamentului IT			
1.6.	Examinarea constituirii structurii funcţionale de IT			
1.7.	Analiza criteriilor avute în vedere la crearea compartimentelor funcţionale ale structurii organizatorice;			
1.8.	Înglobarea activităţilor de control intern în punctele cheie de realizare a activităţilor			
1.9.	Atribuţiile sunt stabilite urmare a evaluării posturilor;			
1.10.	Verificaţi dacă definirea atribuţiilor ţine cont de reglementările legale aplicabile;			
1.11.	Verificaţi dacă atribuţiile executate în cadrul compartimentului IT sunt în responsabilitatea acestui compartiment;			
1.12.	Verificaţi dacă responsabilităţile sunt delimitate clar de atribuţii şi competenţe;			
1.13.	Verificaţi dacă sunt definite atribuţiile şi aria de competenţă			Test nr. 2.1 FIAP nr. 2.1
1.14.	Verificaţi dacă aria de competenţă asigură realizarea activităţilor şi acţiunilor stabilite			
1.15.	Verificaţi dacă relaţiile cu celelalte posturi din cadrul compartimentului cu care ar trebui să aibă relaţii funcţionale sunt clar definite			
1.16.	Verificaţi dacă definirea atribuţiilor ţine cont de obiectivele generale şi specifice;			
2.	**Definirea activităţilor în cadrul structurii organizatorice**			
2.1.	Verificaţi dacă activităţile sunt identificate la nivelul departamentului IT;	X		
2.2.	Verificaţi dacă activităţile sunt definite omogen în cadrul structurii funcţionale	X		
2.3.	Verificaţi dacă atribuţiile specifice care asigură realizarea activităţilor sunt definite în cadrul atribuţiilor generale ale organizaţiei;	X		
2.4.	Verificaţi dacă activităţile repartizate în cadrul compartimentelor			

	respectă criteriile avute în vedere la înfiinţarea acestora, respectiv există atribuţii definite pentru realizarea lor;			
2.5.	Analizaţi dacă acţiunile efectuate pentru realizarea activităţilor se regăsesc în sarcinile definite la nivelul posturilor;			
2.6.	Verificaţi dacă la realizarea unei activităţi contribuie un singur compartiment;			
2.7.	Verificaţi dacă la repartizarea activităţilor pe compartimente se ţine seama de rolul acestora;			
2.8.	Verificaţi dacă atribuţiile stabilite pentru realizarea activităţii asigură competenţa necesară pentru realizarea acesteia;			
2.9.	Verificaţi dacă pentru fiecare activitate sunt stabilite acţiunile necesare;			
2,10.	Verificate dacă pentru fiecare acţiune stabilită există sarcină definită în fişa postului;			
2.11.	Verificaţi dacă personalul are calificarea necesară pentru realizarea activităţilor;			
2.12.	Verificaţi dacă pentru activităţile identificate există competenţa alocată în vederea realizării lor;			
2.13.	Verificaţi dacă activităţile identificate şi alocate obiectivelor asigură realizarea acestora şi obţinerea rezultatelor aşteptate;			
2.14.	Verificaţi dacă activităţile repartizate în cadrul compartimentelor respectă criteriile avute în vedere la înfiinţarea acestora;			Test nr. 2.2. Interviu nr. 2.1. Notă de relaţii nr. 2.1. FIAP nr. 2.2.
	a) definirea omogenă a activităţilor			
	b) activităţile repartizate în cadrul compartimentelor respectă criteriile avute în vedere la înfiinţarea acestora			
	c) atribuţiile stabilite pentru realizarea activităţilor definesc aria necesară realizării activităţilor			
	d) acţiunile stabilite în realizarea activităţilor se regăsesc în sarcinile definite la nivelul posturilor;			
2.15.	Verificaţi dacă personalul are calificarea adecvată pentru realizarea activităţilor;			
B.	**Stabilirea structurii organizatorice**			
1.	**Organizarea funcţională a departamentului IT**			
1.1.	Verificaţi modul de elaborare şi funcţionalitatea organigramei departamentului IT;			
	a) stabilirea structurii funcţionale a departamentului, pe baza organigramei			
	b) organigrama permite vizualizarea de ansamblu a organizării departamentului	X		Test nr. 2.3 FIAP nr. 2.3
	c) definirea în termen a relaţiilor din cadrul departamentului			
	d) definirea raporturilor de subordonare în cadrul organigramei			
	e) definirea numărului de posturi prin intermediul organigramei			
1.2.	Elaborarea organigramei în consens cu structura organizatorică;	X		
1.3.	Constituirea compartimentelor a avut în vedere natura activităţilor;	X		
1.4.	Verificarea aprobării organigramei de către persoanele competente;	X		
1.5.	Examinarea organigramei departamentului IT;	X		
1.6.	Evaluaţi demersurile realizate de departamentul IT pentru ocuparea posturilor de conducere;			
1.7.	Analizaţi consecinţele funcţionării departamentului IT prin delegarea persoanelor de conducere;		X	Test nr. 2.4 Lista de control 2.1 FIAP nr. 2.4
1.8.	Verificaţi dacă organigrama departamentului IT asigură:			
	a) numărul total de posturi de conducere			
	b) numărul total de posturi de conducere ocupate cu delegaţie			
	c) numărul de posturi de execuţie			
	d) numărul de posturi de execuţie neocupate			
1.9.	Verificaţi dacă demersurile efectuate pentru ocuparea posturilor de conducere:			
	a) numărul de concursuri organizate			
	b) numărul de solicitări către departamentul de resurse umane în vederea organizării concursurilor			
1.10.	Verificaţi dacă conducerea a avut preocupări pentru ocuparea posturilor de execuţie			
	a) numărul de concursuri organizate			

	b) numărul de solicitări către departamentul de resurse umane în vederea organizării concursurilor			
1.11.	Verificaţi existenţa un ui plan de implementare a măsurilor necesare, menit să asigure buna desfăşurare a activităţii în cazul existenţei unui număr mare de posturi vacante			
1.8.	Evaluaţi preocuparea conducerii pentru ocuparea posturilor de execuţie;	X		
1.9.	Existenţa unui plan de implementare a măsurilor necesare menite să asigure buna desfăşurare a activităţii în cazul existenţei unui număr mare de posturi vacante;	X		
1.10.	Analizaţi dotarea departamentului cu echipamente hard şi soft adecvate pentru desfăşurarea activităţilor specifice, astfel:	X		
	a) număr suficient de calculatoare dotate corespunzător;			
	b) număr suficient de servere;			
	c) număr suficient de echipamente auxiliare (imprimante, xerox-uri, scanere, conexiuni la intranet/Internet);			
	- programe IT adecvate.			
1.11.	Verificaţi dacă exista responsabil monitorizarea stadiului şi modului de realizare a obiectivelor generale şi specifice ale departamentului;	X		
1.12.	Verificarea limitelor decizionale stabilite în derularea şi realizarea activităţilor;	X		
1.13.	Examinarea modului de analiză a posturilor şi de definire a sarcinilor pe posturi;	X		
1.14.	Analiza modului de specializarea a posturilor în corelaţie cu tipul de activităţi ce sunt realizate	X		
1.15.	Verificaţi dacă elaborarea organigramei este realizată în consens cu structura organizatorică;	X		
1.16.	Verificaţi dacă posturile atribuite compartimentelor asigură realizarea activităţilor repartizate;	X		
1.17.	Verificaţi dacă sistemul informaţional este proiectat în conformitate cu strategia;	X		
1.18.	Verificaţi dacă sunt stabilite circuitele informaţionale;	X		
1.19.	Analizaţi dacă mijloacele de realizare a circuitelor informaţionale sunt definite şi cunoscute;	X		
1.20.	Verificaţi dacă sistemul informaţional este operaţional şi este folosit eficient şi eficace;	X		
1.21.	Verificaţi dacă tehnologiile informaţionale sunt folosite şi exploatate:	X		
	Internetul			
	E-mail-ul			
	Intranetul			
1.22.	Verificaţi dacă oportunitatea, calitatea şi cantitatea informaţiilor este bine precizată;	X		
1.23.	Verificaţi dacă organigrama stabileşte responsabilii structurilor funcţionale corespunzător fiecărui nivel ierarhic;	X		
1.24.	Analizaţi dacă organigrama stabileşte autoritatea de care responsabili structurilor funcţionale dispun.	X		
2.	**Examinarea sistemului de gestionare a riscurilor generale la nivelul departamentului IT**			
2.1.	Verificarea existenţei politicii unitare privind gestionarea riscurilor	X		
2.2.	Verificarea existenţei sistemului de evaluare a riscurilor	X		
2.3.	Verificaţi dacă pentru riscurile identificate sunt stabilite şi funcţionează controale interne			Test nr. 2.5 Interviu 2.2 FIAP nr. 2.5
2.4.	Verificaţi modalitatea de stabilire şi introducere a instrumentelor de control pentru menţinerea lor în limita de acceptare şi dacă acestea menţin riscurile la niveluri inferioare			
2.5.	Analizaţi dacă există un responsabil cu gestionarea riscurilor la nivelul departamentului IT	X		
2.6.	Verificarea existenţei Registrului riscurilor la nivelul Departamentului IT	X		
2.7.	Verificaţi dacă actualizarea Registrului riscurilor se realizează sistematic	X		
2.8.	Verificaţi dacă riscurile majore prezentate în Registrul riscurilor elaborat la nivelul Direcţiei IT se regăsesc în Registrul riscurilor	X		

	elaborat la nivelul întregii entităţi publice;			
2.9.	Verificaţi dacă există un proces formal de analiză a riscurilor, utilizat înainte de introducerea şi ameliorarea noilor sisteme şi pregătirea unor planuri realiste de menţinere a serviciilor în cazul în care operaţiunile nu decurg aşa cum au fost proiectate.	X		
2.10.	Examinaţi dacă se realizează monitorizarea şi administrarea riguroasă a riscurilor care privesc implementarea aplicaţiilor	X		
2.11.	Analizaţi dacă implementarea controlului intern a urmărit dacă acesta este proiectat, implementat şi menţinut pentru a aborda riscurile care ameninţă atingerea oricăruia dintre obiectivele departamentului cu privire la:		X	Test. nr. 2.6 FIAP nr. 2.6
	a) credibilitatea raportării financiare			
	b) eficienţa şi eficacitatea operaţiilor sale			
	c) respectarea legilor şi reglementărilor aplicabile			
2.12.	Verificaţi dacă riscurile sunt clar identificate şi delimitate pe programe;	X		
2.13.	Verificaţi dacă riscurile sunt tratate ca responsabilitate a conducerii superioare, dat fiind impactul potenţial al acestora asupra proiectului şi utilizării resurselor;	X		
2.14.	Evaluaţi dacă probabilitatea şi impactul riscurilor sunt analizate separat şi sunt numite persoane care răspund de reducerea acestora;	X		
2.15.	Verificaţi dacă revizuirea planurilor de diminuare şi de gestionare a riscurilor se realizează în mod regulat;	X		
2.16.	Examinaţi dacă un risc identificat este raportat conducerii superioare şi sunt dispuse măsuri de control intern pentru menţinerea acestuia în limite acceptabile;	X		
2.17.	Verificaţi dacă criteriile de performanţă sunt utilizate corect în procesele informaţionale;	X		
2.18.	Analizaţi dacă aprecierea criteriilor de performanţă are la bază capacităţile şi abilităţile demonstrate de salariaţi;	X		
2.19.	Verificaţi dacă procesul decizional este implementat la toate nivelurile ierarhice;	X		
2.20	Analizaţi dacă structura compartimentala este corect stabilită în funcţie de natura şi omogenitatea activităţilor;	X		
C.	**Stabilirea responsabilităţilor**			
1.	**Definirea sarcinilor prin fişa postului**			
1.1.	Verificaţi dacă elaborarea fişei postului este realizată în corelaţie cu cerinţele postului;	X		
1.2.	Verificaţi dacă sunt definite responsabilităţi în realizarea sarcinilor din fişa postului;	X		
1.3.	Verificaţi dacă fişa postului defineşte corect cunoştinţele IT necesare ocupării postului;	X		
1.4.	Verificaţi dacă este asigurată continuitatea realizării activităţilor la eliberarea postului;	X		
1.5.	Abilităţile, cunoştinţele şi aptitudinile definite posturilor asigură realizarea activităţilor repartizate şi a celor stabilite departamentului;	X		
1.6.	Verificaţi dacă la definirea obiectivelor şi sarcinilor se urmăreşte şi dezvoltarea capacităţii profesionale a salariatului;	X		
1.7.	Verificaţi dacă stabilirea obiectivelor individuale este realizată în corelaţie cu obiectivele departamentului;	X		
1.8.	Verificaţi dacă persoana care ocupă postul are capacitatea de a asigura îndeplinirea atribuţiilor şi sarcinilor stabilite;	X		
1.9.	Verificaţi dacă atribuţiile definite în fişa postului au caracter individual	X		
1.10.	Verificaţi dacă stabilirea sarcinilor din fişa postului este realizată în concordanţă cu atribuţiile din ROF;	X		
1.11.	Analizaţi modul de definire a competenţelor manageriale;	X		
1.12.	Examinarea stabilirii sarcinilor în corelaţie cu gradul profesional pe care îl defineşte postul;	X		
1.13.	Verificaţi dacă atribuţiile definite în fişa postului sunt în concordanţă cu activităţile efectiv realizate de persoana ocupantă a postului;	X		
1.14.	Urmărirea alocării sarcinilor în fişa postului în concordanţă cu competenţele manageriale:	X		
1.15.	a) modul de definire pentru funcţiile de execuţie;	X		

	b) modul de definire pentru funcţiile de conducere;	X		
1.16.	Analizaţi dacă fişa postului defineşte:			Test nr. 2.7 Interviu 2.3 Notă de relaţii nr. 2.1 FIAP nr. 2.7
	a) condiţiile privind studiile de specialitate			
	b) condiţiile privind specializările necesare pentru ocuparea postului			
	c) condiţiile privind cunoştinţele informatice		X	
	d) definirea sarcinilor în funcţie de nivelul postului			
	e) alocarea sarcinilor în concordanţă cu competenţele manageriale necesare postului			
1.17.	Verificarea definirii sarcinilor în conformitate cu activităţile derulate;	X		
1.18.	Verificaţi dacă atribuţiile sunt definite astfel încât să asigure aria de competenţă necesară realizării activităţilor, respectiv:			Test nr. 2.8 FIAP nr. 2.8
	a) analiza atribuţiilor stabilite compartimentului şi stabilirea dacă aria de competenţă a acestora ajută la realizarea activităţilor			
	b) urmărirea ca aria de competenţă să asigure realizarea activităţilor şi acţiunilor stabilite compartimentului funcţional		X	
	c) analiza relaţiilor cu celelalte structuri funcţionale din cadrul organizaţiei cu care are sau ar trebui să aibă relaţii funcţionale pentru realizarea atribuţiilor şi activităţilor			

Auditori,

Popescu Sorin
Radu George

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 2.1.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Obiectul testului	Definirea atribuţiilor şi responsabilităţilor în cadrul Departamentului IT
Obiectivele testului	Evaluarea şi urmărirea dacă atribuţiile stabilite personalului definesc aria de competenţă necesară realizării activităţilor şi acţiunilor;
Descrierea testului	Eşantionul s-a constituit prin selectarea a câte două posturi din cadrul fiecărui compartiment funcţional al Departamentului IT, respectiv un număr de 6 posturi. In cazul acestora se vor evalua atribuţiile şi relaţiile funcţionale definite cu privire la: - definirea atribuţiilor şi a ariei de competenţă a acestora; - urmărirea dacă aria de competenţă asigură realizarea activităţilor şi acţiunilor stabilite; - analiza relaţiilor cu celelalte posturi din cadrul compartimentului cu care ar trebui să aibă relaţii funcţionale.
Constatări	Atribuţiile definite în sarcina salariaţilor nu sunt întotdeauna conforme şi nu asigură competenţa de realizare a activităţilor şi acţiunilor, acestea fiind definite în multe cazuri la modul general, nu indică, prin modul de formulare o acţiune, nu asigură un conţinut clar, fiind definite sub forma unei relaţii funcţionale sau având caracter de activitate.
Concluzii	Atribuţiile stabilite salariaţilor nu asigură întotdeauna aria de competenţă necesară pentru realizarea activităţilor.

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 2.1.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 13.09.2009
Avizat: Dumitru Daniel Data: 13.09.2009

Problema	Atribuţiile stabilite pentru posturile din cadrul Departamentului IT nu asigură întotdeauna aria de competenţă privind realizarea activităţilor şi acţiunilor repartizate.
Constatarea	Atribuţiile definite in sarcina salariaţilor nu sunt întotdeauna conforme şi nu asigură competenţa de realizare a activităţilor şi acţiunilor, acestea fiind definite în multe cazuri la modul general, nu indică, prin modul de formulare o acţiune, nu asigură un conţinut clar, fiind definite sub forma unei relaţii funcţionale sau având caracter de activitate.
Cauza	Definirea atribuţiilor specifice postului s-a realizat de către fiecare şef de compartiment, fără a mai fi analizate şi evaluate de către persoanele responsabile de la nivelul departamentului. Persoanele din cadrul compartimentelor funcţionale nu au dispus de cunoştinţele necesare astfel încât să poată defini corect o atribuţie şi în acelaşi timp să urmărească daca acestea asigură aria de competenţă a realizării activităţilor repartizate postului.
Consecinţa	Nu se asigură o arie de competenţă necesară şi suficientă pentru realizarea activităţilor şi acţiunilor.
Recomandarea	Conştientizarea managementului responsabil cu procesul de stabilire şi definire a atribuţiilor prin informări şi consilieri pentru clarificarea modalităţilor practice de definire a unei atribuţii sau unui set de atribuţii pentru asigurarea ariei de competenţă necesară pentru realizarea activităţilor.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Popescu Sorin	Dumitru Daniel	Structură auditată

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 2.2.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Obiectul testului	Definirea activităţilor în cadrul structurii organizatorice.
Obiectivele testului	Delimitarea activităţilor compartimentului pe posturi.
Descrierea testului	Populaţia eşantionată o reprezintă activităţile şi atribuţiile alocate şi stabilite pentru două servicii din cadrul departamentului IT, respectiv serviciul responsabil de întreţinerea şi implementarea aplicaţiilor şi serviciul responsabil cu programarea în cadrul organizaţiei. Criteriile avute în vedere la analiza şi evaluarea activităţilor sunt reprezentate de cele definite în *Lista de verificare*, şi anume: – definirea omogenă a activităţilor; – activităţile repartizate în cadrul compartimentelor respectă criteriile avute în vedere la înfiinţarea acestora; – atribuţiile stabilite pentru realizarea activităţilor definesc aria necesară; – acţiunile necesare realizării activităţilor se regăsesc în sarcinile definite în fişa postului. Pentru realizarea testului a fost realizat un interviu *privind modul de stabilire a activităţilor în cadrul compartimentului*, cu domnul Ionescu Adrian director general Departament IT şi a fost luată o notă de relaţii domnului Popescu Marin, şef serviciu Întreţinere şi Implementare Aplicaţii.
Constatări	La proiectarea structurii organizatorice se pleacă de la inventarierea activităţilor existente sau necesare pentru realizarea obiectivelor şi se efectuează o analiză critică pentru a se putea constata în ce măsură acestea sunt adecvate realizării funcţiunii. La definirea activităţilor se are în vedere complexitatea acestora, respectiv gradul de diferenţiere a muncii pe orizontală şi pe verticală. Diferenţierea pe orizontală constă în numărul de activităţi (specializări) şi de subunităţi funcţionale (birouri, servicii). Diferenţierea pe verticală se referă la numărul de niveluri ierarhice de-a lungul cărora se exercită autoritatea în organizaţie. Analiza conţinutului şi modului de definire a activităţilor necesare pentru realizarea fiecărui obiectiv specific a pus în evidenţă următoarele: – unele activităţi sunt definite sub forma unor relaţii de colaborare care fie nu indică acţiuni concrete de realizare a acestora, fie indică o acţiune comună de realizare; – altele sunt definite sub forma unor relaţii de colaborare, în condiţiile în care sunt exercitate acţiuni concrete de realizare şi pentru care există rezultate aşteptate stabilite; – nu sunt identificate toate activităţile care contribuie la realizarea obiectivelor specifice şi care asigură conformitatea cu reglementărilor legale. Prin modul de organizare a activităţilor structurilor organizatorice ale direcţiei nu se asigură evitarea dublării acţiunilor, respectiv există activităţi identice sau similare, desfăşurate de mai multe departamente şi probleme semnificative de

	suprapunere şi coordonare. De asemenea, pentru realizarea unor activităţi nu se respectă principiul convergenţei în definirea şi stabilirea conţinutului activităţilor care sunt necesare pentru realizarea unui obiectiv.
Concluzii	Activităţile nu sunt corect identificate şi definite în cadrul compartimentelor, astfel încât să contribuie la realizarea şi implementarea obiectivelor.

Auditor intern,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern

INTERVIU NR. 2.1
privind definirea activităţilor şi responsabilităţilor în cadrul departamentului IT, adresat domnului Adrian Ionescu, director general DGTI

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Nr. crt.	*Întrebări*	Da	Nu	Observaţii
1.	Aveţi o strategie de dezvoltare la nivelul structurii funcţionale?	X		
2.	Există un responsabil cu actualizarea strategiei în cadrul compartimentului IT?	X		
3.	Strategia de dezvoltare a compartimentului IT este în concordanţă cu strategia generală a organizaţiei?	X		
4.	Aţi aprobat un plan de activitate anual pentru compartimentul IT?	X		
5.	Aţi dezvoltat politici publice în domeniul IT pentru asigurarea atingerii obiectivelor stabilite prin plan?	X		
6.	Există proceduri operaţionale de lucru pentru toate activităţile care se desfăşoară în cadrul compartimentului?	X		Da, au fost elaborate proceduri operaţionale de lucru, sunt cunoscute şi însuşite de către salariaţi
7.	Există responsabili desemnaţi pentru elaborarea şi actualizarea sistematică a procedurilor operaţionale?	X		
8.	Aţi aprobat procedurile operaţionale de lucru?	X		
9.	Până în prezent s-a realizat vreo revizie pentru actualizarea procedurilor operaţionale de lucru?	X		Da, anumite proceduri au fost actualizate de 2 ori.
10.	Consideraţi că procedurile operaţionale sunt complete, funcţionale şi asigură desfăşurarea corespunzătoare a activităţilor din cadrul compartimentului IT?	X		Da, după efectuarea mai multor revizii.
11.	Mai aveţi ceva de adăugat referitor la cele de mai sus?		X	

Data: 15.09.2009

Intervievat,
Director General Adrian Ionescu

Elaborat în faţa noastră; Auditori
Popescu Sorin
Radu George

ENTITATEA PUBLICĂ
Serviciul Audit Intern

NOTĂ DE RELAŢII nr. 2.1
privind modul de stabilire a activităţilor în cadrul compartimentului
adresată
domnului Popescu Marin Şef serviciu Întreţinere şi Implementare Aplicaţii.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Întrebarea nr. 1: Aţi participat la stabilirea atribuţiilor şi activităţilor compartimentului?

Răspuns nr. 1: Activităţile în cadrul compartimentului au fost stabilite pe baza atribuţiilor definite.

Întrebarea nr. 2: Aţi fost implicat în elaborarea atribuţiilor compartimentului*?*

Răspuns nr. 2: În anul 2007 a fost elaborat Regulamentul de organizare şi funcţionare unde am participat efectiv pentru departamentul pe care îl coordonez. De fapt atribuţiile stabilite de mine au rămas neschimbate în urma aprobării regulamentului.

Întrebarea nr. 3: La proiectarea structurii organizatorice s-a ţinut cont de inventarierea activităţilor executabile *?*

Răspuns nr. 3: Structura compartimentului şi numărul de posturi au fost prestabilite, iar noi a trebuit doar să alocăm activităţile şi atribuţiile.

Întrebarea nr. 4: Activităţile definite indică acţiuni concrete de realizare şi rezultate aşteptate*?*

Răspuns nr. 4: În unele cazuri da, în alte cazuri le-am definit sub formă de relaţii de colaborare sau participare în funcţie de scopul urmărit.

Întrebarea nr. 5: Cum explicaţi faptul că nu sunt identificate toate activităţile necesare realizării obiectivelor*?*

Răspuns nr. 5: Ulterior direcţia a mai primit şi alte activităţi în vederea realizării, însă pentru acestea nu s-a mai procedat la reanalizarea obiectivelor şi redefinirea acestora.

Întrebarea nr. 6: Din analiza unor activităţi a rezultat că acestea sunt realizate împreună cu alte compartimente, însă, evaluând obiectivele, s-a constatat că realizarea acestora include şi activităţile realizate de celelalte compartimente. Cum explicaţi aceasta*?*

Răspuns nr. 6: Aceste obiective şi activităţi se regăsesc la ambele compartimente, însă fiecare compartiment realizează numai partea pentru care este responsabilizat.

Întrebarea nr. 7: Mai aveţi ceva de adăugat?

Răspuns nr. 7: Nu.

Data: 15.09.2009
Dată în faţa noastră: Auditori
Popescu Sorin
Radu George

Şef serviciu
Popescu Marin

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FISĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 2.2

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Problema	Activităţile nu sunt definite omogen în cadrul structurii funcţionale, iar stabilirea complexităţii acestora nu se realizează în funcţie de nivelurile de calificare ale posturilor existente.
Constatarea	La proiectarea structurii organizatorice se pleacă de la inventarierea activităţilor existente sau necesare pentru realizarea obiectivelor şi se efectuează o analiză critică pentru a se constata în ce măsură acestea sunt adecvate realizării funcţiunii. La definirea activităţilor se are în vedere complexitatea acestora, respectiv gradul de diferenţiere a muncii pe orizontală şi pe verticală. Diferenţierea pe orizontală constă în numărul de activităţi (specializări) şi de subunităţi funcţionale (birouri, servicii). Diferenţierea pe verticală se referă la numărul de niveluri ierarhice de-a lungul cărora se exercită autoritatea în organizaţie. Analiza conţinutului şi modului de definire a activităţilor necesare pentru realizarea fiecărui obiectiv specific a pus în evidenţă următoarele: – unele activităţi sunt definite sub forma unor relaţii de colaborare care fie nu indică acţiuni concrete de realizare a acestora, fie indică o acţiune comună de realizare; – altele sunt definite sub forma unor relaţii de colaborare, în condiţiile în care sunt exercitate acţiuni concrete de realizare şi pentru care există rezultate aşteptate stabilite; – nu sunt identificate toate activităţile care contribuie la realizarea obiectivelor specifice şi care asigură conformitatea cu reglementările legale. Prin modul de organizare a activităţilor structurilor organizatorice ale direcţiei nu se asigură evitarea dublării acţiunilor, respectiv există activităţi identice sau similare, desfăşurate de mai multe departamente şi probleme semnificative de suprapunere şi de coordonare. De asemenea, pentru realizarea unor activităţi, nu se respectă principiul convergenţei în definirea şi stabilirea conţinutului activităţilor care sunt necesare pentru realizarea unui obiectiv.
Cauza	Managementul superior nu a acordat o suficientă atenţie domeniului organizaţional, în vederea reglementării lui formale în cadrul tuturor compartimentelor funcţionale.
Consecinţa	Nestabilirea clară a activităţilor şi acţiunilor poate conduce la nerealizarea, în condiţii optime, a obiectivelor şi nu permite identificarea cauzelor care au stat la baza nerealizării. De asemenea, nu se pot identifica problemele cu care se confruntă personalul şi nici nu se pot implementa politici care să asigure eficienţa şi eficacitatea în realizarea activităţilor.
Recomandarea	Organizarea eficientă a activităţii impune realizarea unei analize riguroase a sarcinilor şi responsabilităţilor fiecărui angajat, care să stea la baza oricărei iniţiative de organizare a activităţii. Constituirea unei echipe, pe baza deciziei managementului general, care să

	analizeze şi să redefinească activităţile şi acţiunile realizate în cadrul compartimentelor şi serviciilor, astfel încât să se asigure că obiectivele vor fi realizate în totalitate. La stabilirea obiectivelor se va urmări dacă sunt ataşate toate activităţile necesare obţinerii rezultatelor stabilite, realizate efectiv în cadrul compartimentului, formulate ca acţiuni concrete.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Radu George	Dumitru Daniel	Structură auditată

Procedura P08:	**Colectarea dovezilor**

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 2.3

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Obiectul testului	Organizarea funcţională a Departamentului IT
Obiectivele testului	Examinarea dacă organigrama reprezintă un instrument la îndemâna conducerii prin care se permite vizualizarea de ansamblu a organizării departamentului IT.
Descrierea testului	Analiza modului de elaborare a organigramei se realizează în conformitate cu actul normativ de organizare şi funcţionare a organizaţiei şi cu modului efectiv de organizare şi funcţionare a structurilor funcţionale din cadrul organizaţiei, punându-se accent pe următoarele: - stabilirea structurii funcţionale a departamentului, pe baza organigramei; - organigrama permite vizualizarea de ansamblu a organizării departamentului; - definirea în termen a relaţiilor din cadrul departamentului; - definirea raporturilor de subordonare în cadrul organigramei; - definirea numărului de posturi prin intermediul organigramei;
Constatări	Organigrama, ca document prin care se relevă grafic structura organizaţiei şi substructurile acesteia, nu pune în evidenţă organizarea şi funcţionarea departamentului. Compartimentele aflate în subordinea departamentului nu sunt nominalizate în totalitate în cadrul organigramei şi nu este precizat nici nivelul de subordonare al departamentului în cadrul organizaţiei. Organigrama nu furnizează o înţelegere a raporturilor de subordonare şi de evitare a suprapunerilor de competenţe. Astfel, cu privire la raporturile de subordonare potrivit organigramei, Serviciul Programare este organizat sub forma unui compartiment care se află în directa subordonare a directorului general adjunct al departamentului, în realitate acest compartiment este organizat la nivel de serviciu şi subordonat directorul general. Postul de director general adjunct a fost desfiinţat în anul 2008 urmare reorganizărilor efectuate. Definirea relaţiilor ierarhice, aşa cum a fost precizat mai sus, nu asigură o integrare corespunzătoare a departamentului în structura organizatorică a organizaţiei şi nu asigură operativitatea fluxului de informaţii şi date între structurile implicate în prelucrarea datelor şi obţinerea rezultatelor finale. În structura organizatorică a departamentului, definită în cadrul organigramei, nu se precizează în cadrul serviciilor, numărul de posturi şi responsabilii structurilor funcţionale corespunzător fiecărui nivel ierarhic şi/sau cine coordonează aceste servicii şi compartimente, ceea ce nu permite identificarea nivelurilor şi relaţiilor ierarhice.
Concluzii	Organigrama nu este funcţional şi nu prezintă în totalitate raporturile funcţionale, nivelurile ierarhice şi relaţiile interne existente între compartimente.

Auditor intern,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FISĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 2.3

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Problema	Organigrama nu permite o vizualizare de ansamblu a organizării departamentului, a numărului de personal repartizat în cadrul compartimentelor şi a relaţiilor existente între compartimente.
Constatarea	Organigrama ca document prin care se relevă grafic structura organizaţiei şi substructurile acesteia nu pune în evidenţă organizarea şi funcţionarea departamentului. Compartimentele aflate în subordinea departamentului nu sunt nominalizate în totalitate în cadrul organigramei şi nu este precizat nici nivelul de subordonare al departamentului în cadrul organizaţiei. Organigrama nu furnizează o înţelegere a raporturilor de subordonare şi de evitare a suprapunerilor de competenţe. Astfel, cu privire la raporturile de subordonare, potrivit organigramei, Serviciul Programare este organizat sub forma unui compartiment care se află în directa subordonare a directorului general adjunct al departamentului, dar în realitate acest compartiment este organizat la nivel de serviciu şi subordonat directorul general. Postul de director general adjunct a fost desfiinţat în anul 2008 urmare a reorganizărilor efectuate. Definirea relaţiilor ierarhice aşa cum a fost precizat mai sus, nu asigură o integrare corespunzătoare a departamentului în structura organizatorică a organizaţiei şi nu se asigură operativitatea fluxului de informaţii şi date între structurile implicate în fluxul tehnologic al activităţilor. În structura organizatorică a departamentului, definită în cadrul organigramei, nu se precizează în cadrul serviciilor numărul de posturi şi responsabilii structurilor funcţionale corespunzător fiecărui nivel ierarhic şi/sau cine coordonează aceste servicii şi compartimente, ceea ce nu permite identificarea nivelurilor şi relaţiilor ierarhice.
Cauza	La nivelul organizaţiei nu au existat reglementări procedurale să definească şi să stabilească o formă cadru de elaborare a organigramei. În ultima perioadă în cadrul organizaţiei au fost realizate mai multe modificări structurale, în sensul că activităţile desfăşurate au fost reorganizate, ceea ce a presupus şi modificări ale structurilor funcţionale.
Consecinţa	Nu se asigură o înţelegere corespunzătoare a modului de organizare şi funcţionare a departamentului, a nivelului ierarhic şi a relaţiilor existente între compartimente. În forma în care este elaborată organigrama, nu conţine o serie de informaţii referitoare la relaţiile interne existente între compartimente şi la nivelurile de subordonare.
Recomandări	Analiza actului normativ de organizare şi funcţionare a organizaţiei. Urmărirea atribuţiilor definite departamentului astfel încât să acopere în totalitate activităţile desfăşurate. Stabilirea corectă a relaţiilor şi subordonărilor dintre compartimente.

Auditor intern, Radu George
Supervizor, Dumitru Daniel
Pentru conformitate, Structură auditată

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 2.4.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Obiectul testului	Organizarea şi funcţionarea departamentului IT.
Obiectivele testului	Analiza corelaţiei dintre numărul de posturi de conducere ocupate şi cele deţinute cu delegaţie.
Descrierea testului	Departamentul IT din cadrul entităţii publice are 3 servicii funcţionale. Eşantionul va fi constituit din posturile de conducere existente şi testarea va urmări modul cum sunt realizate atribuţiile acestor posturi. Testarea a constat în examinarea următoarelor elemente: • Analiza organigramei departamentului IT: - număr total de posturi de conducere - număr posturi de conducere ocupate cu delegaţie - număr total de posturi de execuţie - număr posturi de execuţie neocupate. • Demersurile realizate de departamentul IT pentru ocuparea posturilor de conducere: - număr de examene organizate pentru ocuparea posturilor; - număr de solicitări către compartimentul de Resurse Umane pentru organizarea examenelor. • Preocuparea conducerii pentru ocuparea posturilor de execuţie; - număr de examene organizate pentru ocuparea posturilor - număr de solicitări către compartimentul de Resurse Umane pentru organizarea concursurilor. • Existenţa unui plan de implementare a măsurilor necesare, menit să asigure buna desfăşurare a activităţii în cazul existenţei unui număr mare de posturi vacante.
Constatări	Din analiza modului de acoperire a necesarului de resurse umane la nivelul departamentului IT s-a constatat că două din cele trei posturi de conducere de şef de serviciu sunt ocupate cu delegaţie de circa 18 luni. Examinarea fişelor posturilor pentru posturile de execuţie ocupate de persoanele care au fost numite cu delegaţie în posturi de conducere s-a constatat că acestea nu prevedeau nici o aptitudine managerială. Totodată analiza îndeplinirii/realizării activităţilor celor două servicii a pus în evidenţă faptul că în unele cazuri acestea nu au fost realizate sau au fost realizate cu întârziere. Din verificarea modului de planificare şi realizare zilnică a activităţilor a rezultat că persoanele responsabilizate în posturile de conducere nu au coordonat în nici un fel activităţile care erau realizate zilnic de către salariaţi, nu au îndrumat în nici un fel salariaţii cu privire la modul în care în care să realizeze activităţile şi nici nu au realizat o monitorizare cu privire la modul de realizare a acestora. Salariaţii, în baza sarcinilor stabilite prin fişa postului, au realizat activităţile în funcţie de cunoştinţele şi aptitudinile pe care le deţineau. La nivelul celor două servicii în această perioadă nu a fost luată nici o decizie cu privire la îmbunătăţirea activităţilor sau la dezvoltarea acestora.
Concluzii	Delegarea pe posturi de conducere de persoane care nu deţineau abilităţi manageriale.

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

Procedura P08:	**Colectarea dovezilor**

ENTITATEA PUBLICĂ
Serviciul Audit Intern

Lista control nr. 2.1
privind organizarea şi funcţionarea departamentului IT

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Nr. crt	**Elemente testate / Eşantion**	**Analiza organigramei departamentului IT**				**Evaluarea demersurilor realizate de departamentul IT pentru ocuparea posturilor**		**Analiza consecinţelor funcţionării departamentului IT cu persoane de conducere cu delegaţie**		**Existenţa preocupării pentru ocuparea posturilor de execuţie**		**Existenţa unui plan de implementare a măsurilor necesare menit să asigure buna desf. a act. în cazul existenţei unui număr mare de posturi de conducere şi/sau execuţie vacante**
		Nr. total posturi de conducere	**Nr. posturi de cond. ocupate cu delegaţie**	**Nr. total posturi de execuţie**	**Nr. posturi de execuţie neocup.**	**Nr. de examene organizate pentru ocuparea posturilor**	**Nr. de solicitări către compart. de RU pentru org. ex.**	**Nr. de sesizări ale depart. beneficiare ale serviciilor IT**	**Nr. de subsisteme IT neimpl. la timp**	**Nr. de examene organizate pentru ocuparea posturilor**	**Nr. de solicitări către compart. de RU pentru org. ex.**	
1.	*Serviciul dezvoltare aplicaţii*	3	1	12	4	Nu	Nu	X	X	X	X	Nu
2.	*Serviciul comunicaţii*	1	0	9	5	Nu	Nu	X	X	X	X	Nu
3.	*Serviciul exploatare aplicaţii*	1	0	10	3	Nu	Nu	X	X	X	X	Nu
4.	*Serviciul proiectare şi programare*	3	2	14	3	Nu	Nu	X	X		X	Nu
5.	*Serviciul reţele informatice*	1	0	9	2	Nu	Nu	X	X	X	X	Nu

Procedura P08:	**Colectarea dovezilor**

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FISĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 2.4

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Problema	Grad ridicat de neocupare a posturile existente şi aprobate departamentului IT.
Constatarea	Două din cele trei posturi de conducere de şef de serviciu au fost ocupate cu delegaţie de circa 18 luni. Din verificarea modului de planificare şi realizare zilnică a activităţilor a rezultat că persoanele responsabilizate în posturile de conducere nu au coordonat în nici un fel activităţile care erau realizate zilnic de către salariaţi, nu au îndrumat în nici un fel salariaţii cu privire la modul în care în care să realizeze activităţile şi nici nu au realizat o monitorizare cu privire la modul de realizare a acestora. Salariaţii, în baza sarcinilor stabilite prin fişa postului, au realizat activităţile în funcţie de cunoştinţele şi aptitudinile pe care le deţineau. Examinarea fişelor posturilor pentru posturile de execuţie ocupate de persoanele care au fost numite cu delegaţie în posturi de conducere s-a constatat că acestea nu prevedeau nici o aptitudine managerială. La nivelul celor două servicii în această perioadă nu a fost luată nici o decizie cu privire la îmbunătăţirea activităţilor sau la dezvoltarea acestora.
Cauza	Numirea în posturi de conducere de persoane care nu deţineau abilităţi manageriale adecvate pentru posturile respective.
Consecinţa	Întârzieri în realizarea activităţilor şi/sau nerealizarea acestora, organizarea şi realizarea defectuoasă a activităţilor de către salariaţi.
Recomandarea	Solicitarea desfăşurării procesului de selecţie şi recrutarea în vederea ocupării posturilor de conducere existente la nivelul departamentului IT. Recrutarea va urmări dacă persoanele selectate deţin abilităţile şi aptitudinile manageriale necesare realizării activităţilor specifice celor două servicii şi dacă au pregătirea de bază, de nivel superior, în domeniul IT.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Popescu Sorin	Dumitru Daniel	Structură auditată

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 2.5

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Obiectul testului	Examinarea sistemului de gestionare a riscurilor generale la nivelul departamentului IT
Obiectivele testului	Analiza modului în care riscurile sunt identificate şi gestionate la nivelul departamentului IT, în vederea asigurării existentei controalelor interne corespunzătoare
Descrierea testului	Eşantionul va fi constituit din riscurile identificate şi gestionate de departamentul IT. Pentru fiecare obiectiv al departamentului vor fi selectate 5% din riscuri şi acestea vor fi evaluate cu privire la modul în care au fost stabilite controalele interne, cum au fost stabilite şi introduse instrumente de control pentru menţinerea lor în limite de accesibilitate şi dacă toate aceste instrumente de control introduse menţin riscurile la niveluri inferioare. Totodată s-a urmărit dacă controalele interne introduse sunt funcţionale.
Constatări	Din analiză s-a constatat că nu există preocupări pentru gestionarea riscurilor din cadrul entităţii şi nu a fost ţinut Registrul riscurilor cuprinzând riscurile potenţiale şi istoricul acestora, cu efectele şi consecinţele lor, precum şi activităţile de control intern asociate pentru limitarea acestora.
Concluzii	La nivelul departamentului nu este asigurata o gestiune corespunzătoare a riscurilor. Acestea nu sunt identificate şi monitorizate în vederea menţinerii lor în limitele de accesibilitate.

Auditor intern,
Ionescu Adrian

Supervizor,
Florescu Cristian

ENTITATEA PUBLICĂ
Serviciul Audit Intern

INTERVIU nr. 2.2
privind sistemul de gestionare a riscurilor
adresat
domnului Ionescu Adrian, director general

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Nr. crt.	***Întrebări***	**Da**	**Nu**	**Obs.**
1.	Există o politică de management al riscului?	X		
2.	Există preocupări pentru managementul riscurilor în cadrul departamentului IT?	X		
3.	S-au organizat cursuri cu întreg personalul pentru activitatea de gestionare a riscurilor în conformitate cu metodologia de organizare a sistemului de control intern conform prevederilor OMFP nr. 946/2005 privind Codul controlului intern?		X	
4.	Au fost identificate riscurile la nivelul departamentului IT?		X	
5.	Există un sistem de evaluare a riscurilor?		X	
6.	Au fost prevăzute măsuri de răspuns în cazul apariţiei riscurilor?		X	
7.	Există un sistem de monitorizare şi raportare periodică a riscurilor asociate activităţii Direcţia IT?		X	
8.	Aveţi elaborat şi actualizat Registrul riscurilor?		X	
9.	Este desemnat un responsabil cu gestionarea riscurilor la nivelul departamentului IT?	X		

Data: 15.09.2009

Intervievat,
Ionescu Adrian

Elaborat în prezenţa noastră: Auditori
Popescu Sorin

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 2.5

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Problema	Neimplementarea unui sistem de control managerial potrivit căruia riscurile aferente domeniului IT să fie identificate şi gestionate.
Constatarea	Din analiză s-a constatat că riscurile nu sunt identificate şi gestionate la nivelul departamentului şi nu este condus Registrul riscurilor cuprinzând riscurile potenţiale şi istoricul acestora, precum şi instrumentele de control intern implementate pentru limitarea acestora.
Cauza	Lipsa procedurile de lucru, cât şi a practicii în cadrul organizaţiei privind modul de identificare şi gestionare a riscurilor.
Consecinţa	Stocarea neadecvată a datelor şi informaţiilor; Accesul la date şi informaţii a întregului personal şi nu pe niveluri de autorizare; Sistem informaţional necorespunzător cerinţelor organizaţiei; Posibilitatea sustragerii de date şi informaţii cu importanţă pentru entitate.
Recomandarea	Elaborarea mecanismelor procedurale şi metodologice privind identificarea riscurilor şi gestionarea acestora Evaluarea riscurilor identificate şi diferenţierea acestora în riscuri inerente şi riscuri acceptabile. Implementarea de instrumente de control pentru riscurile inerente, astfel încât manifestarea acestora să fie limitată şi nivelul acestora să devină unul acceptabil.

Auditor intern, Popescu Sorin
Supervizor, Dumitru Daniel
Pentru conformitate, Structură auditată

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 2.6

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Obiectul testului	Examinarea sistemului de gestionare a riscurilor generale la nivelul Departamentului IT
Obiectivele testului	Analiza şi evaluarea riscurilor a urmărit modul în care conducerea departamentului identifică riscurile relevante, estimează semnificaţia acestora, evaluează probabilitatea apariţiei lor şi decide în funcţie de acestea instrumentele de control pentru a le menţine sub control.
Descrierea testului	Analiza implementării controlului intern a urmărit dacă acesta este proiectat, implementat şi menţinut pentru a aborda riscurile care ameninţă atingerea oricăruia dintre obiectivele departamentului cu privire la: - credibilitatea raportării financiare; - eficienţa şi eficacitatea operaţiilor sale; - respectarea legilor şi reglementărilor aplicabile.
Constatări	Din analiza sistemului de control intern instituit la nivelul departamentului IT a rezultat că unele activităţi de control relevante nu au fost cuprinse în politicile şi procedurile de control instituite, astfel: - revizuiri ale performanţei - aceste activităţi de control trebuie să includă revizuiri şi analize ale performanţei efective în comparaţie cu bugetele, previziunile şi performanţa perioadelor precedente; - procesarea informaţiilor – acestea trebuie să includă cele două grupări de activităţi de control ale sistemelor informaţionale, respectiv controalele asupra aplicaţiilor individuale şi controalele generale asupra tehnologiei informaţiei, care sunt de fapt politici şi proceduri care se referă la mai multe aplicaţii şi contribuie la asigurarea funcţionării adecvate şi continue a sistemelor informaţionale. Exemple de controale generale ale tehnologiei informaţiei sunt controalele asupra modificării programului, controalele de restricţionare a accesului la programe sau la date, controalele asupra implementării de noi aplicaţii informatice. Anumite activităţi de control care nu sunt de rutină şi care depind de existenţa unor politici adecvate stabilite de conducere sau de cei însărcinaţi cu guvernanţa nu au o aprobare de la aceste niveluri şi nici nu au fost delegate în responsabilitatea unor posturi inferioare. Din analiza efectuată a rezultat că la nivelul departamentului nu este organizat şi nu se conduce Registrul riscurilor. Riscurile cu care se confruntă organizaţia nu sunt identificate şi nu sunt monitorizate în vederea stăpânirii şi menţinerii lor la un nivel acceptabil. Riscurile relevante includ evenimente, tranzacţii sau împrejurări externe şi interne care pot apărea şi care pot afecta în mod negativ capacitatea departamentului de a iniţia, înregistra, procesa şi raporta date corecte şi conforme. Riscurile apar şi se schimbă din următoarele cauze: - modificări ale mediului în care se desfăşoară activitatea. - personal nou, care poate avea o înţelegere diferită în ceea ce priveşte controlul intern. - extindere semnificativă şi rapidă a operaţiilor, care constrâng controalele şi sporesc apariţia riscului. - introducerea de noi tehnologii în procesele de producţie şi în sistemele

	informaţionale, care modifică riscurile asociate cu controlul intern.
Concluzii	Sistemul de control intern nu cuprinde toate activităţile de control necesare minimizării riscurilor şi realizării obiectivelor.

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FISĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 2.6

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Problema	Sistemul de control intern definit la nivelul organizaţiei nu cuprinde toate activităţile de control ce trebuie alocate în vederea atingerii obiectivelor.
Constatarea	Din analiza sistemului de control intern instituit la nivelul departamentului IT a rezultat că unele activităţi de control relevante nu au fost cuprinse în politicile şi procedurile de control instituite, astfel: - revizuiri ale performanţei - aceste activităţi de control trebuie să includă revizuiri şi analize ale performanţei efective în comparaţie cu bugetele, previziunile şi performanţa perioadelor precedente; - procesarea informaţiilor – acestea trebuie să includă cele două grupări de activităţi de control ale sistemelor informaţionale, respectiv controalele asupra aplicaţiilor individuale şi controalele generale asupra tehnologiei informaţiei, care sunt de fapt politici şi proceduri care se referă la mai multe aplicaţii şi contribuie la asigurarea funcţionării adecvate continue a sistemelor informaţionale. Exemple de controale generale ale tehnologiei informaţiei sunt controalele asupra modificării programului, controalele de restricţionare a accesului la programe sau la date, controalele asupra implementării de noi aplicaţii informatice. Anumite activităţi de control care nu sunt de rutină şi care depind de existenţa unor politici adecvate stabilite de conducere sau de cei însărcinaţi cu guvernanţa nu au o aprobare de la aceste niveluri şi nici nu au fost delegate în responsabilitatea unor posturi inferioare. Din analiza efectuată a rezultat că la nivelul departamentului nu este organizat şi nu se conduce registrul riscurilor. Riscurile cu care se confruntă organizaţia nu sunt identificate şi nu sunt monitorizate în vederea stăpânirii şi menţinerii lor la un nivel acceptabil. Riscurile relevante includ evenimente, tranzacţii sau împrejurări externe şi interne care pot apărea şi care pot afecta în mod negativ capacitatea departamentului de a iniţia, înregistra, procesa şi raporta date corecte şi conforme. Riscurile apar şi se schimbă din următoarele cauze: - modificări ale mediului în care se desfăşoară activitatea. - personal nou, care poate avea o înţelegere diferită în ceea ce priveşte controlul intern. - extindere semnificativă şi rapidă a operaţiilor, care constrâng controalele şi sporesc apariţia riscului. - introducerea de noi tehnologii în procesele de producţie şi de sisteme informaţionale care modifica riscurile asociate cu controlul intern.
Cauza	Persoana responsabilă cu revizuirea controalelor nu înţelege care este scopul acestora şi nu ia măsurile adecvate care se impun.
Consecinţa	Controlul intern nu oferă o asigurare rezonabilă în legătură cu atingerea

	obiectivelor. Activităţile de control, respectiv autorizarea, revizuirea performanţei, procesarea informaţiilor, controalele fizice, separarea responsabilităţilor nu ajută şi nu dau asigurări că deciziile conducerii sunt duse la îndeplinire.
Recomandări	Stabilirea controalelor interne aferente riscurilor identificate şi determinarea gradului de funcţionalitate al acestora. Pentru riscurile care nu se află la un nivel acceptabil, să se proiecteze un instrument sau măsură de introducere de controale interne, fie individuale, fie în combinaţie cu alte controale, capabile să prevină, detecteze şi să corecteze în mod eficient denaturările semnificative. Instituirea şi conducerea Registrului riscurilor la nivelul organizaţiei.

Auditor intern, Popescu Sorin

Supervizor, Dumitru Daniel

Pentru conformitate, Structură auditată

Procedura P08:	**Colectarea dovezilor**

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 2.7

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Obiectul testului	Definirea sarcinilor prin fişa postului
Obiectivele testului	Examinarea dacă cerinţele specifice solicitate la ocuparea postului respectă caracteristicile postului respectiv
Descrierea testului	Urmărirea dacă fişa postului elaborată pentru un anumit post, defineşte corect condiţiile specifice pe care trebuie să le îndeplinească postul, respectiv: a) condiţiile privind studiile de specialitate; b) condiţiile privind specializările necesare pentru ocuparea postului; c) condiţiile privind cunoştinţele informatice; d) definirea sarcinilor în funcţie de nivelul postului, f) alocarea sarcinilor în concordanţă cu competenţele manageriale necesare postului.
Constatări	Studiile de specialitate aferente unui post sunt definite în cadrul fişei postului fără a se ţine cont de scopul postului şi cunoştinţele de bază necesare pentru realizarea atribuţiilor alocate acestuia. Din analiza fişelor posturilor s-a constatat că la concursul organizat pentru ocuparea postului respectiv poate participa orice persoana care are o diploma, deoarece nu se specifică tipul de studii şi nivelul acestora, respectiv în domeniul IT, studii superioare de lungă durată absolvite cu diplomă de licenţă etc.. La stabilirea sarcinilor în fişele posturilor nu se urmăreşte asigurarea unui echilibru între sarcinile şi competenţele titularului postului. Din analiza eşantionului selectat a rezultat că pentru posturile cu un nivel al studiilor medii sunt alocate aceleaşi atribuţii şi responsabilităţi ca şi pentru posturile cu un nivel al studiilor superior. Acestea creează probleme în gestionarea aplicaţiilor şi programelor, deoarece persoanelor încadrate în cadrul departamentului pe studii medii le-au fost date în responsabilitate întreţinerea de aplicaţii şi programe complexe şi chiar realizarea de astfel de aplicaţii pentru organizaţie, care necesită cunoştinţe IT de nivel superior şi chiar anumite specializări.
Concluzii	Studiile de specialitate nu sunt menţionate în fişa postului potrivit cerinţelor de ocupare a postului. Repartizarea sarcinilor în cadrul fişelor posturilor nu se realizează în conformitate cu competenţele titularilor posturilor.

Auditor intern,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern

INTERVIU nr. 2.3
privind definirea sarcinilor pe grade profesionale
adresat
Şefului Serviciului Programare Vasilescu Gheorghe

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Nr. crt.	ÎNTREBĂRI	DA	NU	OBSERVAŢII
1.	Există un responsabil cu elaborarea fişelor posturilor?	**X**		
2.	Există o delimitare a atribuţiilor alocate compartimentelor pentru fiecare post existent?	**X**		
3.	Sarcinile sunt definite pentru fiecare grad profesional în fişa postului?	**X**		
4.	Sarcinile sunt definite în baza atribuţiilor stabilite la nivelul serviciului şi le acoperă în totalitate?	**X**		
5.	Atribuţiile definite asigură realizarea activităţilor identificate?	**X**		
6.	Sarcinile sunt stabilite diferenţiat în funcţie de gradul profesional al postului?		**X**	Activităţile din cadrul serviciului se regăsesc la mai multe posturi
7.	Există definite aceleaşi tipuri de sarcini pentru funcţii profesionale diferite?		**X**	Nu s-a urmărit ca sarcinile să difere în funcţie de gradele profesionale definite de post
8.	Pentru acelaşi tip de sarcini stabilite pentru posturi diferite sunt stabilite aceleaşi obiective individuale?	**X**		
9.	Totalitatea sarcinilor definite pentru posturile existente în cadrul serviciului este asigurată prin atribuţii şi contribuie la realizarea activităţilor?	**X**		
10.	Atribuţiile definite postului acoperă scopul acestuia?	**X**		
11.	Mai aveţi ceva de adăugat referitor la cele de mai sus?		**X**	

Data: 15.09.2009

Intervievat,
Vasilescu Gheorghe

Elaborat în faţa noastră: Auditori
Popescu Sorin
Radu George

ENTITATEA PUBLICĂ
Serviciul Audit Intern

NOTĂ DE RELAŢII nr. 2.2
privind alocarea sarcinilor în funcţie de responsabilităţi
adresată doamnei Vasilescu Maria

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Întrebarea nr. 1: Postul pe care îl ocupaţi este de execuţie*?*

Răspuns nr. 1: Da*.*

Întrebarea nr. 2: Cunoaşteţi atribuţiile definite în fişa postului*?*

Răspuns nr. 2: Da*, dar nu sunt exercitate în totalitate.*

Întrebarea nr. 3: Atribuţia nr. 3 se referă la planificarea activităţilor zilnice în cadrul serviciului. Ce activităţi realizaţi pentru îndeplinirea acesteia*?*

Răspuns nr. 3: Zilnic planific pentru fiecare salariat din cadrul serviciului activităţile pe care trebuie să le execute sau să le realizeze pentru ziua respectivă*.*

Întrebarea nr. 4: La nivelul serviciului există numit sef de serviciu*?*

Răspuns nr. 4: Da*.*

Întrebarea nr. 5: De ce acesta nu realizează planificarea zilnică a activităţilor salariaţilor din subordine*?*

Răspuns nr. 5: Are prea multe sarcini şi a fost nevoit să delege o parte din atribuţii.

Întrebarea nr. 6: Sarcina de planificare a activităţilor serviciului va delegat-o prin fişa postului*?*

Răspuns nr. 6: Nu, mi-a comunicat-o verbal*.*

Întrebarea nr. 7: Cine face analiza rezultatelor activităţilor planificate*?*

Răspuns nr. 7: Nu este realizată această activitate. Eu îi comunic cum am repartizat şi el informează conducerea*.*

Întrebarea nr. 8: *Mai aveţi ceva de adăugat?*

Răspuns nr. 8: *Nu.*

Data: 15.09.2009

Intervievat,
Vasilescu Maria

Elaborat în faţa noastră: Auditori
Popescu Sorin
Radu George

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FISĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 2.7

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Problema	Studiile de specialitate nu sunt menţionate în fişa postului potrivit cerinţelor de ocupare a postului. Repartizarea sarcinilor în cadrul fişelor posturilor nu se realizează în conformitate cu competenţele titularilor posturilor.
Constatarea	Studiile de specialitate aferente unui post sunt definite în cadrul fişei postului fără a se ţine cont de scopul postului şi cunoştinţele de bază necesare pentru realizarea atribuţiilor alocate acestuia. Din analiza fişelor posturilor s-a constatat că la concursul organizat pentru ocuparea postului respectiv poate participa orice persoană care are o diplomă, deoarece nu se specifică tipul de studii şi nivelul acestora, respectiv în domeniul IT, studii superioare de lungă durată absolvite cu diplomă de licenţă etc. La stabilirea sarcinilor în fişele posturilor nu se urmăreşte asigurarea unui echilibru între sarcinile şi competenţele titularului postului. Din analiza eşantionului selectat a rezultat că pentru posturile cu un nivel al studiilor medii sunt alocate aceleaşi atribuţii şi responsabilităţi ca şi pentru posturile cu un nivel al studiilor superiore. Acestea creează probleme în gestionarea aplicaţiilor şi programelor, deoarece persoanelor încadrate în cadrul departamentului pe studii medii le-au fost date în responsabilitate întreţinerea de aplicaţii şi programe complexe şi chiar realizarea de astfel de aplicaţii pentru organizaţie, care necesită cunoştinţe IT de nivel superior şi chiar anumite specializări.
Cauza	Tratarea cu superficialitate a procesului de elaborare a fişelor posturilor. Lipsa de responsabilitate în exercitarea sarcinilor şi responsabilităţilor de către personalul cu atribuţii de conducere.
Consecinţa	Fişa postului nu asigură în toate cazurile informaţii suficiente comisiei de recrutare şi selecţie, necesare pentru identificarea celor mai bune persoane pentru postul respectiv. Nerealizarea în termen şi în condiţii de calitate a obiectivelor individuale în cazul personalului cu funcţii de rang inferior şi care are repartizat un număr mai mare de sarcini în comparaţie cu personalul cu funcţii de rang superior.
Recomandarea	Analiza sarcinilor şi atribuţiilor definite în fişele posturilor şi stabilirea acestora în funcţie de caracteristicile postului, respectiv nivelul postului şi urmărirea definirii aceluiaşi gen de sarcini şi atribuţii numai dacă posturile sunt de acelaşi nivel.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Radu George	Dumitru Daniel	Structură auditată

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 2.8

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Obiectul testului	Definirea sarcinilor prin fişa postului
Obiectivele testului	Atribuţiile stabilite compartimentelor funcţionale vor fi evaluate şi se va urmări dacă acestea definesc aria de competenţă necesară realizării activităţilor şi acţiunilor; În cazul activităţilor realizate prin colaborare cu alte structuri funcţionale din cadrul organizaţiei, se va urmări dacă relaţiile funcţionale de colaborare sau cooperare cu structurile respective sunt corect definite şi stabilite.
Descrierea testului	Eşantionul a fost constituit prin alegerea aleatorie a unui număr de două compartimente din cadrul departamentului IT. în cazul acestora au fost evaluate atribuţiile şi relaţiile funcţionale definite cu privire la: - analiza atribuţiilor stabilite compartimentului şi stabilirea dacă aria de competenţă a acestora ajută la realizarea activităţilor; - urmărirea ca aria de competenţă să asigure realizarea activităţilor şi acţiunilor stabilite compartimentului funcţional. - analiza relaţiilor cu celelalte structuri funcţionale din cadrul organizaţiei cu care are sau ar trebui să aibă relaţii funcţionale pentru realizarea atribuţiilor şi activităţilor; - definirea relaţiilor ierarhice.
Constatări	Atribuţiile definite în sarcina compartimentelor funcţionale nu sunt întotdeauna conforme şi nu asigură competenţa de realizare a activităţilor şi acţiunilor, acestea sunt definite în multe cazuri la modul general, nu indică, prin modul de formulare, o acţiune, nu asigură un conţinut clar, fiind definite sub forma unei relaţii funcţionale sau având caracter de activitate sau de sarcină. Nu sunt definite în cadrul ROF-ului, la capitolul privind departamentul IT, relaţiile cu celelalte structuri funcţionale cu care are sau ar trebui să aibă relaţii funcţionale, respectiv nu este definită relaţia funcţională care reglementează asigurarea conformităţii informaţiilor cu privire la asistarea utilizatorilor în realizarea activităţilor de introducere a datelor şi informaţiilor în cadrul aplicaţiilor şi programelor derulate la nivelul celorlalte departamente funcţionale din cadrul organizaţiei, precum şi cu privire la asistarea în utilizarea echipamentelor din dotare. Totodată, nu sunt prezentate relaţiile ierarhice între posturile de conducere şi posturile de execuţie, ci numai relaţia ierarhică între posturile de conducere situate la niveluri ierarhice diferite din cadrul departamentului IT.
Concluzii	Atribuţiile stabilite compartimentelor funcţionale nu asigură întotdeauna aria de competenţă necesară pentru realizarea activităţilor;

Auditor intern,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FISĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 2.8

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

Problema	Formularea atribuţiilor în cadrul ROF-ului nu asigură întotdeauna aria de competenţă privind realizarea activităţilor şi acţiunilor repartizate unui compartiment.
Constatarea	Atribuţiile definite în sarcina compartimentelor funcţionale nu sunt întotdeauna conforme şi nu asigură competenţa de realizare a activităţilor şi acţiunilor, acestea fiind definite în multe cazuri la modul general, nu indică, prin modul de formulare, o acţiune, nu asigura un conţinut clar, fiind sub forma unei relaţii funcţionale sau având caracter de activitate sau sarcină. Nu sunt definite în cadrul ROF-ului la capitolul privind departamentul IT relaţiile cu celelalte structuri funcţionale cu care are sau ar trebui să aibă relaţii funcţionale, respectiv nu este definită relaţia funcţională care reglementează asigurarea conformităţii informaţiilor cu privire la asistarea utilizatorilor în realizarea activităţilor de introducere a datelor şi informaţiilor în cadrul aplicaţiilor şi programelor derulate la nivelul celorlalte departamente funcţionale din cadrul organizaţiei, precum şi cu privire la asistarea în utilizarea echipamentelor din dotare. Totodată, nu sunt prezentate relaţiile ierarhice între posturile de conducere şi posturile de execuţie, ci numai relaţia ierarhică între posturile de conducere situate la niveluri ierarhice diferite din cadrul departamentului IT.
Cauza	Definirea atribuţiilor specifice s-a realizat de către Departamentul IT, iar cuprinderea lor în cadrul ROF-ului s-a realizat la nivelul Departamentului de resurse umane, fără a mai fi analizată, de către persoanele responsabile, elaborarea coerentă şi corectă a documentului de organizare şi funcţionare. Persoanele din cadrul departamentului IT care au fost responsabilizate cu elaborarea capitolului aferent din cadrul ROF-ului nu au dispus de cunoştinţele necesare astfel încât să poată defini corect o atribuţie şi în acelaşi timp să urmărească ca acestea să asigure aria de competentă a realizării activităţilor din cadrul compartimentului.
Consecinţa	Nu se asigură o arie de competenţă necesară şi suficientă pentru realizarea activităţilor şi acţiunilor.
Recomandarea	Identificarea şi definirea corectă în cadrul documentului de organizare şi funcţionare, a atribuţiilor specifice departamentului, a relaţiilor funcţionale pe care compartimentul la are cu alte structuri funcţionale din cadrul organizaţiei.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Radu George	Dumitru Daniel	Structură auditată

ENTITATEA PUBLICA
Serviciul Audit Intern

LISTA DE VERIFICARE NR. 3

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 16.09.2009
Avizat: Dumitru Daniel Data: 16.09.2009

Obiectivul III.

OPERAŢII ALE SISTEMULUI INFORMATIC

Nr. crt.	Activitatea de audit	Da	Nu	Obs.
A	**Managementul operaţiunilor**			
1.	**Performanţa, capacitatea şi disponibilitatea sistemelor informatice este monitorizată de administratori**			
1.1.	Verificaţi dacă identificarea disfuncţionalităţilor se face conform manualelor de operare	X		
1.2.	Verificaţi dacă mesajele sunt analizate şi interpretate în timpul rulării aplicaţiei, pentru identificarea cauzelor care au condus la apariţia disfuncţionalităţilor;	X		
1.3.	Verificaţi dacă mesajele de eroare se abordează în conformitate cu manualul de operare;	X		
1.4.	Verificaţi dacă a fost identificat şi analizat impactul potenţial al producerii unor evenimente necontrolate asupra continuităţii activităţii;	X		
1.5.	Informatizarea organizaţiei ia în considerarea toate departamentele din cadrul acesteia, precum şi funcţiile acestora, nu doar departamentele unde se procesează datele;	X		
1.6.	Verificaţi dacă este estimat timpul maxim de nefuncţionare care poate fi acceptat şi costurile asociate acestuia;	X		
1.7.	Analizaţi dacă sunt stabilite de către conducere priorităţile pentru procesele necesare a fi informatizate şi de integrare a datelor şi informaţiilor;	X		
1.8.	Verificaţi dacă elaborarea planului de continuitate a activităţilor se realizează prin elaborarea de scenarii de ameninţări;	X		
1.9.	Analizaţi dacă determinarea nevoilor critice se realizează pe baza evaluării funcţiilor, proceselor şi personalului din cadrul fiecărui departament funcţional;	X		
1.10.	Verificaţi dacă pentru fiecare departament sunt stabilite următoarele:	X		
	a) ce echipamente specializate sunt necesare şi cum se utilizează;			
	b) cum va funcţiona departamentul dacă serverul, accesul la reţea (intranet) şi/sau Internet nu sunt disponibile;			
	c) necesarul de personal şi de spaţiu pentru locul unde se face recuperarea;			
	d) ce echipamente sunt necesare la locul unde se face recuperarea;			
	e) ce controale critice operaţionale sau de securitate sunt necesare înainte de a face recuperarea;			
1.11.	Verificaţi dacă personalul este instruit cu privire la salvarea şi stocarea datelor şi securitatea informaţiei;	X		
1.12.	Operaţiile sunt analizate având în vedere interdependenţa lor?	X		
1.13.	Se analizează impactul produs de funcţionarea incorectă a unei operaţii asupra întregului sistem?	X		
1.14.	Analiza a ţinut cont de funcţiile desfăşurate în cadrul entităţii: tehnice sau legate de procese?	X		
1.15.	Verificaţi dacă funcţiile tehnice asigură o utilizare eficientă a echipamentelor		X	Test nr. 3.1.
	a) dacă operaţiile sunt realizate eficient, în timp util şi la intervale bine stabilite			
	b) dacă datele obţinute, situaţiile de ieşire, rapoartele generate sunt stocate şi distribuite în siguranţă şi în timp util			FIAP nr. 3.1.

	c) dacă procedurile de salvare şi restaurare protejează în mod real datele şi aplicaţiile sistemului informatic			
	d) dacă procedurile de mentenanţa a echipamentelor sunt realizate corect şi la intervale de timp stabilite în funcţie de specificul fiecărei componente			
	e) dacă echipamentele hardware sunt asigurate corespunzător			
	f) dacă toate problemele de ordin tehnic apărute în cadrul proceselor, sunt raportate şi documentate corespunzător, astfel încât să se poată elabora soluţiile corespunzătoare de remediere a problemelor			
1.16.	Operaţiile sunt realizate într-o manieră eficientă, în timp util şi la intervale bine stabilite?	X		
1.17.	Există aplicaţii de programare şi executare automată a proceselor?	X		
1.18.	Se urmăreşte reducerea riscului ca un proces:	X		
1.19.	- să nu fie iniţiat corespunzător;	X		
1.20.	- să nu se execute în timpul planificat;	X		
1.21.	- să mărească intervalele de inactivitate	X		
1.22.	- să nu fie monitorizat din punct de vedere al modului şi timpului de execuţie?	X		
1.23.	Se asigură obţinerea rapoartelor detaliate privind procesele derulate?	X		
1.24.	În cazul apariţiei unor erori de funcţionare, administratorul responsabil poate localiza cât mai precis defecţiunea?	X		
1.25.	Se pot elabora soluţiile de remediere?	X		
1.26.	Se realizează monitorizarea operaţiilor din punctul de vedere al resurselor alocate şi utilizate efectiv: procesoare, memorii, mod de salvare?	X		
1.27	Se utilizează aplicaţii în acest scop?	X		
1.28.	Sunt identificate procesele care utilizează o cantitate mai mare de resurse decât cele care ăi sunt alocate?	X		
1.29.	În acest caz, se realizează redimensionări ale resurselor alocate?	X		
1.30.	Sunt identificate procesele care nu utilizează complet resursele disponibile?	X		
1.31.	În acest caz, se are în vedere o reducere a volumului resurselor alocate?	X		
1.32.	Datele obţinute, situaţiile de ieşite, rapoartele sunt stocate şi distribuite în siguranţă şi în timp util?	X		
1.33.	Procesele generează la sfârşitul execuţie diferite tipuri de rapoarte?	X		
1.34.	Aceste rapoarte sunt stocate în liste de aşteptare?	X		
1.35.	Aceste fişiere pot fi listate, copiate, mutate în vederea unor analize sau prelucrări ulterioare?	X		
1.36.	Mediile sau locaţiile de stocare sunt protejate împotriva deteriorării sau a accesului neautorizat?	X		
1.37.	Procedurile de salvare şi restaurare protejează în mod real datele şi aplicaţiile din sistemul informatic?	X		
1.38.	Acestea sunt corect planificate?	X		
1.39.	Sunt executate conform politicilor şi procedurilor de securitate stabilite?	X		
1.40.	Există proceduri de creare a copiilor de siguranţă realizate zilnic sau la intervale de câteva ore, pentru operaţiile curente?	X		
1.41.	Procedurile de salvare executate la intervale mai mari de timp includ copii complete ale sistemelor informatice: date, operaţii, programe?	X		
1.42.	Procedurile de mentenanţă a echipamentelor sunt realizate corect şi la intervale de timp stabilite în funcţie de specificul fiecărei componente?	X		
1.43.	Verificările tehnice sunt realizate ţinând cont de recomandările fabricantului?	X		
1.44.	Sunt realizate de personal autorizat / specializat?	X		
1.45.	Se respectă condiţiile de acordare a garanţiei?	X		
1.46.	Echipamentele hardware sunt asigurate corespunzător?	X		
1.47.	Există poliţe da asigurare încheiate pentru toate tipurile de riscuri?	X		
1.48.	Au fost estimate costurile implicate de eventuale daune?	X		
1.49.	Problemele de ordin tehnic, apărute în cadrul proceselor sunt raportate şi documentate corespunzător, astfel încât să se poată elabora soluţiile corespunzătoare de remediere a problemelor?	X		
1.50.	La nivelul entităţii este constituit un departament specializat în raportarea şi rezolvarea problemelor tehnice (help-desk)?	X		
1.51.	Se acordă suport tehnic utilizatorilor, prin linii telefonice dedicate, e-mail sau deplasări ale echipelor specializate?	X		
1.52.	Problemele apărute sunt definite corect?	X		

1.53.	Definirea cuprinde următoarele: - data apariţiei - etapele premergătoare - modul de manifestare a problemei - departamentul la care a apărut problema - datele de identificare a persoanei de contact?	X		
1.54.	Pentru definirea cât mai precisă a problemelor, se utilizează rapoartele generate automat de către aplicaţiile respective?	X		
1.55.	Se utilizează programe de monitorizare a sistemelor informatice?	X		
1.56.	Verificaţi dacă funcţiile legate de procese asigură integrarea acestora? a) dacă datele de intrare sunt validate b) dacă se verifică integritatea şi completitudinea datelor c) dacă se analizează eficienţa operaţiilor d) dacă se monitorizează şi se gestionează bazele de date		X	Test nr. 3.1. FIAP nr. 3.1.
1.57.	Se realizează validarea datelor de intrare?	X		
1.58.	Se realizează verificarea datelor introduse în sistemul informatic din punct de vedere al tipurilor de date, al lungimii acestora?	X		
1.59.	Pentru coduri, se impun reguli de formare şi validare a acestora?	X		
1.60.	Se utilizează proceduri automate de verificare a intrărilor?	X		
1.61.	Se realizează verificarea integrităţii şi completitudinii datelor?	X		
1.62.	Se utilizează proceduri de verificare a modului în care datele sunt introduse sau importate dintr-o altă aplicaţie?	X		
1.63.	Este avut în vedere riscul ca anumite date să fie pierdute, modificate, cu ocazia preluării dintr-o altă aplicaţie?	X		
1.64.	Se utilizează funcţii de verificare prin totaluri, chei şi algoritmi?	X		
1.65.	Se analizează eficienţa operaţiilor?	X		
1.66.	Se realizează o verificare a modului în care se realizează prelucrările, se implementează funcţiile şi programele?	X		
1.67.	Se urmăreşte modul de iniţiere a unor proceduri?	X		
1.68.	Se urmăreşte timpul de execuţie?	X		
1.69.	Se utilizează programe care să automatizeze aceste prelucrări?	X		
1.70.	Se monitorizează şi se gestionează bazele de date?	X		
1.71.	Se analizează modul în care se obţin rapoartele şi situaţiile de ieşire necesare diferitelor niveluri de management?	X		
1.72.	Se procedează la replicarea anumitor date, în vederea obţinerii unei mai mari flexibilităţi în interacţiunea cu acestea?	X		
1.73.	Utilizatorii finali pot obţine rapoarte diverse fără a afecta tranzacţiile curente?	X		
1.74.	Utilizatorii finali pot obţine datele necesare fără a dispune de cunoştinţe de specialitate?	X		
1.75.	Se acordă suport utilizatorilor pentru aplicaţiile existente?	X		
1.76.	Utilizatorii finali au cunoştinţe aprofundate privind prelucrarea datelor?	X		
1.77.	Interfaţa cu utilizatorul este prietenoasă?	X		
1.78.	Aplicaţiile pot fi utilizate uşor?	X		
1.79.	Există suport tehnic prin documente, sisteme de instruire, manuale, servicii puse la dispoziţie de către producătorii aplicaţiilor?	X		
1.80.	Se realizează administrarea aplicaţiilor?	X		
1.81.	Administrarea aplicaţiilor se realizează de către manageri sau persoane autorizate, specializate, care au ca atribuţii protejarea aplicaţiilor împotriva distrugerilor, a accesului neautorizat sau utilizări incorecte?	X		
1.82.	Administratorii asigură şi suportul tehnic pentru utilizatorii finali?	X		
1.83.	Se realizează rapoarte periodice asupra modului în care sunt utilizate aplicaţiile, alocarea resurselor, realizarea proceselor din cadrul entităţii?	X		
1.84.	Se realizează o analiză a automatizării unor proceduri manuale, a modului în care sunt obţinute şi analizate datele de ieşire, a uşurinţei în utilizarea aplicaţiilor?	X		
2.	**Responsabilitatea pentru supravegherea sarcinilor pe seturi de programe revine administratorilor**			
2.1.	Verificaţi dacă utilizatorii sunt instruiţi pentru însuşirea modului de lucru cu aplicaţia;	X		
2.2.	Verificaţi dacă noutăţile apărute în aplicaţie sunt comunicate utilizatorilor în timp adecvat;	X		
2.3.	Verificaţi dacă instruirea se realizează în conformitate cu documentaţia	X		

	aplicaţiei;			
2.4.	Verificaţi dacă utilizatorii primesc asistenţă în rularea aplicaţiilor ori de câte ori au nevoie;	X		
2.5.	Verificaţi dacă asistenţa tehnică este acordată în conformitate cu manualele de utilizare;	X		
2.6.	Verificaţi dacă responsabilitatea funcţionarii fiecărui program este în sarcina unui administrator;	X		
2.7.	Verificaţi dacă există o supraveghere permanentă în cadrul sistemului asupra derulării unui program sau aplicaţie;	X		
2.8.	Verificaţi dacă sistemul integrat permite depistarea automată a nefuncţionării unui program sau aplicaţie;	X		
3.	**Elaborarea planului anual de activitate**			
3.1.	Verificaţi gradul de acoperire cu activităţi care concură la realizarea planului anual de activitate:	X		
	a) activităţi identificate;			
	b) proceduri aferente realizării activităţilor			
	c) aprobarea procedurilor de către persoanele competente;			
	d) actualizarea sistematică a procedurilor;			
	e) respectarea principiul dublei semnături;			
	f) stabilirea responsabilităţilor persoanelor implicate în activitatea de implementare a sistemului IT;			
3.2.	Examinaţi dacă există atribuţii privind realizarea activităţilor cuprinse în planul anual de activitate în domeniul IT;	X		
3.3.	Analizaţi politica entităţii publice în domeniul IT şi stabiliţi dacă asigură atingerea obiectivelor entităţii publice;	X		
3.4.	Verificaţi dacă politica entităţii publice în domeniul IT se reflectă în planul anual de activitate în domeniul IT;	X		
3.5.	Examinaţi dacă managerii cu responsabilităţi în monitorizarea implementării politicii IT, au fost consultaţi la elaborarea planului anual de activitate în domeniul IT;	X		
3.6.	Analizaţi activitatea de actualizare a planului anual de activitate în domeniul IT;	X		
3.7.	Analizaţi dacă la elaborarea planului anual de activitate în domeniul IT s-au avut în vedere:	X		
	a) analiza sistemului de fundamentare a planului;			
	b) analiza corelării planului anual de activitate cu planul strategic;			
	c) evaluarea sistemului de prioritizare a activităţilor cuprinse în plan;			
	d) verificarea elaborării şi aprobării planului anual			
3.8.	Verificaţi documentele oficiale prin care au fost desemnate persoanele responsabile cu elaborarea şi actualizarea planului;	X		
3.9.	Examinaţi dacă responsabilităţile sunt clar definite pentru realizarea activităţilor IT;	X		
3.10.	Analizaţi dacă fişele posturilor pentru persoanele responsabile au fost actualizate;	X		
3.11.	Identificaţi deciziile luate în vederea elaborării şi actualizării planului şi analizaţi dacă acestea sunt în conformitate cu activităţile stabilite;	X		
3.12.	Examinaţi instrumentele utilizate pentru estimarea resurselor şi termenelor necesare pentru realizarea planului de activitate;	X		
3.13.	Verificaţi dacă prin elaborarea planului de activitate au fost stabilite plafoane bugetare pentru activităţile ce trebuie realizate şi procedurile ce vor fi aplicate în cazul în care acestea sunt depăşite;	X		
3.14.	Verificaţi dacă planul este aprobat de persoanele competente;	X		
3.15.	Analizaţi dacă planul aprobat este în conformitate cu politicile entităţii publice în domeniul IT;	X		
3.16.	Analizaţi împreună cu factorii responsabili de realizarea subsistemelor IT pentru funcţiile principale din cadrul entităţii publice dacă există departamente importante pentru care nu s-au realizat subsisteme IT;	X		
B.	**Managementul problemelor**			
1.	**Programele antivirus asigură protecţia aplicaţiilor**			
1.1.	Verificaţi dacă există proceduri pentru protecţia împotriva viruşilor, care să specifice modul de configurare al programului antivirus;	X		
1.2.	Verificaţi dacă există proceduri pentru protecţia împotriva viruşilor, care să specifice modul de actualizare a programului;	X		

1.3.	Verificaţi dacă riscurile reprezentate de viruşi sunt limitate ca urmare a alegerii celor mai potrivite soluţii antivirus;	X		
1.4.	Verificaţi dacă riscul de virusare al unui program sau aplicaţie este redus ca urmare a scanării antivirus pe servere, staţii de lucru sau poşta electronică;	X		
1.5.	Verificaţi dacă riscul de virusare este limitat urmare actualizării constante a programelor antivirus;	X		
1.6.	Verificaţi dacă programul antivirus scanează automat memoria calculatoarelor, fişierele, mediile de stocare;	X		
1.7.	Verificaţi dacă programul antivirus scanează traficul de date, inclusiv e-mail şi internet, în procesul de de-virusare;	X		
1.8.	Verificaţi dacă programul antivirus emite alerte atunci când detectează un virus;	X		
1.9.	Verificaţi dacă sunt efectuate verificări regulate pentru a se asigura că programul antivirus nu a fost dezactivat;	X		
1.10	Verificaţi dacă implementarea programelor anti-virus se realizează conform procedurilor		X	Test nr. 3.2 Foaie de lucru nr. 3.1. Listă de control nr. 3.1. FIAP nr. 3.2.
	a) instalarea unui program anti-virus adecvat necesităţilor utilizatorilor staţiilor de lucru			
	b) programul anti-virus verifică staţia de lucru la pornire			
	c) programul anti-virus monitorizează toate programele şi aplicaţiile active, mesajele primite şi verifică automat actualizările la intervale regulate			
	d) programul anti-virus se actualizează în reţea, astfel încât să protejeze eficient datele electronice împotriva viruşilor nou-apăruţi			
1.11.	Verificaţi dacă sunt efectuate controale regulate pentru a se asigura că configurarea programului de protecţie este corectă;	X		
1.12.	Verificaţi dacă utilizatorii sunt avertizaţi cu privire la pericolul reprezentat de viruşi;	X		
1.13.	Verificaţi dacă utilizatorii sunt avertizaţi cu privire la apariţia a noi tipuri de viruşi;	X		
1.14.	Verificaţi dacă utilizatorii sunt supravegheaţi permanent cu privire la utilizarea calculatoarelor şi păstrarea programelor sau aplicaţiilor curate.	X		
2.	**Implementarea subsistemelor IT**			
2.1.	Analizaţi criteriile avute în vedere la elaborarea subsistemelor IT pentru funcţiile principale;	X		
2.2.	Examinaţi eficienţa programului pentru instruirea utilizatorilor în vederea utilizării programelor şi aplicaţiilor;	X		
2.3.	Examinaţi dacă subsistemele IT acoperă în totalitate nevoile pentru funcţiile principale ale entităţii publice;	X		
2.4.	Analizaţi dacă nevoile de subsisteme IT pentru funcţiile nou-create au fost acoperite;	X		
2.5.	Verificaţi dacă departamentele înfiinţate ca urmare a funcţiilor principale nou-create au fost solicitate să-şi exprime cerinţele specifice privind realizarea unor subsisteme IT specifice activităţii lor;	X		
2.6.	Analizaţi existenţa corelării între termenele de realizare a subsistemelor;	X		
2.7.	Analizaţi procedurile pe baza cărora se realizează subsistemele IT şi stabiliţi dacă acestea sunt suficiente pentru implementarea acestor subsisteme în condiţii optime;	X		
2.8.	Stabiliţi dacă există studii de fezabilitate pentru subsistemele IT planificate.	X		
2.9.	Verificaţi dacă au fost stabilite responsabilităţi personalului de specialitate, pe linia implementării sistemului IT;	X		
2.10.	Comparaţi atribuţiile cuprinse în fişele posturilor cu cele din procedurile privind implementarea sistemului IT şi evaluaţi completitudinea preluării acestora;	X		
2.11.	Examinaţi cunoaşterea reglementărilor specifice privind implementarea sistemului IT de către responsabilii cu realizarea acestei activităţi;	X		
2.12.	Verificaţi dacă realizarea subsistemelor IT s-a realizat conform planificărilor;	X		
2.13.	Verificaţi dacă subsistemele IT au fost realizate la termenele stabilite;	X		Test nr. 3.3. Interviu nr. 3.1. FIAP nr. 3.3
2.14.	Examinaţi modul de alocare a resurselor necesare realizării subsistemelor IT;			
2.15.	Identificaţi evoluţiile tehnologice ce au determinat schimbarea programelor şi	X		

	aplicaţiilor planificate a fi implementate;			
2.16.	Verificaţi activitatea de monitorizare a implementării subsistemelor IT;	X		
2.17.	Verificaţi complementaritatea subsistemelor IT;	X		
2.18.	Verificaţi dacă există controale de sistem unitare implementate la nivelul subsistemelor IT;	X		
2.19.	Verificaţi dacă sunt implementate controale menite să analizeze datele introduse în aplicaţii;	X		
2.20.	Verificaţi dacă există controale efectuate pe parcursul procesării datelor şi dacă există rapoarte produse în caz de nerealizare a procesării;	X		
2.21.	Analizaţi dacă înregistrările privind controlul datelor rezultate în urma procesării asigură că aceste date sunt complete;	X		
2.22.	Analizaţi dacă datele transferate din alte aplicaţii sunt supuse unui proces standard de validare;	X		
2.23.	Verificaţi dacă sunt implementate controale care verifică înregistrările duble;	X		
2.24.	Verificaţi modul de autorizare electronică şi/sau manuală a tranzacţiilor;	X		
2.25.	Verificaţi dacă operaţiile privind efectuarea tranzacţiilor se realizează numai de la computere definite în prealabil;	X		
2.26.	Examinaţi dacă modul de arhivare a înregistrărilor se face astfel încât să permită urmărirea tranzacţiilor efectuate din faza de iniţiere până la finalizarea lor;	X		
2.27.	Verificaţi modul de raportare a schimbărilor operate la nivelul datelor salvate;	X		
2.28.	Examinaţi dacă utilizatorii înţeleg controalele implementate;	X		
2.29.	Verificaţi funcţionalitatea subsistemelor IT în reţea;	X		
2.30.	Verificaţi respectarea procedurilor privind transmiterea datelor în reţea;	X		
2.31.	Analizaţi dacă subsistemele componente programelor asigură integrarea acestora;	X		
2.32.	Analizaţi modul de soluţionare a neconcordanţelor apărute în integrarea subsistemelor;	X		
2.33.	Examinaţi dacă sunt elaborate manualele de utilizare şi manualele de operare;	X		
2.34.	Analizaţi dacă manualele de utilizare şi de operare sunt comprehensive şi corespund nevoilor utilizatorilor;	X		
2.35.	Verificaţi existenţa programelor de instruire a utilizatorilor subsistemelor IT;	X		
2.36.	Verificaţi existenţa controalelor asupra datelor introduse în aplicaţii;	X		
2.37.	Verificaţi existenţa controalelor pe parcursul procesării datelor şi generarea rapoartelor privind erorile de procesare;	X		
2.38.	Verificaţi existenţa controalelor asupra datelor rezultate în urma procesării, astfel încât să se asigure că acestea sunt complete;	X		
2.39.	Verificaţi dacă subsistemele IT realizate respectă cerinţele stabilite prin politica, procedurile şi studiile de fezabilitate întocmite;	X		
2.40.	Verificaţi dacă subsistemele IT au fost realizate la termenele stabilite;	X		
2.41.	Verificaţi dacă resurselor necesare realizării subsistemelor IT au fost alocate conform planului anual de activitate;	X		
	Este analizat modul de rezolvare şi prevenire a incidentelor care afectează funcţionarea normală a serviciilor IT ale entităţii publice?	X		
	Managementul problemelor asigură corectarea erorilor, prevenind reapariţia acestora?	X		
	Se foloseşte întreţinerea preventivă pentru reducerea probabilităţii ca aceste erori să mai apară?	X		
	Atunci când o problemă nu poate fi rezolvată de prima linie de asistenţă, aceasta este direcţionată către ajutorul din linia a doua?	X		
	Se au în vedere următoarele cinci faze de bază:	X		
	1. iniţierea – raportarea problemei	X		
	2. planificarea – definirea problemei şi conceperea unui plan de atac	X		
	3. execuţia – desfăşurarea planului de atac, adunarea de date, urmărirea problemei, cercetarea tehnică, codarea şi testarea ulterioară	X		
	4. monitorizarea şi analiza – monitorizarea şi confirmare rezultatelor de către utilizatorii finali	X		
	5. încheierea – documentarea problemei şi a acţiunilor de corecţie.	X		
C.	**Funcţionalitatea departamentului IT**			
1.	**Organizarea funcţională a departamentului IT**			
1.1.	Analizaţi dacă departamentul IT este subordonat unui nivel managerial corespunzător;	X		

1.2.	Comparaţi atribuţiile cuprinse în fişele posturilor cu cele din proceduri şi evaluaţi completitudinea acestora;	X		
1.3.	Verificaţi dacă organigrama departamentului IT corespunde organizării actuale a departamentului;	X		
1.4.	Verificaţi dacă organigrama defineşte nivelurile ierarhice din cadrul departamentului;	X		
1.5.	Verificaţi dacă organigrama defineşte relaţiile organizatorice dintre compartimentele funcţionale ale departamentului IT;	X		
1.6.	Verificaţi dacă organigrama stabileşte numărul de posturi pentru fiecare compartiment funcţional al departamentului IT;	X		
1.7.	Verificaţi dacă numărul de posturi existent în cadrul departamentului IT asigură realizarea activităţilor şi atribuţiilor;	X		
1.8.	Analizaţi dacă atribuţiile departamentului sunt definite corect şi în totalitate în cadrul ROF-ului;	X		
1.9.	Verificaţi dacă activităţile sunt repartizate corect în cadrul compartimentelor, în funcţie de atribuţiile alocate;	X		
1.10.	Verificaţi dacă sarcinile stabilite prin fişele posturilor asigură realizarea în totalitate a activităţilor;	X		
1.11.	Verificaţi dacă atribuţiile sunt repartizate omogen pe compartimente, asigurând funcţionalitatea acestora;	X		
1.12.	Analizaţi gradul de ocupare a posturilor în cadrul departamentului IT;	X		
1.13.	Analizaţi modul în care se asigură continuitatea activităţilor în funcţie de pregătirea salariaţilor şi vechimea în muncă;	X		
1.14.	Analizaţi dotarea departamentului cu echipamente hard şi soft adecvate pentru desfăşurarea activităţilor specifice, astfel:	X		
1.15.	a) număr suficient de calculatoare dotate corespunzător;			
	b) număr suficient de servere			
	c) număr suficient de echipamente auxiliare (imprimante, xerox-uri, scanere, conexiuni la intranet/Internet)			
	d) programe IT adecvate			
1.16.	Verificaţi dacă fişele posturilor stabilesc responsabilităţi pentru toate activităţile desfăşurate;	X		
1.17.	Verificaţi dacă actualizarea fişelor posturilor se realizează periodic în funcţie de modificarea activităţilor sau sarcinilor posturilor;	X		
1.18.	Analizaţi dacă pregătirea şi calificarea salariaţilor departamentului IT asigură funcţionalitatea programelor, aplicaţiilor, echipamentelor şi dezvoltarea informaţională a entităţii;	X		
1.19.	Analizaţi dacă planurile de pregătire profesională continuă asigură dezvoltarea cunoştinţelor şi aptitudinilor personalului;	X		
1.20.	Verificaţi dacă se realizează evaluarea performanţelor personalului departamentului IT;	X		
1.21.	Verificaţi dacă există concordanţă între rapoartele de evaluare şi programele de instruire la nivel individual;	X		
1.22.	Verificaţi dacă evaluarea performanţelor asigură corectitudinea aprecierii realizării obiectivelor individuale;	X		
1.23.	Verificaţi dacă criteriile de performanţă sunt stabilite corect în funcţie de gradul de îndeplinire a obiectivelor;	X		
1.24.	Verificaţi dacă evaluarea performanţelor personalului contribuie la dezvoltarea profesională a acestuia;	X		
1.25.	Verificaţi dacă obiectivele individuale sunt stabilite corect în conformitate cu sarcinile atribuite postului;	X		
1.26.	Analizaţi dacă acţiunile necesare pentru realizarea obiectivelor individuale şi realizate efectiv pentru implementarea acestora corespund în totalitate cu acţiunile repartizate postului potrivit fişei postului;	X		
1.27.	Verificaţi dacă există o politică unitară privind gestionarea riscurilor;	X		
1.28.	Verificaţi dacă exista un sistem de gestionare a riscurilor;	X		
1.29.	Analizaţi dacă este desemnat un responsabil privind gestionarea riscurilor la nivelul departamentului IT;	X		
1.30.	Verificaţi existenţa Registrului riscurilor la nivelul Departamentului IT şi modul de conducere al acestuia;	X		
1.31.	Verificaţi dacă sunt stabilite responsabilităţi pentru actualizarea procedurilor de lucru şi instrucţiunilor privind derularea programelor şi aplicaţiilor;	X		

1.32.	Verificaţi condiţiile şi criteriile privind delegarea sarcinilor şi atribuţiilor;	X		
1.33.	Analizaţi sistemul de control managerial exercitat la nivelul departamentului;	X		
1.34.	Examinaţi dacă fişele posturilor stabilesc corect nivelul postului şi complexitatea activităţilor;	X		
1.35.	Verificaţi dacă nivelul de cunoştinţe şi deprinderi al ocupantului postului corespunde necesităţilor şi nivelului postului;	X		
1.36.	Verificarea dacă se respecta principiul segregării atribuţiilor în realizarea sarcinilor şi activităţilor.	X		
2.	**Asigurarea caracterului secret al datelor**			
2.1.	Verificaţi dacă aplicaţiile respectă schemele privind nivele de secretizare în conformitate cu standardele organizaţiei;	X		
2.2.	Verificaţi dacă schema de secretizare a datelor este utilizată pentru determinarea nivelelor diferite de importanţă a sistemelor sau informaţiilor;	X		
2.3.	Verificaţi dacă schema de secretizare a datelor este utilizată pentru determinarea nivelelor diferite de sensibilitate a informaţiilor sau sistemelor;	X		
2.4.	Verificaţi dacă secretizarea informaţiilor ia în considerare impactul pierderii confidenţialităţii, integrităţii sau disponibilităţilor informaţiei asupra activităţii;	X		
2.5.	Verificaţi dacă secretizarea se aplică informaţiilor, sistemelor sau aplicaţiilor şi programelor;	X		
2.6.	Verificaţi dacă secretizarea informaţiei include identitatea persoanelor cu responsabilităţi primare;	X		
2.7.	Verificaţi dacă secretizarea informaţiei este aprobată de emitentul informaţiei;	X		
2.8.	Verificaţi dacă performanţa sistemelor este monitorizată comparativ cu ţintele stabilite;	X		
2.9.	Verificaţi dacă performanţa sistemelor este monitorizată utilizând programe de monitorizare automată;	X		
2.10.	Verificaţi dacă disponibilitatea sistemelor este apreciată din punctul de vedere al utilizatorilor activităţii	X		
2.11.	Verificaţi dacă monitorizarea sistemelor se concentrează pe punctele vulnerabile;	X		
2.12.	Verificaţi dacă mecanismele de detectare asigură semnalizarea atacurilor informatice;	X		
2.13.	Verificaţi dacă mecanismele de detectare includ un proces de actualizare a programelor utilizate în acest scop;	X		
2.14.	Verificaţi dacă mecanismele de detectare emit alerte când se înregistrează activităţi suspecte;	X		
2.15.	Verificaţi dacă rapoartele obţinute în urma procesărilor sunt verificate pentru a descoperi orice utilizare neobişnuită a sistemelor;	X		
2.16.	Verificaţi dacă sunt înregistrate toate evenimentele cheie în cadrul unui sistem;	X		
2.17.	Verificaţi dacă conducerea IT autorizează înregistrarea activităţilor şi revizuirea proceselor care urmează a fi aplicate;	X		
2.18.	Verificaţi dacă înregistrările conţin date referitoare la oprirea/pornirea sistemelor şi proceselor cheie, situaţiile de eroare sau de excepţie, acces sau schimbări ale fişierelor sau programelor;	X		
2.19.	Verificaţi dacă informaţiile înregistrate identifică programele speciale şi informaţiile accesate, data accesării, căile de acces, schimbarea parametrilor de înregistrare în sistem;	X		
2.20.	Verificaţi dacă înregistrările sunt păstrate suficient timp respectând cerinţele utilizatorilor şi pentru a putea fi revizuite;	X		
2.21	Verificaţi dacă revizuirea înregistrărilor este fundamentată pe o evaluare a impactului unor evenimente asupra activităţilor şi este realizată cu instrumente automate;	X		
D.	**Mentenanţa echipamentelor**			
1.	**Întreţinerea calculatorului şi a echipamentelor**			
1.1.	Verificaţi dacă operaţiunile de mentenanţă se efectuează conform planificării, folosindu-se procedurile standard de testare;	X		
1.2.	Verificaţi dacă disfuncţionalităţile hardware sunt identificate corect şi în timp util;	X		
1.3.	Verificaţi dacă disfuncţiunile identificate sunt analizate şi înlăturate în conformitate cu instrucţiunile şi manualele de întreţinere;	X		
1.4.	Verificaţi dacă produsele software sunt instalate şi configurate conform documentaţiilor şi indicaţiilor furnizorilor;	X		

1.5.	Analizaţi dacă funcţionarea sistemului de operare este verificată periodic utilizând instrumente de testare specializate;	X		
1.6.	Analizaţi dacă funcţionarea aplicaţiilor este verificată periodic,	X		
1.7.	Verificaţi dacă parametrii referitori la starea de funcţionare urmare aplicării procedurilor de testare specializate sunt înregistraţi în jurnale;	X		
1.8.	Verificaţi dacă neconformităţile sunt analizate şi readuse la valorile normale;	X		
1.9.	Verificaţi dacă corecţia erorilor se realizează în limita competenţelor	X		
2.	**Instalarea şi configurarea calculatorului**			
2.1.	Verificaţi dacă sursele de alimentare sunt alese şi verificate în conformitate cu cerinţele tehnice;	X		
2.2.	Verificaţi dacă echipamentele periferice sunt instalate şi conectate conform documentaţiei;	X		
2.3.	Verificaţi dacă instalarea respectă condiţiile de calitate şi eficienţă din manuale şi instrucţiuni;	X		
2.4.	Verificaţi dacă conectarea în reţea respectă standardele în vigoare,	X		
2.5.	Verificaţi dacă sistemul de operare, componentele software, componentele de acces în reţea sunt instalate şi configurate corect;	X		
2.6.	Verificaţi dacă partajarea resurselor se face verificând tipul de acces permis utilizatorilor;	X		
2.7.	Verificaţi dacă funcţionarea aplicaţiilor este testată periodic;	X		
D.	**Utilizarea echipamentelor**			
1.	**Realizarea eficientă a operaţiilor în cadrul departamentului IT**			
1.1.	Verificaţi dacă este analizat impactul produs de funcţionarea incorectă a unei operaţii asupra întregului sistem;	X		
1.2.	Verificaţi dacă analiza a ţinut cont de funcţiile desfăşurate în cadrul sistemului;	X		
1.3.	Verificaţi dacă operaţiile IT sunt realizate într-o manieră eficientă, în timp util şi la intervale bine stabilite?	X		
1.4.	Verificaţi dacă procesele IT sunt iniţiate corespunzător;	X		
1.5.	Verificaţi dacă procesele IT se execută în timpul planificat;	X		
1.6.	Verificaţi dacă procesele IT sunt monitorizate din punct de vedere al modului şi timpului de execuţie;	X		
1.7.	Verificaţi dacă se asigură generarea rapoartelor detaliate privind procesele derulate;	X		
1.8.	Verificaţi dacă în cazul apariţiei unor erori de funcţionare, administratorul responsabil le poate localiza cât mai precis;	X		
1.9.	Verificaţi dacă se realizează monitorizarea operaţiilor din punctul de vedere al resurselor alocate şi utilizate: procesoare, memorii, mod de salvare;	X		
1.10.	Verificaţi dacă sunt identificate procesele care utilizează o cantitate mai mare de resurse şi dacă acestea sunt redimensionate;	X		
1.11.	Verificaţi dacă datele obţinute, situaţiile de ieşire, rapoartele sunt stocate şi distribuite în siguranţă şi în timp util;	X		
1.12.	Verificaţi dacă procesele generează la sfârşitul execuţiei diferite tipuri de rapoarte;	X		
1.13.	Verificaţi dacă rapoartele generate sunt stocate în liste de aşteptare;	X		
1.14.	Verificaţi dacă mediile sau locaţiile de stocare sunt protejate împotriva deteriorării sau a accesului neautorizat;	X		
1.15.	Verificaţi dacă procedurile de mentenanţă a echipamentelor sunt realizate corect şi la intervale de timp stabilite în funcţie de specificul fiecărei componente;	X		
1.16.	Examinaţi dacă verificările tehnice sunt realizate ţinând cont de recomandările producătorului;	X		
1.17.	Examinaţi dacă verificările tehnice sunt realizate de personal autorizat / specializat;	X		
1.18.	Verificaţi dacă echipamentele hardware sunt asigurate corespunzător;	X		
1.19.	Verificaţi dacă problemele de ordin tehnic, apărute în cadrul proceselor sunt raportate şi documentate corespunzător, astfel încât să se poată elabora soluţiile corespunzătoare de remediere;	X		
1.20	Verificaţi dacă se acordă suport tehnic utilizatorilor, inclusiv prin deplasări ale echipelor specializate;	X		
1.21.	Verificaţi dacă problemele apărute sunt definite prin specificarea datei apariţiei problemei, modul de manifestare al problemei, departamentul unde a apărut problema;	X		
1.22	Verificaţi dacă pentru identificarea cât mai precisă a problemelor, se utilizează	X		

	rapoartele generate automat de către aplicaţiile respective;			
2.	**Administrarea eficientă a aplicaţiilor şi programelor**			
2.1.	Verificaţi dacă se realizează validarea datelor de intrare;			
2.2.	Examinaţi dacă se realizează verificarea datelor introduse în sistemul informatic din punct de vedere al tipurilor de date, al dimensiunii acestora;	X		
2.3.	Verificaţi dacă pentru coduri, se impun reguli de creare şi validare a acestora;	X		
2.4.	Examinaţi dacă se utilizează proceduri automate de verificare a datelor de intrare;	X		
2.5.	Examinaţi dacă se utilizează proceduri de verificare a modului în care datele sunt introduse sau importate dintr-o altă aplicaţie;	X		
2.6.	Verificaţi dacă este avut în vedere riscul ca anumite date să fie pierdute, modificate, cu ocazia preluării dintr-o altă aplicaţie;	X		
2.7.	Verificaţi dacă se utilizează funcţii de verificare prin totaluri, chei şi algoritmi;	X		
2.8.	Examinaţi dacă se realizează o verificare a modului în care se efectuează prelucrările, se implementează funcţiile şi programele;	X		
2.9.	Verificaţi dacă se monitorizează şi se gestionează bazele de date;	X		
2.10.	Verificaţi dacă se analizează modul în care se obţin rapoartele şi situaţiile de ieşire necesare diferitelor niveluri de management;	X		
2.11.	Verificaţi dacă utilizatorii finali pot obţine rapoarte diverse fără a afecta tranzacţiile curente;	X		
2.12.	Verificaţi dacă se acordă suport tehnic utilizatorilor pentru aplicaţiile existente;	X		
2.13.	Verificaţi dacă utilizatorii finali au cunoştinţe aprofundate privind prelucrarea datelor;	X		
2.14.	Verificaţi dacă interfaţa cu utilizatorul este prietenoasă;	X		
2.15.	Verificaţi dacă aplicaţiile pot fi utilizate uşor;	X		
2.16.	Verificaţi dacă există suport tehnic prin documente, sisteme de instruire, manuale, servicii puse la dispoziţie de către producătorii aplicaţiilor;	X		
2.17.	Verificaţi dacă se realizează administrarea aplicaţiilor;	X		
2.18.	Verificaţi dacă administrarea aplicaţiilor se realizează de către administratori autorizaţi, care au ca atribuţii protejarea aplicaţiilor împotriva distrugerilor, a accesului neautorizat sau utilizării incorecte;	X		
2.19.	Verificaţi dacă administratorii asigură şi suportul tehnic pentru utilizatorii finali;	X		
2.20.	Verificaţi dacă se realizează rapoarte periodice asupra modului în care sunt utilizate aplicaţiile, alocarea resurselor, realizarea proceselor din cadrul entităţii;	X		
2.21.	Verificaţi dacă se realizează o analiză a automatizării unor proceduri manuale, a modului în care sunt obţinute şi analizate datele de ieşire, a uşurinţei în utilizarea aplicaţiilor;	X		
3.	**Evaluarea problemelor şi soluţionarea acestora**			
3.1.	Verificaţi dacă este analizat modul de rezolvare şi prevenire a incidentelor care afectează funcţionarea normală a serviciilor IT;	X		
3.2.	Verificaţi dacă măsurile de corectare a erorilor asigură prevenirea reapariţiei acestora;	X		
3.3.	Verificaţi dacă este utilizat controlul preventiv pentru reducerea probabilităţii ca erorile soluţionate să mai apară;	X		
3.4.	Verificaţi dacă utilizarea unei aplicaţii asigură:		X	Test nr. 3.4. Foaie de lucru nr. 3.2. Listă de control nr. 3.2.
	a) controlul datelor introduse în aplicaţii			
	b) controlul pe parcursul procesării datelor şi rapoartelor produse în caz de nerealizare a procesării			
	c) controlul datelor rezultate în urma procesării, astfel încât să se asigure că aceste date sunt complete			
	d) validarea datelor transferate din alte aplicaţii			
	e) controalelor verifică înregistrările duble			
	f) autorizarea electronică şi/sau manuală a tranzacţiilor			
	g) efectuarea tranzacţiilor numai de la computere definite în prealabil			
	h) păstrarea integrală a înregistrărilor astfel încât să se poată urmări tranzacţiile efectuate din faza de iniţiere până la finalizarea lor			
	Înţelegerea controalelor implementate de către utilizatori			
3.4.	Verificaţi dacă soluţionarea unei probleme are în vedere următoarele etape:	X		
.	a) raportarea problemei;			
	b) definirea problemei şi conceperea unui plan de atac;			

	c) desfăşurarea planului de atac, adunarea de date, urmărirea problemei, cercetarea tehnică, codarea şi testarea ulterioară;			
	d) monitorizarea şi confirmare rezultatelor de către utilizatorii finali;			
	e) documentarea problemei şi a acţiunilor de corecţie.			
3.5.	Verificaţi dacă procedurile de salvare sunt executate la intervale optime şi includ copii complete ale sistemelor informatice: date, operaţii, programe;	X		

Auditori,

Popescu Sorin
Radu George

Procedura - P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

TEST NR. 3.1

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 16.09.2009
Avizat: Dumitru Daniel Data: 16.09.2009

Obiectul testului	Performanţa, capacitatea şi disponibilitatea sistemelor informatice este monitorizată de administratorii de reţea
Obiectivele testului	Controlul operaţiilor realizate de sistemele informatice.
Descrierea testului	Echipa de auditori a procedat la controlul operaţiilor realizate de sistemele informatice, analizând modul în care sunt procesate datele, realizate tranzacţiile şi executate funcţiile aplicaţiilor, pentru a implementa corect procesele desfăşurate în cadrul entităţii. Întrucât aceste operaţii sunt interdependente, auditorii nu au analizat separat fiecare funcţie, ci au considerat procesele desfăşurate în cadrul entităţii ca un tot unitar. Pentru a creşte eficienţa analizei operaţiilor, auditorii le-au împărţit în două categorii: funcţii tehnice şi funcţii legate de procese. Testarea a urmărit următoarele aspecte, stabilite în Lista de verificare 3: **A. funcţii tehnice:** 1. - dacă operaţiile sunt realizate eficient, în timp util şi la intervale bine stabilite; 2. - dacă datele obţinute, situaţiile de ieşire, rapoartele generate sunt stocate şi distribuite în siguranţă şi în timp util; 3. - dacă procedurile de salvare şi restaurare protejează în mod real datele şi aplicaţiile sistemului informatic 4. - dacă procedurile de mentenanţă a echipamentelor sunt realizate corect şi la intervale de timp stabilite în funcţie de specificul fiecărei componente; 5. - dacă echipamentele hardware sunt asigurate corespunzător; 6. - dacă toate problemele de ordin tehnic apărute în cadrul proceselor, sunt raportate şi documentate corespunzător, astfel încât să se poată elabora soluţiile corespunzătoare de remediere a problemelor. **B. funcţii legate de procese:** 7. - dacă datele de intrare sunt validate; 8. - dacă se verifică integritatea şi completitudinea datelor 9. - dacă se analizează eficienţa operaţiilor 10. - dacă se monitorizează şi se gestionează bazele de date. Testul s-a materializat în verificarea pe teren a implementării controlului privind operaţiunile sistemelor informatice.
Constatări	În urma analizei modului de implementare a controlului privind operaţiunile sistemelor informatice, echipa de auditori a constatat următoarele: 1. - dacă operaţiile sunt realizate eficient, în timp util şi la intervale bine stabilite; Echipa de auditori a constatat că la nivelul entităţii se utilizează aplicaţii de programare şi executare automată a proceselor. Acestea reduc riscul ca un proces să nu fie iniţiat corespunzător, să nu se execute în timpul planificat, reduce la minim intervalele de inactivitate, iar fiecare proces poate fi monitorizat din punct de vedere al modului şi al timpului de execuţie. Aplicaţiile de planificare automată generează rapoarte detaliate despre procesele derulate, iar în cazul apariţiei unor erori de funcţionare, permit administratorului responsabil să localizeze cât mai precis defecţiunea şi să elaboreze soluţii de remediere.

	În urma analizei modului de alocare şi utilizare efectivă a resurselor (procesoare, memorie, spaţiu ocupat pe hard-disk, mod de salvare etc.), echipa de auditori a constatat că nu au fost realizată o monitorizare corespunzătoare a operaţiilor desfăşurate, care să ţină cont alocarea resurselor. În acest sens, a fost constatat faptul că procesoarele şi memoriile de lucru ale calculatoarelor din cadrul departamentului IT, pe care sunt instalate programele antivirus şi care asigură o supraveghere permanentă a reţelelor, sunt mai lente decât componentele similare aflate în configuraţiile calculatoarelor din cadrul Direcţiei Generale de Investiţii, Achiziţii Publice şi Servicii Interne. De asemenea, s-a constatat că hard-disk-urile din configuraţiile aceloraşi calculatoare, de la nivelul Direcţiei Generale de Investiţii, Achiziţii Publice şi Servicii Interne, dispun de capacităţi excedentare, în majoritatea cazurilor fiind ocupate în procent de maxim 10-15%. 2. - dacă datele obţinute, situaţiile de ieşire, rapoartele generate sunt stocate şi distribuite în siguranţă şi în timp util; Echipa de auditori a constatat că majoritatea proceselor generează la terminarea execuţiei diferite tipuri de fişiere. De cele mai multe ori, aceste fişiere sunt stocate într-o listă de aşteptare, putând fi copiate, mutate în vederea unor analize sau prelucrări ulterioare. Echipa de auditori a observat că listele generate în urma prelucrărilor pe un anumit computer puteau fi vizualizate şi modificate de pe toate celelalte computere din reţea, accesul la ele nefiind restricţionat. 3. - dacă procedurile de salvare şi restaurare protejează în mod real datele şi aplicaţiile sistemului informatic. Echipa de auditori a constatat că procedurile de salvare sunt corect planificate şi sunt executate conform politicilor şi procedurilor de securitate stabilite. În plus, s-a constat faptul că există proceduri de creare a copiilor de siguranţă realizate zilnic sau la intervale de câteva ore, pentru operaţiunile curente, şi proceduri de salvare executate la intervale mai mari de timp, care includ copii complete ale sistemelor informatice: date, operaţiuni, programe. 4. - dacă procedurile de mentenanţă a echipamentelor sunt realizate corect şi la intervale de timp stabilite în funcţie de specificul fiecărei componente; Echipa de auditori analizat procedurile de mentenanţă privind sistemele IT. În acest sens, au fost inventariate intervenţiile efectuate asupra computerelor şi imprimantelor/copiatoarelor aflate în cadrul Biroului Multiplicare, din cadrul Serviciului Administrativ şi Gospodărirea Patrimoniului. Astfel, s-a constatat că 3 din cele 7 imprimante care deserveau necesităţile biroului foloseau consumabile compatibile sau care au fost reîncărcate, fapt ce a condus la o calitate mai slabă a printărilor, dar şi la pierderea garanţiei oferită de furnizor. De asemenea, s-a constatat că două din cele 6 computere din cadrul aceluiaşi birou se blocau în cazul efectuării unor operaţiuni mai complexe. Acest fapt se datorează faptului că sursele de alimentare iniţiale s-au defectat şi au fost înlocuite cu unele asemănătoare ca design, dar care nu ofereau suficientă energie pentru prelucrările mai complexe. Întrucât aceste surse nu respectau specificaţiile fabricantului, a fost pierdută garanţia respectivelor echipamente. În cazul multiplicatoarelor de mare capacitate, s-a constatat că în 2 din 3 cazuri, a fost depăşit termenul la care trebuia efectuată inspecţia tehnică periodică, fapt ce a condus la o uzură mai pronunţată a acestora, dar şi la ieşirea mai rapidă din garanţie. Au fost constatate 2 computere care aveau sigiliile furnizorului rupte, fapt ce denotă intervenţii ale personalului neautorizat. Şi aceste aspecte au condus la pierderea garanţiei. 5. - dacă echipamentele hardware sunt asigurate corespunzător; Echipa de auditori a constatat că pentru echipamentele hardware nu au fost încheiate polițe de asigurare, care să acopere diferitele tipuri de riscuri şi costurile implicate de eventuale daune. 6. - dacă toate problemele de ordin tehnic apărute în cadrul proceselor, sunt raportate şi documentate corespunzător, astfel încât să se poată elabora soluţiile corespunzătoare de remediere a problemelor. Analizând modul de soluţionare a unui număr de 6 probleme de ordin tehnic apărute în cadrul proceselor, echipa de auditori a constatat că au fost efectuate intervenţii punctuale din partea personalului specializat din cadrul departamentului IT al entităţii, urmărindu-se strict remedierea respectivelor probleme şi fără a se avea în vedere etapele premergătoare apariţiei problemei, cauzele şi modul de propagare etc.

	B. funcţii legate de procese: 7. - dacă datele de intrare sunt validate; 8. - dacă se verifică integritatea şi completitudinea datelor 9. - dacă se analizează eficienţa operaţiilor 10. - dacă se monitorizează şi se gestionează bazele de date. 7. - dacă datele de intrare sunt validate; Echipa de auditori a constatat că la nivelul entităţii au fost realizate verificări ale datelor introduse în sistemul informatic din punct de vedere al tipurilor de date, al lungimii acestora, iar pentru coduri au fost utilizate reguli speciale de creare şi validare a acestora. De asemenea, se folosesc proceduri automate de verificare a intrărilor. 8. - dacă se verifică integritatea şi completitudinea datelor Echipa de auditori a verificat existenţa unor proceduri de verificare a modului în care datele au fost introduse sau importate dintr-o aplicaţie în alta. În aceste situaţii, anumite înregistrări se pot pierde sau datele pot fi modificate, ducând la apariţia unor probleme în prelucrare. Aceste aspecte au făcut obiectul FIAP-ului de la testul nr. 6. Recomandare: Utilizarea unor funcţii de verificare prin totaluri, chei şi algoritmi. 9. - dacă se analizează eficienţa operaţiilor Analizând modul de efectuare a verificărilor asupra prelucrărilor, implementării funcţiilor şi programelor, asupra modului de iniţiere a unor proceduri sau a timpului de execuţie, echipa de auditori a constatat că o anumită parte din aceste verificări se realizează manual. 10. - dacă se monitorizează şi se gestionează bazele de date. În urma analizei modului de monitorizare şi gestionare a bazelor de date, echipa de auditori a concluzionat că rapoartele şi situaţiile de ieşire oferă suficiente informaţii managementului în vederea luării deciziilor corecte.
Concluzii	În urma deficienţelor constatate cu ocazia testării operaţiunilor efectuate de sistemele informatice, s-a întocmit FIAP-ul nr. 3.1.

Auditor intern,
Radu George

Supervizor,
Dumitru Daniel

Procedura - P08:	**Colectarea dovezilor**

Entitatea Publică
Serviciul Audit Public Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI NR. 3.1

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.09.2009
Avizat: Dumitru Daniel Data: 15.09.2009

PROBLEMA	Existenţa unor controale interne slabe privind managementul operaţiunilor IT, reflectate în disfuncţii legate de gestionarea acestora.
CONSTATĂRI	Echipa de auditori a constatat următoarele: 1. în urma analizei modului de alocare şi utilizare efectivă a resurselor IT disponibile, echipa de auditori a constatat că unele departamente dispun de resurse insuficiente (departamentul IT), în timp ce altele dispun de resurse excedentare (Direcţia Generală de Investiţii, Achiziţii Publice şi Servicii Interne), fiind utilizate în proporţie de max. 10-15%. 2. Echipa de auditori a constatat că listele generate în urma prelucrărilor pe un anumit computer puteau fi vizualizate şi modificate de pe toate celelalte computere din reţea, accesul la ele nefiind restricţionat. 4. În urma inventarierii intervenţiilor efectuate asupra computerelor şi imprimantelor/copiatoarelor aflate în cadrul biroului Multiplicare, s-a constatat că procedurile privind mentenanţa nu au fost realizate cu respectarea specificaţiilor producătorului, de către personal autorizat, fapt ce a condus, în majoritatea cazurilor, la pierderea garanţiei, dar a fost afectată şi performanţa echipamentelor respective. 6. Analizând modul de soluţionare a unui număr de 6 probleme de ordin tehnic apărute în cadrul proceselor, echipa de auditori a constatat că au fost efectuate intervenţii punctuale din partea personalului specializat din cadrul departamentului IT al entităţii, urmărindu-se strict remedierea respectivelor probleme şi fără a se avea în vedere etapele premergătoare apariţiei problemei, cauzele şi modul de propagare etc. 9. - dacă se analizează eficienţa operaţiilor Analizând modul de efectuare a verificărilor asupra prelucrărilor, implementării funcţiilor şi programelor, asupra modului de iniţiere a unor proceduri sau a timpului de execuţie, echipa de auditori a constatat că o anumită parte din aceste verificări se realizează manual.
CAUZE	1. Lipsa unei imagini de ansamblu asupra alocării şi utilizării efective a resurselor de IT. 2. Lipsa protecţiilor şi a restricţionării accesului la rezultatele prelucrărilor. 4. Alocarea de fonduri insuficiente pentru achiziţia de consumabile originale. De asemenea, anumite probleme tehnice au trebuit soluţionate în regim de urgenţă, fapt ce a fost realizat prin utilizarea unor componente luate de pe alte sisteme nefuncţionale, fără a avea în vedere respectarea în totalitate a cerinţelor producătorului. 6. Datorită insuficienţei personalului de specialitate, anumite intervenţii tehnice s-au limitat doar la remedierea problemelor punctuale, fără a avea în

	vedere etapele premergătoare, cauzele, şi modul de propagare ale acestora. Neconstituirea la nivelul departamentului IT a unui colectiv însărcinat cu raportarea şi soluţionarea rapidă a problemelor de ordin tehnic (Help-desk). Lipsa utilizării programelor de monitorizare a sistemelor informatice. 9. Neutilizarea unor programe care să automatizeze într-un grad cât mai mare verificările efectuate asupra operaţiile informatice.
CONSECINŢE	Anumite procese de importanţă vitală dispun de resurse insuficiente, în timp ce anumite resurse nu sunt complet utilizate. Vulnerabilitate ridicată a rezultatelor prelucrărilor. Calitate scăzută a rezultatelor prelucrărilor. Pierderea garanţiilor pentru anumite echipamente. Uzura mai rapidă a acestora. Înlăturarea doar a consecinţelor anumitor probleme de ordin tehnic, nu şi a cauzelor. Verificarea manuală a operaţiunilor informatice prezintă un risc mai mare de nedetectare a problemelor, decât verificarea automatizată.
RECOMANDĂRI	Implementarea unei aplicaţii care să monitorizeze alocarea şi utilizarea resurselor în funcţie de gradul de complexitate al operaţiilor efectuate. Urmărirea în permanenţă a echilibrului între necesităţile IT şi resursele alocate acestor scopuri. Mediile sau locaţiile de stocare să fie protejate împotriva deteriorării sau accesului neautorizat. Procedurile de mentenanţă a echipamentelor să fie realizate corect şi la intervale de timp stabilite în funcţie de specificul fiecărei componente, numai de către personal autorizat în acest sens. Constituirea în cadrul departamentului IT a unui colectiv specializat în raportarea şi rezolvarea operativă a problemelor de ordin tehnic (Help Desk), care să asigure şi acordarea suportului tehnic de specialitate către utilizatori, fie prin linii telefonice dedicate, fie prin e-mail sau deplasări ale echipelor specializate. De asemenea, să se aibă în vedere definirea corectă a problemelor: data apariţiei, frecvenţa, etapele premergătoare, modul de manifestare, datele de identificare ale persoanelor de contact etc. În acelaşi scop pot fi utilizate şi raportările generate automat sau se pot utiliza programe de monitorizare a sistemelor informatice. Elaborarea şi implementarea unor programe care să automatizeze pe cât posibil verificările efectuate asupra operaţiilor informatice.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Radu George	Dumitru Daniel	Structură auditată

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 3.2.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin / Radu George Data: 16.09.2009
Avizat: Dumitru Daniel Data: 16.09.2009

Obiectul testului	Programele antivirus asigură protecţia aplicaţiilor
Obiectivele testului	*Analiza programelor anti-virus*
Descrierea testului	Populaţia statistică testată a fost constituită din totalul calculatoarelor personale utilizate la nivelul entităţii publice, adică 250 de computere. Eşantionul pentru realizarea testării programelor anti-virus a fost stabilit pe baza unui procent de 2%, din totalul populaţiei de 250 de calculatoare, respectiv 5 calculatoare personale, eşantionarea utilizată a fost la întâmplare, conform *Foii de lucru nr. ...* • Testările au constat în verificarea implementării programelor anti-virus conform procedurilor: - instalarea unui program anti-virus adecvat necesităţilor utilizatorilor staţiilor de lucru; - programul anti-virus să verifice staţia de lucru la pornire; - programul anti-virus să monitorizeze toate programele şi aplicaţiile active, mesajele primite şi să verifice automat actualizările la intervale regulate (zilnic); - programul anti-virus să se actualizeze în reţea, astfel încât să protejeze eficient datele electronice împotriva viruşilor nou-apăruţi.
Constatări	O politică adecvată de securitate IT trebuie să prevadă instalarea unui program anti-virus pe toate staţiile de lucru, ca acesta să verifice staţia de lucru la pornire, să monitorizeze toate programele de aplicaţii active, mesajele primite şi să verifice automat actualizările la intervale regulate (poate chiar zilnic). Din analiza echipamentelor de calcul selectate în eşantion cu privire la modul în care programele şi aplicaţiile conţinute de acestea sunt protejate împotriva atacurilor din reţea şi din afara reţelei, s-a constatat că: - în cazul a 2 calculatoare din cadrul entităţii publice, configuraţia programului anti-virus a fost modificată pentru a întrerupe monitorizarea întregii activităţi şi verificarea e-mail-ului şi, în special, a fişierelor anexate. Acest lucru s-a realizat la cererea conducătorului departamentului, deoarece se considera că programul anti-virus are un efect negativ asupra performanţei sistemului; Urmare acestei constatări, am verificat respectivele staţii de lucru pentru a descoperi prezenţa viruşilor şi am constatat că acestea erau infectate cu viruşi.
Concluzii	Programele anti-virus nu sunt utilizate conform instrucţiunilor şi licenţelor.

Auditor,
Radu George

Supervizor,
Dumitru Daniel

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FOAIE DE LUCRU NR. 3.1.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Obiectiv: Protejarea anti-virus a sistemelor informatice

Testarea se va realiza pe un eşantion care a fost constituit astfel:
- populaţia totală este de 250 calculatoare personale;
- eşantionul va fi de 2%, respectiv 250 x 2% = 5 calculatoare personale;
- pasul de selecţie va fi 250 : 5 = 50;
- eşantionul se va constitui din calculatoarele existente în Lista IP-urilor calculatoarelor ce se conectează la reţeaua entităţii publice la poziţiile:

11, 61, 111, 161, 211,

conform celor prezentate în Lista de control anexată la Testul nr. 4.6.:
- eşantionul constituit va fi verificat integral;
- în urma verificării se va întocmi un test.

Auditor,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICA
Serviciul Audit Intern

Lista control nr. 3.1.

privind Programele anti-virus

Elemente testate / **Eşantion**	Verificarea implementării programelor anti-virus conform procedurilor				Monitorizarea sistematică a funcţionalităţii programelor anti-virus	Verificarea sistemului de actualizare a programelor anti-virus
	Instalarea unui program anti-virus adecvat necesităţilor utilizatorilor staţiilor de lucru	Programul anti-virus să verifică staţia de lucru la pornire	Programul anti-virus monitorizează toate programele şi aplicaţiile active, mesajele primite şi verifică automat actualizările la intervale regulate (zilnic)	Programul anti-virus se actualizează în reţea, astfel încât să protejeze eficient datele electronice împotriva viruşilor nou-apăruţi		
Computer aflat la poziţia 11	X	X	X	X	X	X
Computer aflat la poziţia 61	X	X	X	X	X	X
Computer aflat la poziţia 111	FIAP	FIAP	FIAP	FIAP	FIAP	FIAP
Computer aflat la poziţia 161	FIAP	FIAP	FIAP	FIAP	FIAP	FIAP
Computer aflat la poziţia 211	NU	X	X	X	X	X

Auditor,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICA
Serviciul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 3.2.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 16.09.2009
Avizat: Dumitru Daniel Data: 16.09.2009

Problema	Neaplicarea în mod unitar a politicii de securitate IT a condus la infectarea cu viruşi a unor staţii de lucru din sistemul IT al entităţii publice.
Constatarea	O politică adecvată de securitate IT trebuie să prevadă instalarea unui program anti-virus pe toate staţiile de lucru, ca acesta să verifice staţia de lucru la pornire, să monitorizeze toate programele de aplicaţii active, mesajele primite şi să verifice automat actualizările la intervale regulate (poate chiar zilnic). Echipa de auditori a verificat 5 de staţii de lucru, selectate în mod aleator, din cadrul tuturor departamentelor şi a constatat următoarele: - în 2 departamente din cadrul entităţii publice configuraţia programului anti-virus pentru un număr de doua calculatoare a fost modificată pentru a întrerupe monitorizarea întregii activităţi şi verificarea e-mail-ului şi, în special, a fişierelor anexate. Acest lucru s-a realizat la cererea conducătorului departamentului, deoarece se considera că programul anti-virus are un efect negativ asupra performanţei sistemului; Urmare acestei constatări, am verificat respectivele staţii de lucru pentru a descoperi prezenţa viruşilor şi am descoperit că toate erau infectate cu viruşi.
Cauza	Lipsa monitorizării permanente a staţiilor de lucru cu privire la funcţionarea programelor antivirus, precum şi responsabilizarea utilizatorilor în cazul în care dezactivează un program antivirus.
Consecinţa	Prezenţa viruşilor şi a altor programe dăunătoare pe staţiile de lucru afectează în mod negativ activitatea staţiilor de lucru putând duce la blocarea acestora sau chiar a întregului sistem program, aplicaţie sau sistem informatic.
Recomandarea	Constituirea unor echipe pentru efectuarea de verificări anti-virus la nivelul tuturor staţiilor de lucru din cadrul entităţii publice, configurarea corecta în cazurile în care aceste programe au fost dezactivate, stabilirea de responsabilităţi în cazul în care acestea sunt dezactivate şi produc disfuncţii în cadrul organizaţiei.

Auditor,	Supervizor,	Pentru conformitate
Radu George	Dumitru Daniel	Structura auditată

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 3.3.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 16.09.2009
Avizat: Dumitru Daniel Data: 16.09.2009

Obiectul testului	Implementarea subsistemelor IT
Obiectivele testului	Realizarea subsistemelor IT conform aprobărilor şi planificărilor.
Descrierea testului	Populaţia este formata din aplicaţiile şi programele aprobate de conducerea organizaţiei pentru a fi implementate în perioada suspusă evaluării. Acestea vor fi evaluare în totalitate. Analiza va urmări dacă un program sau aplicaţie aprobată a fost implementată cu respectarea termenelor. Pentru fiecare aplicaţie sau program aprobat se va urmări şi dacă au fost stabilite resursele financiare necesare, inclusiv cuprinderea lor în buget.
Constatări	Analiza implementării subsistemelor IT, potrivit planului anual întocmit şi aprobat, a pus în evidenţă faptul că termenele stabilite pentru implementarea programelor nu sunt respectate, iar departamentele ce ar trebui să utilizeze deja noile aplicaţii IT întâmpină dificultăţi în transmiterea datelor în format electronic celorlalte departamente care au nevoie de aceste informaţii şi unde funcţionează deja de programe performante.
Concluzii	Programele şi aplicaţiile aprobate şi pentru care au fost stabilite şi aprobate şi resursele nu sunt implementate în termen.

Auditor intern,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern

INTERVIU nr. 3.1.
privind gradul de realizare a subsistemelor IT stabilite prin planul strategic
adresat
domnului Eleodor Darius, şef Serviciul analiza, proiectare şi programare

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Nr. crt.	***Întrebări***	**Da**	**Nu**	**Observaţii**
1.	Există un sistem procedurat de realizare a subsistemelor IT	X		
2.	Sistemele implementate au fost stabilite prin planul strategic şi prin planurile anuale?		X	
3.	Există persoane responsabile de implementarea subsistemelor IT?		X	
4.	Subsistemele IT au fost realizate la termenele stabilite?		X	
5.	Există resurse alocate pentru realizarea subsistemelor IT?	X		
6.	Aveţi o procedură pentru monitorizarea implementării subsistemelor IT?		X	
7.	În toate cazurile în care persoanele responsabile au primit alte sarcini de serviciu au fost desemnate alte persoane care să monitorizeze implementarea subsistemelor IT?		X	
8.	Nu mai aveţi ceva de adăugat?	X		

Data: 16.09.2009

Dat în faţa noastră
Auditori:
Popescu Sorin
Radu George

Intervievat
Sef serviciu
Eleodor Darius

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FISĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 3.3.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 16.09.2009
Avizat: Dumitru Daniel Data: 16.09.2009

Problema	Subsistemele IT nu au fost realizate la termenele stabilite.
Constatarea	Analiza implementării subsistemelor IT, potrivit planului anual întocmit şi aprobat, a pus în evidenta faptul ca termenele stabilite pentru implementarea programelor nu sunt respectate, iar departamentele ce ar trebui să utilizeze deja noile aplicaţii IT întâmpină deficienţe în transmiterea datelor în format electronic celorlalte departamente care au nevoie de aceste informaţii şi unde funcţionează deja de programe performante.
Cauza	Resursele financiare alocate pentru implementarea acestor aplicaţii în cadrul programelor deja existente au fost utilizate pentru finalizarea unor aplicaţii şi programe deja începute şi nefinalizate.
Consecinţa	Întârzieri în realizarea activităţilor planificate atât în cadrul departamentului IT cât şi în cadrul altor departamente, deoarece datele şi informaţiile sunt reluate şi introduse manual.
Recomandarea	Analiza tuturor aplicaţiilor şi programelor începute şi nefinalizate, identificarea resurselor financiare necesare pentru finalizarea acestora, stabilirea de termene de finalizare şi urmărirea respectării acestora. Noile aplicaţii şi programe vor fi aprobate şi achiziţionate numai dacă sunt compatibile cu cele deja implementate sau aflate în faza de implementare şi numai dacă exista resursele necesare aprobate prin buget.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Radu George	Dumitru Daniel	Structură auditată

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST nr. 3.4.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 16.09.2009
Avizat: Dumitru Daniel Data: 16.09.2009

Obiectul testului	Evaluarea problemelor şi soluţionarea acestora
Obiectivele testului	Verificarea existenţei unor controale generale implementate la nivelul subsistemelor IT
Descrierea testului	Populaţia statistică este reprezentată de 15 subsisteme IT ce reprezintă numărul total al subsistemelor IT funcţionale la nivelul entităţii publice. Eşantionarea va fi reprezentat de 5 elemente din întreaga populaţie, deci 30%, pentru că este un număr rezonabil de subsisteme. Testarea a constat în examinarea următoarelor elemente stabilite prin *Lista de verificare nr. 3, poz*….., şi anume: - Controlul datelor introduse în aplicaţii; - Controlul pe parcursul procesării datelor şi rapoartele produse în caz de nerealizarea procesării (întreruperi, transfer). - Controlul datelor rezultate în urma procesării, astfel încât să se asigure că aceste date sunt complete - Validarea datelor transferate din alte aplicaţii - Controalelor care verifică înregistrările duble; - Autorizarea electronică şi/sau manuală a tranzacţiilor - Efectuarea tranzacţiilor numai de la computere definite în prealabil - Păstrarea integrală a înregistrărilor astfel încât să se poată urmări tranzacţiile efectuate din faza de iniţiere până la finalizarea lor; - Înţelegerea controalelor implementate de către utilizatori. Testarea s-a concretizat în elaborarea *Listei de control nr…… privind existenţa controalelor generale la nivelul subsistemelor IT.*
Constatări	Din analiza modului de implementare şi funcţionare a controalelor la nivelul subsistemelor IT, s-a constat inexistenţa următoarelor controale generale: - Controlul asupra datelor introduse în aplicaţii; - Controlul asupra datelor rezultate în urma procesării astfel încât să se asigure că aceste date sunt complete; - Controlul pe parcursul procesării datelor şi rapoartelor rezultate; - Controlul privind validarea datelor transferate din alte aplicaţii; - Controlul asupra tranzacţiilor efectuate.
Concluzii	Controalele generale nu sunt implementate în totalitate la nivelul subsistemelor informatice.

Auditor intern, **Supervizor,**
Radu George Dumitru Daniel

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICA
Serviciul Audit Intern

FOAIE DE LUCRU nr. 3.2.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Obiect: Existenţa controalelor generale la nivelul subsistemelor IT

Obiectivul	*Verificarea existenţei unor controale generale implementate la nivelul subsistemelor IT.*

Testarea se va realiza pe un eşantion care a fost constituit astfel:

- populaţia totală este de 15 subsisteme IT;
- eşantionul va fi de 30%, respectiv 15 x 30% = 5 subsisteme IT;
- eşantionul se va constitui din:
  - *Subsistemul IT pentru gestiunea resurselor umane*
  - *Subsistemul IT pentru operaţiuni financiare*
  - *Subsistemul IT pentru activitatea contabilă*
  - *Subsistemul IT pentru activitatea juridică*
  - *Subsistemul IT de coordonare a relaţiilor bugetare cu Uniunea Europeană*

  conform celor prezentate în *Lista de control nr. 3.2.*.:
- eşantionul constituit va fi verificat integral;
- în urma verificării se va întocmi un test.

Data: 16.09.2009

Auditor intern,
Radu George

Supervizor,
Dumitru Daniel

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

Lista control nr. 3.2.

privind existenţa controalelor generale la nivelul subsistemelor IT

Nr. Crt.	Elemente testate / Eşantion	Controlul datelor introduse în aplicaţii	Controlul pe parcursul procesării datelor şi rapoartele produse în caz de nerealizare a procesării	Controlul datelor rezultate în urma procesării, astfel încât să se asigure că aceste date sunt complete	Validarea datelor transferate din alte aplicaţii	Controale care verifică înregistrările duble	Autorizarea electronică şi/sau manuală a tranzacţiilor	Efectuarea tranzacţiilor numai de la computere definite în prealabil	Păstrarea integrală a înregistrărilor astfel încât să se poată urmări tranzacţiile efectuate din faza de iniţiere până la finalizarea lor	Înţelegerea controalelor implementate de către utilizatori
1.	*Subsistemul IT pentru gestiunea resurselor umane*	FIAP	FIAP	FIAP	FIAP	X	X	FIAP	X	X
2.	*Subsistemul IT pentru operaţiuni financiare*	X	X	X	FIAP	X	X	FIAP	X	X
3.	*Subsistemul IT pentru activitatea contabilă*	X	X	X	FIAP	X	X	FIAP	X	X
4.	*Subsistemul IT pentru activitatea juridică*	FIAP	FIAP	FIAP	FIAP	X	X	X	X	X
5.	*Subsistemul IT de coordonare a relaţiilor bugetare cu Uniunea Europeană*	X	X	X	FIAP	X	X	X	X	X

Data> 16.09.2009

Auditor intern,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICA
Serviciul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 3.4.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 16.09.2009
Avizat: Dumitru Daniel Data: 16.09.2009

Problema	Inexistenţa controalelor generale implementate la nivelul subsistemelor IT
Constatarea	Din evaluare, auditorii interni au constatat că nu există un sistem de controale generale care să fie avute în vedere în cadrul procesului de proiectare, realizare, testare şi implementare a tuturor subsistemelor IT ce rulează pe echipamentele entităţii publice, astfel: - Controlul datelor introduse în aplicaţii; - Controlul pe parcursul procesării datelor şi rapoartele produse în caz de nerealizarea procesării (întreruperi, transfer); - Controlul datelor rezultate în urma procesării, astfel încât să se asigure că aceste date sunt complete; - Controlul privind validarea datelor transferate din alte aplicaţii; - Controlul privind tranzacţiile efectuate.
Cauza	Lipsa unei bune gestiuni a riscului, pe baza căreia sa fie identificate controalele interne şi modul în care acestea funcţionează.
Consecinţa	Inexistenţa unui set de controale generale, armonizat pentru toate subsistemele IT, poate să conducă la nedetectarea modificărilor neautorizate aduse datelor procesate şi astfel apare probabilitatea ca date eronate să fie introduse, prelucrate şi stocate în sistemul IT.
Recomandarea	Identificarea riscurilor care guvernează toate subsistemele IT, stabilirea controalelor interne care ar trebui să existe pentru ca acestea să funcţioneze corect, urmărirea controalelor interne care există şi funcţionează, identificarea şi implementarea de instrumente de control pentru controalele interne care nu sunt implementate sau nu funcţionează.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Radu George	Dumitru Daniel	Structură auditată

Procedura – P10 – INTERVENŢIA LA FAŢA LOCULUI

ENTITATEA PUBLICA
Serviciul Audit Intern

LISTA DE VERIFICARE NR. 4

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 16.09.2009
Avizat: Dumitru Daniel Data: 16.09.2009

Obiectivul I.
SECURITATEA INFORMAŢIEI

Nr. crt.	Activitatea de audit	Da	Nu	Obs.
A	**Organizarea securităţii informaţiilor**			
1.	**Elaborarea politicii privind securitatea informaţiei**			
1.1.	Verificaţi dacă există o politică de securitate a informaţiei;	X		
1.2.	Verificaţi dacă politica de securitate a informaţiei este aprobată de conducerea organizaţiei;	X		
1.3.	Verificaţi dacă politica privind securitatea informaţiei stabileşte responsabilităţile asociate şi principiile de securitate care trebuie urmate de către personal;	X		
1.4.	Verificaţi dacă politica de securitate a informaţiei supune informaţiile şi sistemele importante unei analize de risc în mod regulat;	X		
1.5.	Verificaţi dacă politica de securitate a informaţiei impune ca sistemele să fie clasificate într-un mod care să indice importanţa acestora pentru organizaţie;	X		
1.6.	Verificaţi dacă politica de securitate a informaţiei impune utilizarea numai a programelor licenţiate;	X		
1.7.	Verificaţi dacă politica de securitate a informaţiei asigură condiţiile de raportare sau abaterile de la regularitate;	X		
1.8.	Verificaţi dacă protejarea informaţiei este asigurată în condiţii de confidenţialitate, integritate şi disponibilitate;	X		
1.9.	Verificaţi dacă politica de securitate interzice utilizarea informaţiilor şi sistemelor organizaţiei fără autorizare;	X		
1.10.	Verificaţi dacă politica de securitate interzice scoaterea informaţiei sau echipamentelor din cadrul organizaţiei fără autorizare;	X		
1.11.	Verificaţi dacă politica de securitate interzice utilizarea informaţiilor, inclusiv a infrastructurii sau echipamentelor IT în alte scopuri;	X		
1.12.	Verificaţi dacă politica de securitate interzice copierea neautorizată a datelor şi informaţiilor;	X		
1.13.	Verificaţi dacă politica de securitate interzice divulgarea informaţiilor către persoane neautorizate;	X		
1.14.	Verificaţi dacă politica de securitate obligă utilizatorii să închidă programele sau aplicaţiile când nu sunt utilizate;	X		
1.15.	Verificaţi dacă politica de securitate obligă utilizatorii să se deconecteze de la aplicaţii, atunci când lasă calculatorul	X		

	nesupravegheat;			
1.16.	Verificaţi dacă politica de securitate este comunicată întregului personal;	X		
1.17.	Verificaţi dacă politica de securitate are în vedere prevenirea falsificării probelor în cazul unui incident;	X		
1.18	Verificaţi dacă politica de securitate stabileşte măsurile disciplinare ce pot fi luate în cazul nerespectării ei;	X		
1.19	Verificaţi dacă politica de securitate este revizuită şi actualizată periodic.	X		
2.	**Stabilirea responsabilităţilor în cadrul politicii de securitate**			
2.1.	Verificaţi dacă există o persoană din conducerea de vârf cu responsabilitate generală pentru securitatea informaţiei;	X		
2.2.	Verificaţi dacă există un comitet însărcinat cu coordonarea activităţii de securitate a informaţiei;	X		
2.3.	Verificaţi dacă comitetul responsabil de securitatea informaţiei coordonează această activitate la nivelul întregii organizaţii;	X		
2.4.	Verificaţi dacă din comitetul însărcinat cu coordonarea activităţii de securitate a informaţiei fac parte persoane din conducerea de vârf a organizaţiei;	X		
2.5.	Verificaţi dacă comitetul însărcinat cu coordonarea activităţii de securitate a informaţiei este responsabil pentru integrarea informaţiei pentru toate sectoarele organizaţiei;	X		
2.6.	Verificaţi dacă comitetul însărcinat cu coordonarea activităţii de securitate a informaţiei asigură tratarea intereselor privind securitatea informaţiei curent şi consecvent;	X		
2.7.	Verificaţi dacă comitetul însărcinat cu coordonarea activităţii de securitate a informaţiei este responsabil pentru aprobarea politicilor şi standardelor de securitate a informaţiei;	X		
2.8.	Verificaţi dacă comitetul însărcinat cu coordonarea activităţii de securitate a informaţiei este responsabil pentru aprobarea procedurilor de securitate a informaţiei;	X		
2.9.	Verificaţi dacă comitetul însărcinat cu coordonarea activităţii de securitate a informaţiei este responsabil pentru aprobarea şi stabilirea priorităţilor activităţii de îmbunătăţire a securităţii informaţiei;	X		
2.10.	Verificaţi dacă comitetul însărcinat cu coordonarea activităţii de securitate a informaţiei asigură coordonarea implementării instrumentelor de control aferente securităţii informaţiei;	X		
2.11.	Verificaţi dacă comitetul însărcinat cu coordonarea activităţii de securitate a informaţiei accentuează importanţa securităţii informaţiei în cadrul organizaţiei;	X		
3.	**Securitatea datelor asigură disponibilitatea acestora doar pentru utilizatorii autorizaţi**			
3.1.	Verificaţi dacă regulile de securitate privind accesul la echipamentele şi datele stabilite sunt respectate cu strictețe;	X		
3.2.	Verificaţi dacă abaterile de la regulile impuse sunt imediat semnalate persoanelor responsabile;	X		
3.3.	Verificaţi dacă dispozitivele de stocare sunt păstrate în condiţii de securitate pentru a evita distrugerea fizică, pierderea sau modificarea conţinutului;	X		
3.4.	Verificaţi dacă condiţiile de păstrare sunt verificate periodic şi îmbunătăţite;	X		
3.5.	Verificaţi dacă salvările de date sunt efectuate cu periodicitatea impusă de importanţa datelor şi de regulile prestabilite;	X		
3.6.	Verificaţi dacă arhivarea datelor este realizată cu frecvenţa impusă de reglementările de operare;	X		
3.7.	Verificaţi dacă drepturile utilizatorilor sunt verificate periodic, în conformitate cu sarcinile alocate acestora;	X		
3.8.	Verificaţi dacă permisiunile curente de acces la resursele partajate sunt verificate, în vederea conformităţii cu regulile de securitate impuse;	X		
3.9.	Verificaţi dacă accesul la directoarele şi fişierele cu caracter secret se realizează în conformitate cu reglementările interne;	X		

3.10.	Verificaţi dacă arhivarea datelor este realizată adecvat importanţei acestora;	X		
3.11.	Verificaţi dacă duplicarea datelor se realizează conform cu reglementările interne;	X		
3.12.	Verificaţi asigurarea securităţii dispozitivelor de stocare a datelor;	X		
B.	**Disponibilitatea datelor**			
1.	**Protejarea datelor împotriva viruşilor**			
1.1.	Verificaţi dacă programele sunt protejate faţă de viruşi;	X		
1.2.	Verificaţi dacă viruşii detectaţi sunt înlăturaţi prin utilizarea de produse specializate antivirus;	X		
1.3.	Verificaţi dacă actualizarea produselor antivirus se face permanent;	X		
1.4	Verificaţi dacă procedurile de scanare şi eliminare a viruşilor sunt lansate periodic în execuţie;	X		
1.5.	Verificaţi dacă programul antivirus intră în funcţiune întotdeauna la pornirea computerelor;	X		
1.6.	Verificaţi dacă viruşii sunt detectaţi cu operativitate utilizând metode adecvate;	X		
1.7.	Verificaţi dacă există continuitate în asigurarea licenţelor programelor antivirus;	X		
1.8.	Verificaţi dacă implementarea programelor anti-virus asigură:	X		
1.9.	a) instalarea unui program anti-virus adecvat necesităţilor utilizatorilor staţiilor de lucru;	X		
1.10.	b) verificarea computerelor la pornire;	X		
1.11.	c) monitorizarea tuturor programelor şi aplicaţiilor active, a mesajelor primite şi verificarea automată a actualizărilor la intervale regulate (zilnic);	X		
1.12.	d) actualizarea în reţea, astfel încât să protejeze eficient datele împotriva viruşilor nou-apăruţi;	X		
1.13.	Verificaţi dacă este realizată o monitorizarea sistematică a funcţionalităţii programelor anti-virus;	X		
1.14.	Verificaţi dacă sistemul de actualizare a programelor anti-virus este adecvat necesităţilor programelor şi aplicaţiilor utilizate în cadrul entităţii;	X		
2.	**Asigurarea continuităţii activităţilor**			
2.1.	Verificaţi dacă planul privind asigurarea continuităţii activităţilor permite cunoaşterea măsurilor ce trebuie luate în cazul producerii unui eveniment nedorit;	X		
2.2.	Verificaţi dacă scopul planului de asigurare a continuităţii activităţii este de a minimiza efectele produse de un dezastru;	X		
2.3.	Verificaţi dacă planul privind continuitatea activităţilor are impact major asupra activităţilor curente critice;	X		
2.4.	Verificaţi dacă resursele umane, precum şi cele hardware/software implicate în procesul de aplicare a planului sunt prestabilite şi sunt disponibile;	X		
2.5.	Verificaţi dacă planul descrie strategia generală de asigurare a continuităţii activităţii;	X		
2.6.	Verificaţi dacă planul stabileşte rolurile şi responsabilităţile personalului implicat;	X		
2.7.	Verificaţi dacă planul stabileşte criteriile şi procedurile de recunoaştere a unei crize;	X		
2.8.	Verificaţi dacă planul defineşte procedurile tehnice de reluare sau continuare a proceselor critice;	X		
2.9.	Verificaţi dacă planul stabileşte procedurile de revenire la modul normal de operare;	X		
2.10.	Verificaţi dacă planul conţine procedurile de întreţinere, actualizare şi testare periodică a acestuia;	X		
2.11.	Verificaţi dacă echipa de coordonare, în caz de producere a evenimentului nedorit, este condusă de managementul de vârf;	X		
2.12.	Verificaţi dacă echipa de coordonare în caz de producere a evenimentului nedorit este responsabilă pentru iniţierea planului privind continuitatea activităţilor;	X		

2.13.	Verificaţi dacă echipa de intervenţie în caz de dezastru este implicată în conceperea planului privind continuitatea activităţilor;	X		
2.14.	Verificaţi dacă elaborarea planurilor privind continuitatea activităţilor a avut în vedere următoarele etape:	X		
	a) iniţierea planului			
	b) analiza de risc şi de impact			
	c) definirea cerinţelor şi dezvoltarea strategiei			
	d) implementarea strategiei şi reducerea riscului			
	e) dezvoltarea şi implementarea planurilor;			
	f) testarea şi asigurarea mentenanţei planurilor.			
2.15.	Verificaţi dacă planurile privind continuitatea activităţilor sunt conforme cu obiectivele generale şi cu strategia de administrare a riscurilor;	X		
2.16.	Verificaţi dacă funcţiile critice sunt identificate de administratorii sistemelor, dându-se prioritate proceselor din cadrul acestor funcţii;	X		
2.17.	Verificaţi dacă obiectivele avute în vedere pentru asigurarea continuităţii activităţii sistemelor au ca scop reluarea şi recuperarea funcţiilor critice;	X		
2.18.	Verificaţi dacă planurile privind continuitatea activităţilor includ cel puţin o locaţie secundară pentru salvarea datelor;	X		
2.19.	Verificaţi dacă sunt stabilite proceduri alternative/de urgenţă pentru realizarea funcţiilor critice în cazul căderii reţelelor;	X		
2.20.	Verificaţi dacă părţile implicate în planul de asigurare a continuităţii activităţilor, comunică eficient, atât în interiorul, cât şi în exteriorul organizaţiei, utilizând mijloace de comunicare sigure şi testate;	X		
2.21.	Verificaţi dacă elementele planurilor privind asigurarea continuităţii activităţii sunt testate periodic.	X		
3.	**Recuperarea datelor în caz de dezastru**			
3.1.	Verificaţi dacă a fost elaborat planul de recuperare a datelor în caz de dezastru;			
3.2.	Verificaţi dacă planul de recuperare a datelor în caz de dezastru a fost aprobat;	X		
3.3.	Verificaţi dacă este responsabilizată echipa de implementare a planului şi sunt stabilite responsabilităţile adecvate membrilor echipei;	X		
3.4.	Verificaţi dacă planul este comunicat personalului cu responsabilităţi în punerea în aplicare a acestuia în caz de dezastru;	X		
3.5.	Analizaţi dacă planul de recuperare a datelor a fost testat şi modificat periodic în baza rezultatelor obţinute în urma testării;	X		
3.6.	Verificaţi dacă sunt definite în cadrul planului domeniile de acţiune importante ale entităţii publice;	X		
3.7.	Verificaţi dacă sunt identificate principalele procese şi aplicaţii IT ce trebuie recuperate;	X		
3.8.	Verificaţi dacă au fost analizate cerinţele specifice cu privire la recuperarea datelor în caz de dezastru la nivelul sistemului IT;	X		
3.9.	Verificaţi dacă sunt stabiliţi responsabili cu monitorizarea respectării procedurilor privind recuperarea datelor în caz de dezastru;	X		
3.10.	Verificaţi dacă salvările de siguranţă sunt actualizate sistematic;	X		
3.11.	Stabiliţi dacă locaţia în care sunt stocate datele pentru a fi recuperate în caz de dezastru este adecvată;	X		
3.12.	Analizaţi sistemul de arhivare a datelor.	X		
C.	**Asigurarea funcţionării programelor şi aplicaţiilor**			
1.	**Asigurarea introducerii corecte a datelor**			
1.1.	Verificaţi dacă documentele primare sunt analizate pentru identificarea tipurilor de date care trebuie introduse sau modificate;	X		
1.2.	Verificaţi dacă datele sunt pregătite şi verificate pentru a fi introduse în sistemul informatic în vederea prelucrării;	X		

1.3.	Verificaţi dacă se verifică şi se testează toate procedurile de introducere a datelor;	X		
1.4.	Verificaţi dacă se monitorizează prelucrarea electronică a datelor;	X		
1.5.	Verificaţi se urmăresc rapoartele de erori înregistrate de sistemul informatic şi dacă se efectuează teste pentru identificarea cauzelor apariţiei acestora;	X		
1.6.	Verificaţi modul de urmărire a rezultatelor prelucrărilor şi modul de distribuire către utilizatori;	X		
1.7.	Verificaţi modul de întocmire a jurnalului intervenţiilor operatorilor, jurnalul utilizării bibliotecii de programe şi a arhivelor de date şi aplicaţii	X		
1.8.	Verificaţi dacă aplicaţiile informatice sunt utilizate în conformitate cu instrucţiunile de exploatare;	X		
1.9.	Verificaţi dacă şablonul de introducere a datelor este identificat corect, conform metodologiei proprii;	X		
1.10.	Verificaţi dacă elementele şablonului sunt analizate cu responsabilitate, în vederea introducerii datelor în condiţii de eficienţă;	X		
1.11.	Verificaţi dacă introducerea datelor se realizează cu respectarea specificaţiilor programului utilizat;	X		
1.12.	Verificaţi dacă se urmăreşte permanent conformitatea datelor introduse cu documentele primare;	X		
1.13.	Verificaţi dacă datele introduse sunt salvate pe suport de stocare în formatul de fişier adecvat;	X		
1.14.	Verificaţi dacă datele introduse sunt salvate corect şi complet;	X		
1.15.	Verificaţi dacă datele sunt salvate la intervale de timp prestabilite;	X		
1.16.	Verificaţi dacă datele salvate sunt organizate adecvat, pentru a fi regăsite cu uşurinţă;	X		
1.17.	Verificaţi dacă salvările de rezervă se realizează automat sau manual, în funcţie de opţiuni;	X		
1.18.	Verificaţi dacă datele neconforme cu documentele primare sunt corectate;	X		
1.19.	Analizaţi dacă datele introduse sunt verificate prin modalităţi adecvate, în scopul identificării operative a erorilor;	X		
1.20.	Verificaţi dacă datele corectate sunt salvate.	X		
2.	**Prelucrarea datelor**			
2.1.	Verificaţi dacă programul de prelucrare a datelor este adecvat;			
2.2.	Verificaţi dacă programul de prelucrare a datelor este corect identificat, în funcţie de necesităţi şi de rezultatele urmărite;	X		
2.3.	Verificaţi modul de depistare şi corectare a erorilor apărute în timpul rulărilor aplicaţiilor informatice;	X		
2.4.	Verificaţi dacă procesările aplicate datelor introduse sunt corecte;	X		
2.5.	Verificaţi modul de funcţionare a programelor, folosind ca date de test fie înregistrări originale, fie înregistrări mostră şi corectarea eventualelor erori apărute în procesul de introducere a datelor;	X		
2.6.	Verificaţi dacă prelucrarea datelor cu ajutorul aplicaţiilor informatice se realizează în conformitate cu instrucţiunile de exploatare;	X		
2.7.	Verificaţi dacă prelucrările efectuate sunt vizualizate în scopul verificării şi sunt prezentate pe suportul de redare specificat;	X		
2.8.	Verificaţi dacă alegerea suportului de redare se realizează ţinând cont de destinaţia datelor;	X		
2.9.	Verificaţi dacă priorităţile suportului de redare respectă cerinţele;	X		
2.10.	Verificaţi dacă documentul este pregătit pentru redare prin setarea caracteristicilor specifice;	X		
2.11.	Verificaţi dacă echipamentul de ieşire este ales adecvat, în scopul îndeplinirii condiţiilor optime de furnizare a datelor.	X		
3.	**Asigurarea securităţii datelor şi documentelor**			
3.1.	Verificaţi dacă sunt realizate copii de siguranţă pe suporturi de stocare adecvate;			
3.2.	Verificaţi dacă copiile de siguranţă sunt realizate la intervalele de timp menţionate în procedura internă;	X		

3.3.	Verificaţi dacă copiile de siguranţă sunt verificate pentru conformitate cu originalele;	X		
3.4.	Verificaţi dacă arhivarea sau duplicarea datelor este realizată în funcţie de importanţa acestora şi cu frecvenţa necesară;	X		
3.5.	Verificaţi dacă accesul la calculator este realizat prin conturi şi parole asociate, cu asigurarea caracterului de confidenţialitate;	X		
3.6.	Verificaţi dacă accesul la directoarele şi fişierele cu caracter secret se face corespunzător reglementărilor interne;	X		
3.7.	Verificaţi dacă documentele primare şi cele rezultate în urma imprimării sunt păstrate în condiţii de securitate;	X		
3.8.	Verificaţi dacă suporturile de stocare sunt verificate pentru a le depista pe cele virusate sau defecte;	X		
3.9.	Verificaţi dacă dispozitivele de stocare a datelor sunt păstrate în condiţii de securitate pentru a evita distrugerea fizică, pierderea sau modificarea conţinutului;	X		
3.10.	Verificaţi dacă condiţiile de păstrare sunt verificate periodic şi îmbunătăţite după caz;	X		
3.11.	Verificaţi dacă funcţionarea severelor şi a sistemelor este permanent şi atent monitorizată;	X		
3.12.	Verificaţi dacă accesul utilizatorilor la echipamente şi la suporturi de date este realizat numai în limita permisiunilor cerute de efectuarea sarcinilor curente;	X		
3.13.	Verificaţi dacă regulile de securitate referitoare la accesul la echipamente sunt respectate;	X		
3.14.	Verificaţi dacă abaterile de la regulile de securitate sunt semnalate prompt persoanelor responsabile;	X		
D.	**Implementarea instrumentelor de control**			
1.	**Accesul la aplicaţie este oferit pe baza necesităţilor utilizatorului**			
1.1.	Verificaţi dacă drepturile de acces sunt acordate conform regulilor impuse prin manualele de instalare a aplicaţiei;	X		
1.2.	Verificaţi dacă drepturile de acces sunt respectate de către utilizatori;	X		
1.3.	Verificaţi dacă responsabilitatea pentru administrarea şi operarea aplicaţiei este definită clar;	X		
1.4.	Verificaţi dacă utilizatorii sunt instruiţi cu privire la utilizarea reţelei şi securitatea acesteia;	X		
1.5.	Verificaţi dacă administratorii de reţea primesc instruirea adecvată şi potrivită cu privire la siguranţa şi controlul reţelei;	X		
1.6.	Verificaţi dacă activitatea în reţea este monitorizată, asigurându-se că securitatea acesteia este adecvată;	X		
1.7.	Verificaţi dacă doar utilizatorii autorizaţi pot efectua conexiuni la reţea şi există proceduri pentru verificarea conexiunilor neautorizate;	X		
1.8.	Verificaţi dacă codificarea utilizată previne accesul neautorizat la datele transmise prin reţea;	X		
1.9.	Verificaţi dacă instrumentele de control stabilite asigură datele şi programele împotriva pierderii, deteriorării, coruperii deliberate sau accidentale, şi a atacurile informatice;	X		
1.10.	Verificaţi dacă reţelele sunt proiectate şi construite pentru a asigura eficienţa traficului de date;	X		
1.11.	Verificaţi dacă programele de administrare a reţelei şi fişierele de pe server sunt salvate pentru siguranţă şi copii ale acestora sunt păstrate în locuri sigure;	X		
1.12.	Verificaţi dacă există metode de recuperare şi de continuitate a activităţii în eventualitatea defectării liniilor sau nodurilor de reţea;	X		
1.13.	Verificaţi dacă accesul fizic la domeniile critice ale reţelei este restricţionat numai pentru personalul autorizat;	X		
1.14.	Verificaţi dacă pentru echipamentele importante şi pentru nodurile reţelelor s-au alocat resurse suplimentare de securitate.	X		
2.	**Introducerea instrumentelor de control fizic asupra echipamentelor IT al aplicaţiilor**			

2.1.	Verificaţi dacă accesul fizic la sistemele de calculatoare este restricţionat prin:			
	a) sistem adecvat de încuietori;	X		
	b) blocarea accesului atunci când mediul este eliberat;			
	c) instalarea de alarme;			
	d) asigurarea de personal de pază;			
2.2.	Verificaţi dacă efectuarea controalelor fizice se realizează conform procedurilor;	X		
2.3.	Verificaţi dacă accesul la servere este restricţionat, având în vedere datele critice procesate, fiind permis numai persoanelor autorizate;	X		
2.4.	Verificaţi camerele în care se află severele şi echipamentele, dacă se respectă următoarele cerinţe: a) sunt dotate cu camere de supraveghere, care acoperă întreaga zonă de acces la server şi sunt monitorizate permanent: b) sunt prevăzute cu senzori de mişcare; c) dispun de sistem de alarmă în caz de incendiu; d) dispun de sisteme de stingere a incendiilor; e) sunt prevăzute cu echipamente de aer condiţionat; f) sunt prevăzute cu uşi neinflamabile echipate cu încuietori adecvate.	X		Test nr. 4.3. Listă de control nr. 4.1. FIAP nr. 4.3.
2.5.	Verificaţi dacă echipamentele şi documentaţia de importanţă critică sunt asigurate suplimentar;	X		
2.6.	Verificaţi dacă sistemele de detectare a accesului neautorizat instalate sunt verificate periodic;	X		
2.7.	Verificaţi dacă calculatoarele portabile sunt protejate împotriva furtului;	X		
2.8.	Verificaţi dacă utilizatorii sistemului au acces numai pentru scopuri clare şi autorizate;	X		
2.9.	Verificaţi dacă utilizatorii sistemului sunt supravegheaţi permanent;	X		
2.10.	Verificaţi dacă echipamentele şi facilităţile critice sunt protejate prin montarea lor în afara zonei de acces a publicului;	X		
2.11.	Verificaţi dacă perimetrul de securitate fizică al camerelor care adăpostesc echipamente şi facilităţi critice este întărit şi protejat;	X		
2.12.	Verificaţi dacă se realizează supravegherea continuă a camerelor în care sunt adăpostite echipamente şi facilităţi critice;	X		
2.13.	Verificaţi dacă autorizaţiile pentru accesul fizic la echipamente sunt emise în conformitate cu procedurile documentate;	X		
2.14.	Verificaţi dacă autorizaţiile pentru accesul fizic sunt revizuite periodic pentru a se asigura accesul la acestea numai a persoanelor autorizate;	X		
2.15.	Verificaţi dacă sunt luate măsuri pentru restricţionarea accesului la calculatoare şi la informaţiile păstrate de acestea;	X		
2.16.	Verificaţi dacă măsurile de protecţie sunt în acord cu politica de securitate a organizaţiei;			
2.17.	Verificaţi dacă măsurile de control ţin seama de clasificarea nivelurilor de securitate;	X		
2.18.	Verificaţi dacă măsurile de control ţin seama de cerinţele stabilite de responsabilii sistemelor şi ale organelor de reglementare;	X		
2.19.	Verificaţi dacă măsurile de control ţin seama de necesitatea de a pune în practică răspunderea personală;	X		
2.20.	Verificaţi dacă măsurile de control asigură punerea în practică a unor instrumente suplimentare de control;	X		
2.21.	Verificaţi dacă măsurile de control asigură separarea sarcinilor;	X		
2.22.	Verificaţi dacă accesul este restricţionat conform politicii de securitate;	X		
2.23.	Verificaţi dacă măsurile de control privind accesul restricţionează capacităţile sistemului care pot fi utilizate;	X		
2.24.	Verificaţi dacă măsurile de control ale accesului identifică locaţia terminalelor aflate în exploatare;	X		
2.25.	Verificaţi dacă măsurile de control privind accesul sunt realizate	X		

	pe baza unui sistem de parole;			
2.26.	Verificaţi dacă măsurile de control privind accesul sunt revizuite ca răspuns la noi ameninţări, cerinţe ale activităţii sau noi capacităţi;	X		
E.	**Securitatea reţelei**			
1.	**Monitorizarea securităţii reţelelor**			
1.1.	Verificaţi dacă riscurile ce ameninţă securitatea şi disponibilitatea reţelei şi a aplicaţiilor sunt inventariate;	X		
1.2.	Verificaţi dacă securitatea reţelei are în vedere vulnerabilitatea aplicaţiilor şi sistemelor de operare, greşelile de configurare şi erorile;	X		
1.3.	Verificaţi dacă este realizată o hartă a reţelei;	X		
1.4.	Verificaţi identificarea elementelor de bază din reţea	X		
1.5.	Verificaţi dacă este realizată o hartă exactă a reţelei;	X		
1.6.	Verificaţi dacă sunt identificate toate elementele din reţea, respectiv servere, sisteme desktop, sisteme laptop, routere, puncte de acces, imprimante, sau alte dispozitive;	X		
1.7.	Verificaţi dacă este implementat un program de management al vulnerabilităţilor;	X		
1.8.	Verificaţi dacă există posibilitatea de a actualiza situaţia reţelei de câte ori este nevoie.	X		
1.9.	Verificaţi clasificarea elementelor din reţea	X		
1.10.	Verificaţi dacă se realizează o clasificare a sistemelor desktop, a serverelor şi a aplicaţiilor, în funcţie de valoarea pe care acestea o reprezintă pentru entitatea publică;	X		
1.11.	Verificaţi dacă se realizează o grupare şi clasificare a dispozitivelor din reţea în funcţie de priorităţi, de la sisteme cu importanţă redusă, cum sunt cele de test, la sistemele de importanţă medie, cum sunt sistemele laptop folosite la biroul aprovizionare şi până la sistemele de importanţă vitală pentru entitate (tranzacţii, operaţiuni financiare)	X		
1.12.	Verificaţi modul de clasificare a sistemelor depinde de natura operaţiunilor desfăşurate;	X		
1.13.	Verificaţi modul de identificarea rapidă şi precisă a vulnerabilităţilor	X		
1.14.	Verificaţi dacă identificarea vulnerabilităţilor pleacă de la analiza topologiei reţelelor formate din servere, sisteme de operare sau platforme web diferite;	X		
1.15.	Verificaţi dacă este realizată protecţia prin implementarea unui sistem adecvat de management al vulnerabilităţilor	X		
1.16.	Verificaţi dacă acesta se bazează pe informaţii precise şi configuraţii de sistem şi reţea adecvate;	X		
1.17.	Verificaţi dacă se realizează protecţia în profunzime prin implementarea unui sistem adecvat de management al vulnerabilităţilor;	X		
1.18.	Verificaţi dacă se realizează corelarea gradului de risc cu valoarea pentru activităţile entităţii, reprezentată de vulnerabilităţile sistemelor şi a segmentelor de reţea;	X		
1.19.	Verificaţi transformarea datelor de securitate brute în informaţii	X		
1.20.	Verificaţi dacă în urma prelucrărilor, administratorii obţin rapoarte complete care detaliază nivelul critic al vulnerabilităţilor;	X		
1.21.	Verificaţi dacă este asigurat accesul instant la soluţiile de remediere;	X		
1.22.	Verificaţi dacă se folosesc patch-uri de securitate furnizate de dezvoltătorul de aplicaţii;	X		
1.23.	Verificaţi dacă se folosesc strategii ocolitoare sau alte măsuri defensive;	X		
1.24.	Verificaţi dacă pe lângă rapoartele generate pentru administratorii şi responsabilii cu securitatea, informaţiile sunt strânse, adaptate şi prezentate acelor persoane care necesită detalii despre situaţia securităţii în cadrul entităţii;	X		
1.25.	Verificaţi dacă rapoartele sunt prezentate conducerii.	X		

1.26.	Verificaţi modul de monitorizarea securităţii reţelelor, în timp	X		
1.27.	Verificaţi dacă expunerea la risc este monitorizată prin reprezentarea stării de ansamblu a reţelei;	X		
1.28.	Verificaţi dacă se utilizează un panou de afişare în timp real, privind expunerea la risc, prin reprezentarea vizuală a stării de ansamblu a reţelei;	X		
1.29.	Verificaţi dacă se realizează actualizarea continuă a acestuia;	X		
1.30.	Verificaţi dacă panoul de afişare privind expunerea la risc este adaptat nevoilor de securitate ale organizaţiei;	X		
1.31.	Verificaţi dacă la fiecare evaluare a vulnerabilităţilor se creează o înregistrare care consemnează data şi ora scanării, numărul vulnerabilităţilor identificate, gradul de severitate şi impactul asupra activităţilor;	X		
1.32.	Verificaţi dacă supă aplicarea patch-urilor, o scanare ulterioară validează aplicarea corectă a soluţiilor pentru fiecare sistem;	X		
1.33.	Verificaţi dacă se obţine reducerea riscurilor asociate;	X		
1.34.	Verificaţi dacă politica de securitate a gestionării reţelelor informatice este implementată şi asigură protejarea datelor şi informaţiilor, respectiv:			
	a) identificarea elementelor de bază din reţea		X	Test nr. 4.1. FIAP nr. 4.1.
	b) clasificarea elementelor din reţea			
	c) identificarea vulnerabilităţilor reţelei			
	d) transformarea datelor de securitate, în informaţii			
	e) monitorizarea securităţii reţelelor în timp			
	f) procesul de remediere a vulnerabilităţilor reţelelor			
1.35.	Verificaţi dacă se urmăreşte mentenanţa sistemelor.	X		
1.36.	Verificaţi integrarea procesului de remediere a vulnerabilităţilor	X		
1.37.	Verificaţi dacă entitatea este preocupată de aplicarea măsurilor proactive şi reactive, pentru remedierea vulnerabilităţilor descoperite şi a erorilor de configurare;	X		
1.38.	Verificaţi dacă entitatea este preocupată de remedierea rapidă şi eficientă a vulnerabilităţilor.	X		
F.	**Gestionarea parolelor**			
1.	**Utilizatori au parole de acces individuale**			
1.1.	Verificaţi dacă fiecare calculator este parolat;	X		
1.2.	Verificaţi dacă parola alocată este individuală;	X		
1.3.	Verificaţi dacă parola este cunoscută doar de utilizator;	X		
1.4.	Verificaţi dacă programele şi aplicaţiile au nivele de acces în funcţie de nivelul postului;	X		
1.5.	Verificaţi dacă parolele sunt schimbate periodic, respectând regulile de complexitate impuse;			Test nr. 4.2. Interviu nr. 4.1. FIAP nr. 4.2.
1.6.	Verificaţi dacă există un calendar privind parolele de acces	X		
1.7.	Verificaţi dacă există desemnată o persoană responsabilă cu verificarea periodică a sistemului de parole de acces			
1.8.	Verificaţi dacă accesul la calculator, la folosirea resurselor locale şi a celor din reţea este realizat prin conturi şi parole asociate fiecărui utilizator;	X		
1.9.	Verificaţi dacă alocarea conturilor şi parolelor respectă caracterul de confidenţialitate;	X		
2.	**Schimbarea periodică a parolelor**			
2.1.	Verificaţi dacă parolele de acces sunt asigurate în scopul păstrării caracterului secret;	X		
2.2.	Verificaţi dacă permisiunile sau drepturile utilizatorilor sunt verificate periodic, pentru a corespunde strict sarcinilor acestora;	X		
2.3.	Verificaţi dacă accesul la directoarele şi fişierele cu caracter secret se face corespunzător reglementărilor interne;	X		
2.4.	Verificaţi dacă parolele asigură următoarele reguli:			
2.5.	a) număr minim de caractere este opt;			
	b) conţin caractere alfa numerice;	X		
	c) sunt case-sensitive;			
	d) sunt mascate pe ecran, pentru a nu fi văzute;			
2.6.	Verificaţi dacă administratorul sistemului creează şi configurează	X		

	corespunzător conturile fiecărui utilizator;			
2.7.	Verificaţi dacă parolele generice iniţiale sunt schimbate de către fiecare utilizator în parte;	X		
2.8.	Verificaţi dacă sistemul beneficiază de următoarele caracteristici:			
	a) suspendarea conturilor şi parolelor după o anumită perioadă de inactivitate;			
	b) schimbarea parolelor la intervale stabilite de timp;			
	c) suspendarea conturilor după încercări succesive nereuşite de acces la sistem;	X		
	d) accesul utilizatorilor restricţionat la anumite perioade de timp;			
	e) deconectarea utilizatorilor după un anumit timp de inactivitate;			
2.9.	Verificaţi dacă configurarea conturilor se face în funcţie de tipurile de utilizatori;	X		
2.10.	Verificaţi dacă contul de administrare poate fi şters;	X		
2.11.	Verificaţi dacă sistemul permite configurarea şi controlul parametrilor de sistem.	X		
3.	**Protejarea parolelor**			
	Verificaţi dacă parolele respectă următoarele reguli:	X		
	- număr minim de 8 caractere;	X		
	- să conţină caractere alfanumerice;	X		
	- să fie CASE-SENSITIVE;	X		
	- să fie mascate pe ecran pentru a nu fi văzute.	X		
	Verificaţi dacă administratorul sistemului creează şi configurează corespunzător conturile fiecărui utilizator;	X		
	Verificaţi dacă parolele generice iniţiale sunt schimbate de către fiecare utilizator în parte;	X		
4.	**Persoanele autorizate au acces la sistemul de operare**			
4.1.	Verificaţi dacă accesul la sistem se realizează numai pe baza conturilor de utilizatori în funcţie de tipurile specifice şi de atribuţiile specifice fiecărui angajat	X		
4.2.	Verificaţi dacă conturile de utilizatori respectă condiţii privind parolele, modul de acces, restricţiile specifice;	X		
4.3.	Verificaţi dacă utilizatorii sunt instruiţi să respecte regulile privind securitatea logică;	X		
4.4.	Verificaţi dacă există proceduri legate de accesul neautorizat;	X		
G.	**Securitatea logică**			
1.	**Asigurarea securităţii funcţionării programelor şi aplicaţiilor**			
1.1.	Verificaţi dacă înainte proiectării unui plan de control al securităţii, sunt identificate riscurile la care sunt supuse sistemele informatice din punct de vedere logic;	X		
1.2.	Verificaţi dacă echipa care realizează planul de securitate include specialişti din diverse domenii informatice şi auditori interni, pentru a putea identifica toţi factorii de risc şi a se formula cele mai bune soluţii de înlăturare a acestora;	X		
1.3.	Verificaţi dacă planul de securitate include metodele de asigurare a securităţii pentru fiecare etapă din funcţionarea sistemelor, pentru tipuri de operaţii, protecţia bazelor de date, a sistemelor de operare;	X		
1.4.	Verificaţi asigurarea securităţii în faza de implementare a noilor sisteme informatice			
1.5.	Verificaţi dacă la instalarea sistemelor informatice noi, se creează conturi de sistem şi conturi de acces;	X		
1.6.	Verificaţi dacă parolele iniţiale ale acestor conturi sunt schimbate după accesarea sistemului;	X		
1.7.	Verificaţi dacă sistemul beneficiază de următoarele caracteristici:	X		
	- numărul minim de caractere pentru parole;			
	- suspendarea conturilor şi parolelor după o anumită perioadă de inactivitate;			
	- schimbarea parolelor la intervale stabilite de timp;			
	- suspendarea conturilor după încercări succesive nereuşite de			

	acces la sistem; - accesul la sistem al utilizatorilor să fie restricţionat la anumite perioade de timp, între anumite ore; - deconectarea utilizatorilor după un anumit timp de inactivitate; - configurarea conturilor în funcţie de tipurile de utilizatori; - contul de administrare (system user) să nu poată fi şters;			
1.8.	Verificaţi dacă sistemul permite configurarea şi controlul parametrilor cheie;	X		
1.9.	Verificaţi dacă salvarea datelor se realizează periodic în conformitate cu specificaţiile manualului;	X		
1.10.	Verificaţi dacă copiile de siguranţă se realizează conform indicatorilor din manualele de operare;	X		
1.11.	Verificaţi dacă modulele/programele/datele salvate sunt corecte şi complete, conform manualelor de operare;	X		
1.12.	Verificaţi dacă identificarea modulelor/programelor/datelor salvate se face cu uşurinţă;	X		
1.13.	Verificaţi dacă suporturile/dispozitivele de stocare sunt depozitate în condiţii speciale, conform manualelor de operare;	X		
1.14.	Verificaţi dacă conţinutul fiecărui suport/dispozitiv de stocare este consemnat pe etichetă şi înregistrat în registru;	X		
1.15.	Verificaţi dacă dispozitivele de stocare au asigurată securitatea conform instrucţiunilor de stocare;	X		
1.16.	Verificaţi dacă există un acces sigur şi controlat la echipamentele şi dispozitivele de stocare;	X		
1.17.	Verificaţi dacă dispozitivele de stocare sunt păstrate în condiţii de securitate;	X		
1.18.	Verificaţi dacă modulele/programele, datele sunt salvate pe dispozitivele sau suporturile de stocare precizate de manuale;	X		
1.19.	Verificaţi dacă echipamentele şi componentele hardware sunt înregistrate corect şi cu toate detaliile relevante pentru accesarea operativă a informaţiilor privind starea de funcţionare şi configuraţia lor,	X		
1.20.	Verificaţi dacă evidenţele dispozitivelor de stocare a datelor sunt conduse, în scopul identificării prompte a conţinutului acestora.	X		
1.21.	Verificaţi dacă accesul în cadrul sistemului se realizează numai pe baza conturilor de utilizatori în funcţie de tipurile specifice şi de atribuţiunile fiecărui angajat;	X		
1.22	Verificaţi dacă aceste conturi respectă anumite condiţii privind parolele, modul de acces, restricţiile pe care le are fiecare cont în parte;	X		
1.23.	Verificaţi dacă utilizatorii sunt instruiţi să respecte regulile de securitate logică;	X		
1.24.	Verificaţi dacă există proceduri pentru rezolvarea problemelor legate de accesul neautorizat;	X		
1.25	Verificaţi dacă accesul la distanţă permite accesarea diferitelor tipuri de aplicaţii;	X		
1.26.	Verificaţi dacă securizarea transferurilor se realizează prin linii dedicate;	X		
1.27	Verificaţi dacă securizarea transferurilor utilizează protocoale specifice de comunicaţie;	X		
1.28	Verificaţi dacă la liniile dedicate au acces numai persoanele autorizate din cadrul organizaţiei;	X		
1.29	Verificaţi dacă se folosesc algoritmi de criptare a datelor;	X		
1.30	Verificaţi dacă algoritmii de criptare ţin cont de tipul informaţiei;	X		
1.31.	Verificaţi dacă datele transferate sunt criptate;	X		
1.32.	Verificaţi dacă este evaluat riscul de interceptare neautorizată a transferurilor;	X		
1.33.	Verificaţi dacă utilizatorul aflat la distanţă se poate conecta la reţeaua entităţii, numai printr-un canal prestabilit, alocat special comunicării / traficului la distanţă;	X		
1.34.	Verificaţi dacă terminalul utilizatorului furnizează anumite date de identificare astfel încât conexiunea să poată fi realizată;	X		

1.35.	Verificaţi dacă, în cazul dispozitivelor wireless, se realizează o blocare a accesului posibililor utilizatori, aflaţi în raza de acţiune a acestora;	X		
1.36.	Verificaţi dacă SSL (este un protocol pentru producerea şi păstrarea de conexiuni codificate între browser-ul de web şi serverul de web) foloseşte protocolul TCP/IP în acţionarea asupra protocoalelor de nivel înalt;	X		
1.37.	Verificaţi dacă se realizează autentificarea clientului către server;	X		
1.38.	Verificaţi dacă protocolul oferă ambelor staţii posibilitatea de a stabili o conexiune codificată;	X		
1.39.	Verificaţi dacă certificatele de server asigură identitatea celeilalte părţi;	X		
1.40.	Verificaţi dacă este asigurată evidenţa dispozitivelor token, pentru cazurile în care accesul utilizatorilor la sistem se realizează prin validări multiple;	X		
1.41.	Verificaţi dacă pentru tranzacţiile importante cum ar fi e-banking, bursa, e-commerce şi tranzacţiile financiare sunt realizate autentificări garantate cu ajutorul acestor dispozitive?	X		
1.42.	Verificaţi dacă administrarea securităţii sistemelor este realizată de către persoane specializate;	X		
1.43.	Verificaţi dacă managerii de pe diferitele nivele sunt responsabilizaţi cu implementarea corectă a procedurilor şi politicilor de securitate?	X		
1.44.	Verificaţi dacă aceştia sunt responsabili cu instruirea utilizatorilor în respectarea regulilor de securitate, de monitorizare permanentă a sistemelor, de concepere şi modificare a politicilor şi regulilor de securitate;	X		
1.45.	Verificaţi dacă administratorii responsabili cu protecţia sistemelor se consultă cu auditorii interni pentru implementarea celor mai bune soluţii;	X		

Auditori,

Popescu Sorin

Radu George

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICA
Serviciul Audit Intern

TEST nr. 4.1.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2008
Întocmit: Popescu Sorin/ Radu George Data: 16.09.2009
Avizat: Dumitru Daniel Data: 16.09.2009

Obiectul testului	Monitorizarea securităţii reţelelor.
Obiectivele testului	Asigurarea că datele şi informaţiile sunt protejate în cadrul sistemului informatic, limitând accesul în funcţie de nivelele de autorizare sau pe baza unui sistem adecvat de parole.
Descrierea testului	1. ***Populaţia*** avută în vedere pentru constituirea eşantionului este formată din reţelele de calculatoare existente în cadrul entităţii, în număr de 8. 2. ***Eşantionul*** a fost reprezentat de 3 reţele, respectiv din cadrul direcţiei generale resurse umane, direcţiei generale buget-finanţe şi direcţiei generale administrativ - achiziţii. 3. ***Prin testarea*** ce se va realiza se va urmări, dacă politica de securitate a gestionării reţelelor informatice existente în cadrul organizaţiei este implementată şi asigurată protejarea datelor şi informaţiilor. Testarea s-a axat pe managementul securităţii reţelelor şi a avut în vedere următoarele: identificarea elementelor de bază din reţea clasificarea elementelor din reţea identificarea vulnerabilităţilor reţelei transformarea datelor de securitate, în informaţii monitorizarea securităţii reţelelor în timp procesul de remediere a vulnerabilităţilor reţelelor
Constatări	În urma analizei modului de gestionare a securităţii reţelelor, au rezultat următoarele: 1. La nivelul entităţii au fost elaborate harţi privind reţele informatice existente. În acest sens, au fost stabilite locaţiile serverelor, sistemelor desktop, sistemelor laptop, a routerelor, a punctelor de acces, a imprimantelor şi a celorlalte dispozitive conectate la reţea. Aceste hărţi au stat la baza elaborării sistemului de management al securităţii reţelelor din cadrul entităţii. Analiza celor 3 reţele care a constituit eşantionul, a pus în evidenţă faptul că pentru două reţele hărţile erau corespunzătoare, însă referitor la reţeaua care deservea direcţia generală buget-finanţe s-a constatat că, au fost achiziţionate şi conectate 4 noi computere şi o imprimantă de reţea, toate deservite prin intermediul unui nou router, care nu au fost consemnate în cadrul hărţii. De asemenea, pe cele 3 computere au fost copiate aplicaţiile contabile utilizate la nivelul direcţiei, fără a fi luate măsuri pentru asigurarea securităţii datelor şi informaţiilor prin controlarea accesului şi implementarea de programe antivirus adecvate. 2. La nivelul departamentului IT există o clasificare a sistemelor hardware, în funcţie de importanţa fiecărei categorii pentru buna desfăşurare a activităţii în cadrul entităţii. În acest sens, dispozitivele din reţea au fost grupate în funcţie de priorităţi, de la sisteme cu importanţă redusă, cum sunt sistemele de test sau care sunt folosite independent pentru asigurarea funcţiilor mai puţin importante ale entităţii şi sistemele de

	importanţă medie, cum sunt sistemele laptop folosite de unii angajaţi în cadrul delegaţiilor sau pentru lucrul acasă, la sisteme de importanţă majoră pentru asigurarea continuităţii activităţilor organizaţiei, cum ar fi sistemele care gestionează bazele de date, serverele care deservesc compartimentele cheie ale entităţii (tranzacţii, operaţiuni financiare etc.). Însă, în ceea ce priveşte aplicaţiile informatice la nivelul entităţii nu există o prioritizare a importanţei fiecăreia, în vederea implementării măsurilor corespunzătoare de securitate. Ex. - aplicaţia informatică utilizată la nivelul serviciului secretariat pentru urmărirea circuitului documentelor beneficiază de aceleaşi măsuri de securitate ca şi sistemul integrat privind conducerea organizaţiei. 3. Datorită faptului că în cadrul entităţii se folosesc servere, sisteme de operare şi platforme web diferite, identificarea vulnerabilităţilor sistemului în ansamblu este o activitate complexă şi necesară. Analiza rapoartele de activitate a pus în evidenţă faptul că s-a procedat la „peticirea" a vulnerabilităţilor, după care atenţia a fost îndreptată către riscurile medii şi mici. Acest mod de abordare are eficienţă în reducerea riscurilor, însă nu a fost corelat gradului de risc cu importanţa fiecărei activităţi realizate, ceea ce poate afecta vulnerabilitatea unor sisteme sau segmente de reţea.
Concluzii	Nu există stabilită în mod clar a hartă cu toate posturile din cadrul organizaţiei dotate cu computer, iar securitatea datelor şi informaţiilor nu este asigurată pe baza unui sistem de autorizare a accesului şi unui sistem adecvat de parole.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Radu George	Dumitru Daniel	Structură auditată

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 4.1.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2008
Întocmit: Popescu Sorin/ Radu George Data: 16.09.2009
Avizat: Dumitru Daniel Data: 16.09.2009

Problema	Posturile de lucru dotate cu computer nu sunt evidenţiate la nivelul Departamentului IT, neasigurându-se o intervenţie promptă şi rapidă. Securitatea datelor şi informaţiilor nu este asigurată pe baza unui sistem de autorizare a accesului şi unui sistem adecvat de parole.
Constatarea	1. La nivelul entităţii au fost elaborate harţi privind reţele informatice existente. În acest sens, au fost stabilite locaţiile serverelor, sistemelor desktop, sistemelor laptop, a routerelor, a punctelor de acces, a imprimantelor şi a celorlalte dispozitive conectate la reţea. Aceste hărţi au stat la baza elaborării sistemului de management al securităţii reţelelor din cadrul entităţii. Analiza celor 3 reţele care a constituit eşantionul, a pus în evidenţă faptul că pentru două reţele hărţile erau corespunzătoare, însă referitor la reţeaua care deservea direcţia generală buget-finanţe s-a constatat că, au fost achiziţionate şi conectate 4 noi computere şi o imprimantă de reţea, toate deservite prin intermediul unui nou router, care nu au fost consemnate în cadrul hărţii. De asemenea, pe cele 3 computere au fost copiate aplicaţiile contabile utilizate la nivelul direcţiei, fără a fi luate măsuri pentru asigurarea securităţii datelor şi informaţiilor prin controlarea accesului şi implementarea de programe antivirus adecvate. 2. La nivelul departamentului IT există o clasificare a sistemelor hardware, în funcţie de importanţa fiecărei categorii pentru buna desfăşurare a activităţii în cadrul entităţii. În acest sens, dispozitivele din reţea au fost grupate în funcţie de priorităţi, de la sisteme cu importanţă redusă, cum sunt sistemele de test sau care sunt folosite independent pentru asigurarea funcţiilor mai puţin importante ale entităţii şi sistemele de importanţă medie, cum sunt sistemele laptop folosite de unii angajaţi în cadrul delegaţiilor sau pentru lucrul acasă, la sisteme de importanţă majoră pentru asigurarea continuităţii activităţilor organizaţiei, cum ar fi sistemele care gestionează bazele de date, serverele care deservesc compartimentele cheie ale entităţii (tranzacţii, operaţiuni financiare etc.). Deşi există o clasificare a sistemelor hardware, în funcţie de importanţa fiecărei categorii în parte, în ceea ce priveşte aplicaţiile informatice, nu a fost avută în vedere o prioritizare a importanţei acestora în vederea alocării corespunzătoare a resurselor de securitate. Ex. - aplicaţia informatică utilizată la nivelul serviciului secretariat pentru urmărirea circuitului documentelor beneficiază de aceleaşi măsuri de securitate ca şi sistemul integrat privind conducerea organizaţiei. 3. Datorită faptului că în cadrul entităţii se folosesc servere, sisteme de operare şi platforme web diferite, identificarea vulnerabilităţilor sistemului în ansamblu este o activitate complexă şi necesară. Analiza rapoartelor de activitate a pus în evidenţă faptul că s-a procedat la „peticirea" vulnerabilităţilor, după care atenţia a fost îndreptată către riscurile medii şi mici. Acest mod de abordare are eficienţă în reducerea riscurilor, însă nu a fost corelat gradului de risc cu importanţa fiecărei activităţi realizate, ceea ce poate afecta

	vulnerabilitatea unor sisteme sau segmente de reţea. Administratorii de reţea au procedat la întocmirea de rapoarte prin care detaliază nivelul vulnerabilităţilor şi furnizează soluţii de remediere, însă informaţiile nu sunt adaptate şi prezentate persoanelor cu responsabilităţi decizionale asupra securităţii informaţionale.
Cauza	Lipsa unei prioritizări a aplicaţiilor în funcţie de importanţa lor în desfăşurarea activităţilor din cadrul entităţii. Lipsa unui sistem de analiză şi monitorizare a vulnerabilităţilor, care să identifice şi actualizeze vulnerabilităţile sistemului şi remedieze greşelile de configurare.
Consecinţa	Imposibilitatea protejării integrale a reţelelor IT, a alocării corespunzătoare a resurselor (spaţii de memorie, viteză de procesare, stabilitate) în cadrul reţelelor IT. Lipsa unei viziuni de ansamblu asupra vulnerabilităţilor care afectează funcţionalitatea reţelelor.
Recomandarea	Prioritizarea aplicaţiilor informatice, în funcţie de importanţa acestora, în vederea alocării corespunzătoare a măsurilor de securitate şi tratarea securităţii reţelelor ca pe un proces continuu. Implementarea unui sistem de management al vulnerabilităţilor, care să identifice vulnerabilităţile şi greşelile de configurare şi să dispună măsurile operative de soluţionare. Rapoartele întocmite în urma identificării şi soluţionării vulnerabilităţilor reţelelor să fie corelate şi aduse la cunoştinţa conducerii organizaţiei.

Auditor intern, Popescu Sorin

Supervizor, Dumitru Daniel

Pentru conformitate, Structura auditată

ENTITATEA PUBLICA
Serviciul Audit Intern

TEST nr. 4.2.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 16.09.2009
Avizat: Dumitru Daniel Data: 16.09.2009

Obiectul testului	Utilizatorii au parole de acces individuale
Obiectivele testului	Verificarea sistemului de prevenire şi detectare a accesărilor şi modificărilor sau transmiterilor neautorizate de baze de date.
Descrierea testului	Eşantionul cuprinde administratorul şi utilizatorii sistemului informatic din cadrul departamentului IT, care au în dotare 5 calculatoare. Testarea privind securitatea sistemului informatic a avut la bază Lista de verificare nr. 4, poziţia 4.2 astfel: • existenţa unui sistem de parole care să fie modificate periodic; • realizarea calendarului privind parolele de acces; • desemnarea unei persoane responsabile cu verificarea periodică a sistemului de parole de acces; Testul s-a materializat prin verificarea pe teren a existenţei sistemului de parole de acces şi a existenţei unui responsabil cu verificarea schimbării periodice a acestora de către utilizatori.
Constatări	Din verificarea sistemului de parole existent, pentru cele 5 calculatoare utilizate, prin observarea directă pe teren, s-a constatat: – inexistenţa unui sistem de parole de acces; – nedesemnarea unui responsabil cu verificarea schimbării sistemului de parole de acces; – inexistenţa unui sistem de informare sistematică a utilizatorilor.
Concluzii	Sistem inadecvat de parole utilizat în cadrul entităţii

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICA
Serviciul Audit Intern

INTERVIU nr.4.1.
privind Politica de securitate IT
adresat
domnului Pătrulescu George, Director Direcţia IT

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Nr. crt.	**Întrebări**	**Da**	**Nu**	**Obs.**
1.	Există o politică de securitate IT?	X		
2.	Există preocupări pentru securitatea IT?	X		
3.	Politica de securitate IT este actualizată?	X		
4.	Este desemnat un responsabil cu monitorizarea implementării politicii de securitate IT?	X		
5.	Este desemnat un responsabil cu gestionarea riscurilor la nivelul departamentului IT?	X		.
6.	Au fost întocmite şi transmise sistematic rapoarte de monitorizare?	X		
7.	Mai aveţi ceva de adăugat?		X	

Data: 16.09.2009

Dat în faţa noastră
Auditori,
Popescu Sorin
Radu George

Intervievat,
Pătrulescu George

ENTITATEA PUBLICA
Serviciul Audit Intern

FISĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 4.2.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 16.09.2009
Avizat: Dumitru Daniel Data: 16.09.2009

Problema	Neasigurarea securităţii sistemului informatic
Constatarea	Inexistenţa unui sistem de stabilire de către fiecare utilizator a parolelor şi a unui responsabil cu verificarea schimbării periodice a parolelor de acces. Analiza interviului a scos în evidenţă, de asemenea, faptul că nu există un sistem de securitate a sistemului informatic şi un responsabil cu administrarea acestui sistem.
Cauza	Entitatea nu aplică procedura care prevede schimbarea sistematică a parolelor, precum şi verificarea acestora de către o persoană responsabilă;
Consecinţa	Posibilitatea utilizării datelor şi informaţiilor din sistem în mod neadecvat de către persoane neautorizate; Vulnerabilitatea ridicată a sistemului în faţa unor intrări nedorite sau unor atacuri informaţionale.
Recomandarea	Schimbarea sistematică a parolelor de acces de către utilizatorii sistemului informatic; Stabilirea unei persoane care să aibă în responsabilitate atribuţii şi competenţe de verificare a schimbării periodice a parolelor de acces.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Radu George	Dumitru Daniel	Structură auditată

ENTITATEA PUBLICA
Serviciul Audit Intern

TEST nr. 4.3.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 16.09.2009
Avizat: Dumitru Daniel Data: 16.09.2009

Obiectul testului	Introducerea instrumentelor de control fizic asupra echipamentelor IT al aplicaţiilor.
Obiectivele testului	Examinarea modului de efectuare a controalelor fizice conform procedurilor
Descrierea testului	Populaţia statistică a fost constituită din structurile funcţionale ale organizaţiei identificate pe baza analizei organigramei entităţii publice. Eşantionul a fost constituit prin selectarea aleatoare a Direcţiei IT precum şi a Departamentului Financiar Contabil şi a Departamentului Resurse Umane unde sunt localizate servere ce deservesc necesităţile lor specifice, respectiv 20% din totalul populaţiei. Testarea a constat în examinarea următoarelor elemente stabilite prin *Lista de verificare, respectiv*: • Verificarea dotării camerelor în care se află servere-le cu echipamente adecvate, astfel: - camere de supraveghere care acoperă zona de intrare în camera serverului monitorizate permanent de serviciul ce asigură paza clădirii; - senzori de mişcare; - sistem de alarmă în caz de incendiu; - sistem de stingere a incendiilor; - echipamente de aer condiţionat; - uşi ignifugate echipate cu încuietori adecvate. Testarea s-a concretizat în elaborarea *Listei de control nr. 4.4 privind Evaluarea controalelor fizice în domeniul IT*.
Constatări	Din examinarea efectuata si observarea la fata locului s-au constatat unele disfuncţii legate de accesul necontrolat la toate cele trei locaţii selectate (Centrul IT, Departamentului Financiar Contabil, Departamentul Resurse Umane) atât a persoanelor din cadrul altor departamente cât şi a altor persoane din afara entităţii publice; Totodată, deşi au fost instalate camere de supraveghere, acestea nu sunt permanent monitorizate. Deseori, camerele în care sunt localizate servere-le sunt lăsate descuiate şi nesupravegheate, deşi sunt echipate cu încuietori adecvate; La scoaterea echipamentelor din cadrul organizaţiei nu există obligativitatea prezentării unei autorizaţii scrise.
Concluzii	Controalele fizice nu sunt implementate in mod eficient pentru a asigura securitatea echipamentelor

Auditor intern, **Supervizor,**
Popescu Sorin Dumitru Daniel

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICA
Serviciul Audit Intern

Lista control nr. 4.1.

privind efectuarea controalelor fizice conform procedurilor

Elemente testate / Eşantion	***Sistemul de controale fizice* implementat la nivelul camerelor în care se află servere**					
	Camere de supraveghere care acoperă zona de intrare în camera serverului monitorizate permanent de serviciul ce asigură paza clădirii	**Senzori de mişcare**	**Sistem de alarmă în caz de incendiu**	**Sistem de stingere a incendiilor**	**Echipamente de aer condiţionat**	**Uşi ignifugate echipate cu încuietori adecvate**
Direcţia IT	X	X	**X**	**X**	X	NU
Departamentul Financiar Contabil	X	X	**X**	X	X	NU
Departamentul Resurse Umane	NU	NU	**X**	X	X	NU

Data: 16.09.2009

Auditori,
Popescu Sorin
Radu George

Nota :
Echipa de auditori a constatat că nu au fost instalate nici camere de supraveghere care acoperă zona de intrare în camera serverului monitorizate permanent de serviciul ce asigură paza clădirii nici senzori de mişcare la nivelul Departamentul Resurse Umane. În prezenta Listă de control auditorii au punctat lipsa acestor controale cu menţiunea ”Nu” deoarece situaţia a fost remediată în timpul misiunii de audit şi nu s-a mai întocmit FIAP, dar aspectele negative constatate vor fi menţionate în Raportul de audit intern.

ENTITATEA PUBLICA
Serviciul Audit Intern

FISĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 4.3.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 16.09.2009
Avizat: Dumitru Daniel Data: 16.09.2009

Problema	Controalele fizice nu sunt implementate in mod eficient pentru a asigura securitatea echipamentelor
Constatarea	Din examinarea efectuata si observarea la fata locului s-a constatat unele disfuncţii legate de accesul necontrolat la toate cele trei locaţii selectate (Centrul IT, Departamentului Financiar Contabil, Departamentul Resurse Umane) atât a persoanelor din cadrul altor departamente cât şi a altor persoane din afara entităţii publice; Totodată, deşi au fost instalate camere de supraveghere, acestea nu sunt permanent monitorizate. Deseori, camerele în care sunt localizate servere-le sunt lăsate descuiate şi nesupravegheate, deşi sunt echipate cu încuietori adecvate; La scoaterea echipamentelor din cadrul organizaţiei nu există obligativitatea prezentării unei autorizaţii scrise.
Cauza	Controalele interne nu sunt implementate in totalitate si nu sunt stabilite responsabilităţi cu privire la asigurarea fizica a echipamentelor.
Consecinţa	Posibilitatea de dispariţie a unor echipamente lăsate nesupravegheate, cat si accesul nepermis la date si informaţii ale organizaţiei si utilizarea acestora in alte scopuri fata de interesul organizaţiei.
Recomandarea	Introducerea de instrumente de control adecvate astfel incit orice acces la echipamentele sau datele si informaţiile organizaţiei sa fie limitat, sau in cazurile in care acesta este permis sa fie supravegheat in totalitate.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Popesc Sorin	Dumitru Daniel	Structură auditată

Procedura – P10 – INTERVENŢIA LA FAŢA LOCULUI

ENTITATEA PUBLICĂ
Serviciul Audit Intern

LISTA DE VERIFICARE NR. 5

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 17.09.2009
Avizat: Dumitru Daniel Data: 17.09.2009

Obiectivul V.
PROIECTAREA ŞI TESTAREA PROGRAMELOR ŞI APLICAŢIILOR

Nr. crt.	Activitatea de audit	Da	Nu	Observaţii
A	**Proiectarea şi elaborarea programelor şi aplicaţiilor**			
1.	**Achiziţia programelor informatice**			
	Verificaţi dacă s-a realizat o fundamentare a deciziei privind achiziţia unui program existent pe piaţă, sau dezvoltarea acestuia în cadrul entităţii;	X		
	Verificaţi dacă s-a realizat un studiu al pieţei care să vizeze ofertele furnizorilor de programe necesare a fi achiziţionate;	X		
	Verificaţi dacă modul de concepere a programelor ţine cont de cerinţele activităţii utilizatorilor şi sunt compatibile cu alte sisteme utilizate de entitate;	X		
	Verificaţi dacă aplicaţia/programul este conceput astfel încât să suporte situaţii imprevizibile în utilizarea lui de către organizaţie;	X		
	Verificaţi dacă activităţile de testare se realizează astfel încât să nu afecteze prelucrările;	X		
1.	**Proiectarea programului informatic**			
1.1.	Verificaţi dacă în proiectarea unui program/aplicaţii fluxul de date a fost identificat corect şi complet în funcţie de specificul activităţilor şi periodicitatea acestora;	X		
1.2.	Verificaţi dacă în proiectarea programului/ aplicaţiei fluxul de date se au în vedere rezultatele aşteptate;	X		
1.3.	Verificaţi dacă pentru proiectarea unui program sau aplicaţie, procedurile sunt stabilite corect şi complet în funcţie de prelucrările care se vor aplica datelor în vederea obţinerii rezultatelor aşteptate;	X		
1.4.	Verificaţi dacă proiectarea unui program aplicaţie analizează situaţia existentă pentru a identifica potenţialele deficienţe în fluxul de date;	X		
1.5.	Verificaţi dacă algoritmul programului este elaborat adecvat pentru rezolvarea corectă a problemei;	X		
1.6.	Verificaţi dacă interfaţa programului ţine cont de structura şi formatul datelor de intrare;	X		
1.7.	Verificaţi dacă modelele de organizare, accesare, prelucrare şi arhivare a datelor sunt elaborate riguros prin folosirea celor mai adecvate soluţii tehnice;	X		
1.8.	Verificaţi dacă nivelul de independenţă faţă de platforma suport hardware şi software sunt stabilite conform specificaţiilor;	X		
1.9.	Verificaţi dacă mediile şi instrumentele de dezvoltare a programului/aplicaţiei sunt stabilite cu respectarea specificaţiilor;	X		

1.10.	Verificaţi dacă structura datelor introduse asigură o minimă redundanţă;	X		
1.11.	Verificaţi dacă sunt definite criterii de performanţă;			
1.12.	Verificaţi dacă pentru fiecare aplicaţie în parte sunt stabilite următoarele: numărul de utilizatori, rolurile acestora, privilegiile şi restricţiile aplicabile fiecărui rol in parte, accesul restricţionat;	X		
1.13.	Verificaţi dacă aplicaţia funcţionează cu respectarea filtrelor, protecţiilor, verificărilor implicite;	X		
1.14.	Verificaţi dacă au fost definite criterii pentru acceptarea aplicaţiilor;	X		
1.15.	Verificaţi dacă proiectarea aplicaţiei este monitorizată;	X		
1.16.	Verificaţi dacă erorile de funcţionare sunt transmise programatorilor;	X		
1.17.	Verificaţi dacă aplicaţia este instalată conform instrucţiunilor;	X		
1.18.	Verificaţi dacă versiunile aplicaţiilor instalate ulterior sunt compatibile şi utilizează toate resursele versiunilor anterioare;	X		
1.19.	Verificaţi dacă, în cazul în care noile versiuni nu sunt funcţionale, se mai pot restaura versiunile anterioare;	X		
1.20.	Verificaţi dacă cerinţele de dezvoltare a aplicaţiei sunt identificate de către utilizatori;	X		
1.21.	Verificaţi dacă comunicarea cu echipa de specialişti este permanentă pe timpul proiectării şi utilizării aplicaţiei;	X		
1.22	Verificaţi dacă schemele logice ale fiecărui program/aplicaţie sunt realizate corect şi complet;	X		
1.23.	Verificaţi dacă aplicaţiile permit reconfigurarea anumitor algoritmi, indicatori sau modele de calcul (de exemplu programele contabile să permită modificarea cotei TVA, etc.) în funcţie de schimbările legislative sau de altă natură.	X		
1.24.	Verificaţi dacă este implementat un sistem de raportare a erorilor către departamentul de suport tehnic.	X		
2.	**Elaborarea programului informatic**			
2.1.	Verificaţi dacă algoritmul programului/aplicaţiei este conform cu logica operaţiilor pentru obţinerea rezultatelor dorite;	X		
2.2.	Verificaţi dacă algoritmul respectă cerinţele de integrare ale aplicaţiei;	X		
2.3.	Verificaţi dacă interfaţa programului cu utilizatorul corespunde cerinţelor de comunicare om-calculator;	X		
2.4.	Verificaţi dacă limbajul de programare ales corespunde cerinţelor de proiectare;	X		
2.5.	Verificaţi dacă soluţiile de programare sunt utilizate în mod performant;	X		
2.6.	Verificaţi dacă graficul de realizare a programului şi bugetul sunt respectate;	X		
2.7.	Verificaţi dacă disfuncţionalităţile sau neconformităţile apărute în rularea programului sunt identificate pe baza mesajelor generate;	X		
2.8.	Verificaţi dacă identificarea erorilor este completată cu anumite coduri de eroare care însoţesc mesajele furnizate de aplicaţie;	X		
2.9.	Verificaţi dacă mesajele sunt analizate şi interpretate pentru identificarea cauzelor care au condus la apariţia lor;	X		
2.10.	Verificaţi dacă integrarea părţilor componente ale unui program se face respectând cerinţele utilizatorilor;	X		
2.11.	Verificaţi dacă documentaţia programului este conformă cu funcţiile realizate de acesta;	X		
2.12.	Verificaţi dacă documentaţia realizată prezintă în detaliu necesităţile tehnice hardware şi software;	X		
B.	**Testarea şi implementarea programelor şi aplicaţiilor**			
1.	**Testarea programului şi aplicaţiei**			
1.1.	Verificaţi dacă modul de testare al programului este stabilit în concordanţă cu precizările din documentaţie;	X		
1.2.	Verificaţi dacă datele de test sunt definite corespunzător prelucrărilor programului pe toate ramurile acestuia;	X		
1.3.	Verificaţi dacă datele de test evidenţiază riguros condiţiile de validare definite de program;	X		
1.4.	Verificaţi dacă programul / aplicaţia este executată cu date de test specifice pentru a constata modul de funcţionare a acestuia;	X		
1.5.	Verificaţi dacă neconformităţile şi erorile constatate în cursul testării sunt analizate cu atenţie;	X		

1.6.	Verificaţi dacă există un sistem automat de testare unitară a funcţionalităţilor de bază ale aplicaţiei.	X		
1.7.	Verificaţi dacă componentele testate sunt integrate în sistemul informatic după un plan bine stabilit, cu minimizarea consecinţelor negative;	X		
1.8.	Verificaţi dacă componentele nou integrate sunt testate cu rigurozitate;	X		
1.9.	Rezultatele testării sunt evaluate în concordanţă cu precizările din documentaţia programului/aplicaţiei;	X		
1.10.	Verificaţi dacă neconformităţile şi erorile semnalate în cursul testării sunt analizate şi soluţionate;	X		
1.11.	Verificaţi dacă corecţiile ce trebuie operate în program sunt stabilite şi conduc la o îmbunătăţire;	X		
1.12.	Verificaţi dacă programul/aplicaţia este instalată la utilizator conform procedurii specifice;	X		
1.13.	Verificaţi dacă datele de testare sunt generate în conformitate cu manualele de operare şi utilizare;	X		
1.14.	Verificaţi dacă simulările se realizează conform manualului de utilizare;	X		
1.15.	Verificaţi dacă rezultatele testărilor sunt analizate centralizat;	X		
1.16.	Verificaţi dacă rezultatele testării sunt interpretate conform manualelor de utilizare şi operare;	X		
1.17.	Verificaţi dacă aplicaţia corespunde cerinţelor reale;	X		
1.18.	Verificaţi dacă aplicaţia cu date reale rulează conform manualului de utilizare;	X		
1.19	Verificaţi dacă rezultatele sunt interpretate conform documentaţiei aplicaţiei;	X		
1.20.	Verificaţi dacă erorile constatate sunt comunicate programatorilor;	X		
1.21.	Verificaţi dacă corectitudinea rezultatelor este asigurată prin algoritmii de calcul utilizaţi de program/aplicaţie	X		
1.22.	Verificaţi dacă corectitudinea datelor este verificată prin modalităţi specifice;	X		
1.23.	Verificaţi dacă sunt puse la dispoziţia utilizatorului up-date-uri ale aplicaţiilor;	X		
1.24.	Verificaţi dacă filtrele, protecţiile şi verificările asigurate de program/aplicaţie sunt semnalate beneficiarului;	X		
1.25.	Verificaţi dacă erorile cauzate de algoritmii de calcul sunt îndepărtate prin corectarea acestora;	X		
1.26.	Verificaţi dacă etapele de testare sunt reluate corect şi în totalitate pentru a verifica îndepărtarea erorilor şi pentru a se asigura că nu au apărut altele noi.	X		
1.27	Verificaţi dacă după implementarea unui nou modul al aplicaţiei, documentaţia aferentă este actualizată.	X		
2.	**Asigurarea corectitudinii rezultatelor**			
2.1	Verificaţi dacă opţiunile şi parametrii de lucru ai programului/aplicaţiei sunt stabiliţi conform specificaţiilor din documentaţii;	X		
2.2.	Verificaţi dacă cerinţele hardware /software necesare rulării programului/aplicaţiei sunt adecvat specificate;	X		
2.3.	Verificaţi dacă condiţiile de funcţionare a programului/aplicaţiei sunt stabilite în concordanţă cu solicitările beneficiarului şi în funcţie de cerinţele aplicaţiei;	X		
2.4.	Verificaţi dacă condiţiile de funcţionare a programului/aplicaţiei sunt stabilite în concordanţă cu solicitările utilizatorului.	X		
2.5.	Verificaţi dacă procedura de instalare este elaborată cu respectarea condiţiilor de funcţionare a programului;	X		
2.6.	Verificaţi dacă programul/aplicaţia este instalată la beneficiar conform procedurii specifice şi urmare a solicitării acestuia;	X		
2.7.	Verificaţi dacă stocarea datelor asigură următoarele:		X	Test nr. 5.1. FIAP nr. 5.1.
	a) dacă o dată sau informaţie este stocată într-un singur fişier			
	b) dacă accesul se realizează uşor la o dată stocată şi în funcţie de nivelul de autorizare			
	c) dacă datele se pot accesa în mod global în cazul realizării de noi programe sau de utilizare a celor existente			
	d) dacă o dată sau informaţie este prezentată sau transmisă în aceeaşi formă de la un fişier la altul			

2.8.	Verificaţi dacă opţiunile şi parametrii de operare ai programului/aplicaţiei sunt setaţi conform specificaţiilor din documentaţii;	X		
2.9.	Verificaţi dacă condiţiile de funcţionare a programului/ aplicaţiei sunt refăcute după incidente hardware sau software;	X		
2.10.	Verificaţi dacă implementarea programului/aplicaţiei este monitorizată;	X		
2.11.	Verificaţi dacă istoricul aplicaţiilor menţionează operaţiile de întreţinere sau up-date-urile realizate;	X		
2.12.	Verificaţi dacă istoricul programului/ aplicaţiei este păstrat în siguranţă;	X		
2.13.	Verificaţi dacă utilizatori sunt instruiţi pentru însuşirea modului de operare cu programul/aplicaţia în conformitate cu documentaţia aferentă;	X		
2.14.	Verificaţi dacă eventualele dezvoltării ale aplicaţiei sunt aduse la cunoştinţa utilizatorilor;	X		
2.15.	Verificaţi dacă utilizatorii sunt asistaţi în lucrul efectiv cu programul/aplicaţia;	X		
2.16.	Verificaţi dacă reinstalarea aplicaţiei se realizează respectând procedurile standardizate;	X		
2.17.	Verificaţi dacă jurnalul privind intervenţiile de service este adus la cunoştinţa persoanelor responsabile;	X		
2.18.	Verificaţi dacă opţiunile şi parametrii de lucru ai aplicaţiei sunt setaţi conform documentaţiei aplicaţiei;	X		

Auditori,

Popescu Sorin
Radu George

ENTITATEA PUBLICA
Serviciul Audit Intern

TEST nr. 5.1.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 17.09.2009
Avizat: Dumitru Daniel Data: 17.09.2009

Obiectul testului	Asigurarea corectitudini datelor în cadrul programelor informatice
Obiectivele testului	Organizarea datelor în sistemele informatice
Descrierea testului	Populaţia statistică a fost constituită din fişierele da date constituite în vederea organizării şi păstrării datelor. Eşantionul pentru realizarea testării modului de organizare a datelor în sistemele informatice a fost constituit prin selectarea unui eşantion reprezentativ care cuprinde date din cadrul tuturor domeniilor de activitate din cadrul entităţii. Testarea a constat în examinarea următoarelor elemente: - dacă o dată sau informaţie este stocată într-un singur fişier - dacă accesul se realizează uşor la o dată stocată şi în funcţie de nivelul de autorizare - dată datele se pot accesa în mod global în cazul realizării de noi programe sau de utilizare a acelor existente - dacă o dată sau informaţie este prezentată sau transmisă în aceeaşi formă de la un fişier la altul Testarea s-a concretizat în elaborarea unei *Liste de control privind organizarea şi păstrarea datelor în cadrul sistemelor informatice*.
Constatări	Datele sunt stocate în memoria internă şi memoria externă a oricărui sistem de calcul. Organizarea datelor trebuie să asigure: - timp de acces minim la date; - apariţia în sistem a datelor o singură dată; - spaţiu de memorie internă şi externă pentru date cât mai mic; - reflectarea prin organizare a tuturor legăturilor dintre procesele economice pe care aceste date le reprezintă; - posibilitatea modificării structurii datelor şi a relaţiilor dintre date fără a produce schimbări în programele care le gestionează. Accesul la o înregistrare din fişierul de date se obţine prin parcurgerea înregistrărilor fişierului în secvenţa în care au fost stocate sau pe bază unui cod de identificare care să permită regăsirea rapidă a înregistrării. Accesul direct se obţine prin indexarea fişierelor, adică prin crearea unor tabele de indecşi care pentru fiecare valoare atributului care permite identificarea în mod unic a unei înregistrări din fişier. Organizarea datelor în fişierele de date prezintă următoarele disfuncţii: - redundanţă mare – stocarea datelor în mai multe fişiere - acces dificil la date – exploatarea multiutilizator a datelor necesită operaţii suplimentare de sortare, fuziune, ventilare - izolarea datelor – imposibilitatea realizării de programe pe calculator care să

	acceseze datele într-o manieră globală - actualizarea datelor prin adăugare, modificare, ştergere generează erori atunci când mai mulţi utilizatori doresc să modifice simultan aceleaşi date - dependenţa programelor faţă de date – modificările din structura datelor obligă la efectuarea de corecturi în programele de calculator - fiecare dată este descrisă independent în toate fişierele în care apar – dacă într-un fişier se modifică formatul şi valoarea unei date, acea modificare nu se transmite automat, pentru aceeaşi dată, în toate fişierele de date.
Concluzii	Organizarea datelor în fişierele de date nu asigură o stocare şi utilizare eficientă a acestora.

Auditor intern,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICA
Serviciul Audit Intern

FISĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 5.1.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 17.09.2009
Avizat: Dumitru Daniel Data: 17.09.2009

Problema	Organizarea datelor şi stocarea acestora nu asigură o utilizare şi exploatare eficientă a acestora.
Constatarea	Datele sunt stocate în memoria internă şi memoria externă a oricărui sistem de calcul. Organizarea datelor trebuie să asigure: - timp de acces minim la date; - apariţia în sistem a datelor o singură dată; - spaţiu de memorie internă şi externă pentru date cât mai mic; - reflectarea prin organizare a tuturor legăturilor dintre procesele economice pe care aceste date le reprezintă; - posibilitatea modificării structurii datelor şi a relaţiilor dintre date fără a produce schimbări în programele care le gestionează. Accesul la o înregistrare din fişierul de date se obţine prin parcurgerea înregistrărilor fişierului în secvenţa în care au fost stocate sau pe bază unui cod de identificare care să permită regăsirea rapidă a înregistrării. Accesul direct se obţine prin indexarea fişierelor, adică prin crearea unor tabele de indecşi care pentru fiecare valoare atributului care permite identificarea în mod unic a unei înregistrări din fişier. Organizarea datelor în fişierele de date prezintă următoarele disfuncţii: - redundanţă mare – stocarea datelor în mai multe fişiere - acces dificil la date – exploatarea multiutilizator a datelor necesită operaţii suplimentare de sortare, fuziune, ventilare - izolarea datelor – imposibilitatea realizării de programe pe calculator care să acceseze datele într-o manieră globală - actualizarea datelor prin adăugare, modificare, ştergere generează erori atunci când mai mulţi utilizatori doresc să modifice simultan aceleaşi date - dependenţa programelor faţă de date – modificările din structura datelor obligă la efectuarea de corecturi în programele de calculator fiecare dată este descrisă independent în toate fişierele în care apar – dacă într-un fişier se modifică formatul şi valoarea unei date, acea modificare nu se transmite automat, pentru aceeaşi dată, în toate fişierele de date.
Cauza	Lipsa specialiştilor, precum şi a participării personalului la diversele cursuri de specialitate organizate în afara entităţii, în vederea dobândirii cunoştinţelor necesare pentru organizarea eficientă a datelor.
Consecinţa	Exploatarea cu dificultate a datelor, apariţia erorilor în cadrul sistemelor de date existente urmare utilizării şi stocării incorecte a datelor, posibilitatea de modificare în mod necontrolat a unui sistem de date.
Recomandarea	Urmare creşterii necesarului de date şi informaţii şi a progreselor tehnologiilor informaţiei este necesară organizarea datelor în baze de date, respectiv un fişier format din înregistrări, care conţin câmpuri şi operaţii de căutare, sortare sau recombinare. Pentru aceasta este necesar realizarea următoarelor: - definirea, structurarea, ordonarea şi gruparea datelor în colecţii de date omogene;

	- stabilirea legăturilor între date, între elementele unei colecţii de date şi între colecţiile de date, după o ierarhie bine precizată; - memorarea datelor pe un suport informaţional prelucrabil într-un sistem de calcul.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Radu George	Dumitru Daniel	Structură auditată

ENTITATEA PUBLICĂ
Serviciul Audit Intern

LISTA DE VERIFICARE NR. 6

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 18.09.2009
Avizat: Dumitru Daniel Data: 18.09.2009

Obiectivul VI.
ELABORAREA ŞI IMPLEMENTAREA PROIECTELOR IT

Nr. crt.	Activitatea de audit	Da	Nu	Observaţii
A	**Dezvoltarea proiectelor IT**			
1.	**Iniţierea şi elaborarea proiectelor IT**			
1.1.	Analizaţi dacă situaţia pentru care trebuie implementat un proiect IT este bine izolată şi evaluată folosind mijloace specifice;	X		
1.2.	Analizaţi dacă lansarea proiectului pentru implementarea unor noi soluţii IT este stabilită după analiza detaliată a cauzelor şi efectelor pe termen lung ale perpetuării deficienţelor actuale;	X		
1.3.	Verificaţi dacă soluţiile propuse pentru implementarea unui proiect IT corespund cerinţelor identificate;	X		
1.4.	Verificaţi dacă obiectivele generale ale proiectului sunt stabilite cu respectarea strategiei generale a organizaţiei;	X		
1.5.	Analizaţi dacă componentele proiectului reflectă soluţiile ce trebuie implementate şi care vor conduce la realizarea obiectivelor stabilite;	X		
1.6.	Verificaţi dacă componentele proiectului sunt compatibile direct sau prin interfeţe cu proiectele aflate în derulare;	X		
1.7.	Verificaţi dacă rezultatele intermediare şi finale ale proiectului sunt evaluate folosind criterii adecvate;	X		
1.8.	Verificaţi dacă bugetul alocat proiectului permite obţinerea configuraţiilor hard/soft propuse;	X		
1.9.	Verificaţi dacă cheltuielile cu mentenanţa acoperă durata optimă de exploatare;	X		
1.10.	Verificaţi dacă implementarea proiectului propus beneficiază de asistenţă tehnică;	X		
1.11.	Verificaţi dacă cerinţele utilizatorilor proiectului sunt identificate corect şi complet;	X		
1.12.	Verificaţi dacă proiectele IT se pliază pe cerinţele utilizatorilor cărora le sunt destinate;	X		
1.13.	Verificaţi dacă proiectul propus a fi elaborat este comparat cu cele din portofoliul organizaţiei, pentru a identifica asemănări şi deosebiri de care să se ţină cont;	X		
1.14.	Verificaţi dacă proiectele propuse sunt competitive pentru organizaţie;	X		
1.15.	Verificaţi dacă monitorizarea riscurilor asigură viabilitatea planului de continuitate a activităţilor;	X		
1.16.	Verificaţi dacă frecvenţa şi complexitatea testărilor proiectelor implementate se bazează pe riscurile necontrolate.	X		
2.	**Monitorizarea performanţelor soluţiilor IT implementate**			

2.1.	Verificaţi dacă parametrii de referinţă şi valorile etalon ale programelor elaborate respectă specificaţiile şi se încadrează în standarde;	X		
2.2.	Verificaţi dacă regulile şi procedurile stabilite pentru supravegherea şi colectarea valorilor parametrilor de referinţă nu afectează lucrul utilizatorilor şi nici funcţionarea aplicaţiilor;	X		
2.3.	Verificaţi dacă regulile şi procedurile utilizate pentru evaluarea programelor nu conduc la ambiguităţi şi identifică posibilitatea apariţiei unei erori de funcţionare;	X		
2.4.	Verificaţi dacă jurnalele cu valorile de referinţă monitorizate sunt păstrate şi analizate periodic, pentru a se stabili corecţiile necesare;	X		
2.5.	Verificaţi dacă disfuncţionalităţile hard şi soft sesizate de către utilizatori sunt recepţionate şi sunt detectate cauzele;	X		
2.6.	Verificaţi dacă analizele şi rapoartele privind implementarea proiectelor IT propuse sunt întocmite riguros şi dacă evenimentele sau disfuncţiunile sunt evaluate şi se elaborează soluţii de remediere.	X		
B.	**Implementarea şi funcţionarea programelor şi aplicaţiilor**			
1.	**Reproiectarea soluţiilor IT pentru programe şi aplicaţii**			
1.1.	Verificaţi dacă punctele slabe, critice şi limitările unui program/aplicaţie sunt identificate;	X		
1.2.	Verificaţi dacă documentaţia cu fluxul de date şi prelucrările necesare este elaborată adecvat situaţiei reale;	X		
1.3.	Verificaţi dacă documentaţia întocmită constituie baza procesului de proiectare;	X		
1.4.	Verificaţi dacă soluţiile IT sunt proiectate pornind de la punctele slabe, critice detectate, de la evoluţiile tehnologice existente şi cele prefigurate de dezvoltarea entităţii;	X		
1.5.	Verificaţi dacă soluţiile noi propuse sunt axate pe atingerea obiectivelor strategiei de dezvoltare a organizaţiei;	X		
1.6.	Verificaţi dacă soluţiile noi au la bază o analiză cauză-efect, o analiză tehnică, precum şi o analiză a eficienţei investiţiei;	X		
1.7.	Verificaţi dacă soluţiile acceptate conduc la îmbunătăţirea performanţelor ţintelor propuse;	X		
1.8.	Verificaţi dacă soluţiile noi ţin cont de constrângerile existente în cadrul entităţii;	X		
1.9.	Verificaţi dacă soluţiile noi se încadrează în strategia de funcţionare şi dezvoltare a organizaţiei;	X		
1.10.	Verificaţi dacă studiile şi analizele elaborate evidenţiază clar impactul tehnologiilor propuse;	X		
1.11.	Verificaţi dacă riscurile legate de securitatea datelor sunt identificate şi evaluate corect şi complet;	X		
1.12.	Verificaţi dacă măsurile pentru prevenirea şi contracararea riscurilor sunt gândite adecvat situaţiei;	X		
1.13.	Verificaţi dacă procedurile pentru minimizarea unui atac la securitatea sistemului sunt elaborate şi sunt adecvate;	X		
2.	**Întreţinerea aplicaţiilor garantează funcţionarea proceselor la parametrii optimi**			
2.1.	Verificaţi dacă utilizarea computerelor/echipamentelor periferice sau a componentelor de conectare în reţea se realizează potrivit procedurilor specifice;	X		
2.2.	Verificaţi dacă se monitorizează mesajele de eroare în funcţionarea echipamentelor/aplicaţiilor;	X		
2.3.	Verificaţi dacă erorile sunt corectate direct sau prin intervenţii ale personalului de specialitate;	X		
2.4.	Verificaţi dacă informaţiile despre modul de funcţionare a calculatorului sau a echipamentelor sunt transmise în timp util utilizatorului;	X		
2.5.	Verificaţi dacă supravegherea proceselor aflate în execuţie şi a performanţelor aplicaţiilor, sistemelor sau programelor se realizează prin aplicarea procedurilor şi respectarea lor;	X		
2.6.	Verificaţi dacă evenimentele care indică performanţele şi starea sistemelor sunt înscrise şi păstrate în jurnale;	X		
2.7.	Verificaţi dacă imprimantele şi alte echipamente de reţea sunt corect	X		

	instalate şi sunt configurate corespunzător accesului partajat;			
2.8.	Verificaţi dacă funcţionarea echipamentelor de tipărire şi accesul utilizatorilor la acestea sunt verificate periodic;	X		
2.9.	Verificaţi dacă utilizatorii beneficiază permanent de asistenţă tehnică;		X	Test nr. 6.1. Foaie de lucru nr. 6.1. Listă de control 6.1. FIAP nr. 6.1.
	Verificaţi situaţia licenţelor deţinute pentru sistemul de operare Windows			
	Verificaţi situaţia licenţelor deţinute pentru pachetul de programe Microsoft Office			
	Verificaşi dacă entitatea publică a achiziţionat licenţe pentru programele utilizate			
	Analizaţi dacă au fost identificate limitările bugetare în privinţa achiziţiilor licenţelor şi dacă au fost găsite soluţii alternative			
	Analizaţi eventualele disfuncţionalităţi apărute în procesul de achiziţionare a licenţelor			
	Verificaţi existenţa soft-urilor nelicenţiate instalate de utilizatori			
	Verificaţi desemnarea responsabilităţilor privind achiziţionarea licenţelor pentru programele de calculator			
	Verificaţi existenţa controalelor de sistem ce alertează administratorul în cazul utilizării de soft-uri pentru care nu s-au achiziţionat licenţe			
2.10.	Verificaţi dacă conectarea şi comunicarea calculatoarelor în reţea sunt permanent supravegheate şi menţinute;	X		
2.11.	Verificaţi dacă funcţionarea serviciilor din reţea şi accesul utilizatorilor la servicii sunt atent monitorizate;	X		
2.12.	Verificaţi dacă interconectarea reţelelor, inclusiv conectarea la reţeaua Internet este supravegheată cu responsabilitate;	X		
2.13.	Verificaţi dacă apariţia situaţiilor deosebite sunt aduse la cunoştinţa administratorului de reţea;	X		
2.14.	Verificaţi dacă dispozitivele de stocare a datelor sunt utilizate conform instrucţiunilor specifice de lucru;	X		
2.15.	Verificaţi dacă salvările de siguranţă sunt păstrate în condiţii adecvate;	X		
2.16.	Verificaţi dacă datele salvate anterior se pot restaura la nevoie şi utilizatorii sunt asistaţi pentru recuperarea integrală a acestora;	X		
2.17.	Verificaţi dacă procedurile de salvare sunt corespunzătoare strategiei de securitate;	X		
2.18.	Verificaţi dacă sistemele de operare şi aplicaţiile sunt instalate, modernizate sau configurate folosind proceduri standardizate;	X		
2.19.	Verificaţi dacă modul de funcţionare a echipamentelor, a sistemelor de operare şi a aplicaţiilor folosite de utilizatori este verificat periodic;	X		
2.20.	Verificaţi dacă erorile şi incidentele apărute sunt remediate operativ;	X		

Auditori,

Popescu Sorin

Radu George

ENTITATEA PUBLICA
Serviciul Audit Intern

TEST nr. 6.1.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 18.09.2009
Avizat: Dumitru Daniel Data: 18.09.2009

Obiectul testului	Situaţia licenţelor pentru programele de calculator
Obiectivele testului	Verificarea achiziţionării de licenţe pentru programele utilizate de către entitatea publică; Identificarea eventualelor limitări bugetare în privinţa achiziţionării licenţelor şi a acţiunilor întreprinse de departamentul IT în aceste condiţii; Analiza eventualelor disfuncţionalităţi apărute în procesul de achiziţionare a licenţelor şi a modului de soluţionare a lor.
Descrierea testului	Eşantionul pentru realizarea testării situaţiei licenţelor pentru programele de calculator utilizate a fost stabilit pe baza unui procent de 5%, din totalul populaţiei de 580 de calculatoare, respectiv 29 calculatoare personale, conform *foii de lucru* anexate. Pentru fiecare post de lucru dotat cu calculator a fost verificată situaţia licenţelor deţinute atât pentru sistemul de operare Windows, cât şi pentru pachetul de programe Microsoft Office. Testarea a constat în examinarea elementelor stabilite potrivit listei de verificare, şi anume: - verificarea situaţiei licenţelor deţinute pentru sistemul de operare Windows; - verificarea situaţiei licenţelor deţinute pentru pachetul de programe Microsoft Office; - verificarea dacă entitatea publică a achiziţionat licenţe pentru programele utilizate; - identificarea eventualelor limitări bugetare în privinţa achiziţionării licenţelor; - analiza eventualelor disfuncţionalităţi apărute în procesul de achiziţionare a licenţelor; - verificarea existenţei soft-urilor nelicenţiate instalate de utilizatori; - verificarea desemnării responsabilităţilor privind achiziţionarea licenţelor pentru programele de calculator; - verificarea existenţei controalelor de sistem ce alertează administratorul în cazul utilizării de soft-uri pentru care nu s-au achiziţionat licenţe. Testarea s-a concretizat în elaborarea *Listei de control nr. 3.5. privind situaţia licenţelor pentru programele de calculator.*
Constatări	Din analiza Listei de control nr. 3.5, s-au constatat ca angajaţii unor departamente folosesc programe aferente pachetului Microsoft Office fără ca pentru acestea entitatea publică să fi achiziţionat licenţe. Aceste programe au fost instalate folosind coduri piratate. De asemenea, sistemul IT al entităţii publice nu a fost prevăzut cu controale care să-i permită alertarea administratorului de sistem în cazul utilizării unor astfel de programe, fără licenţă.
Concluzii	Utilizarea în cadrul entităţii publice a unor programe software fără licenţă

Auditor intern,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICA
Serviciul Audit Intern

FOAIE DE LUCRU NR. 6.1.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Obiectul nr. 3: *Situaţia licenţelor pentru programele de calculator*

Obiectivul : *Verificarea achiziţionării de licenţe pentru programele utilizate de către entitatea publică*

Testarea se va realiza pe un eşantion care a fost constituit astfel:

- populaţia totală este de 250 calculatoare personale;
- eşantionul va fi de 2%, respectiv 250 x 2% = 5 calculatoare personale;
- pasul de selecţie va fi 250 : 5 = 50;
- eşantionul se va constitui din calculatoarele existente în Lista de inventariere a calculatoarelor personale din entitatea publică începând de la poziţia 0 şi va cuprinde computerele cu numerele de inventar: 50, 100, 150, 200, 250
- eşantionul constituit va fi verificat integral;
- în urma verificării se va întocmi un test.

Data: 18.04.2009

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICA
Serviciul Audit Intern

Lista control nr. 6.1.

privind Situaţia licenţelor pentru programele de calculator

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Elemente testate / **Eşantion**	**Verificarea situaţiei licenţelor deţinute atât pentru sistemul de operare Windows**	**Verificarea situaţiei licenţelor deţinute atât pentru pachetul de programe Microsoft Office**	**Verificarea existenţei soft-urilor nelicenţiate instalate de utilizatori**	**Verificarea existenţei controalelor de sistem ce alertează administratorul în cazul utilizării de soft-uri pentru care nu s-au achiziţionat licenţe**
*Computer înregistrat cu număr de inventar **50***	X	X	X	FIAP
*Computer înregistrat cu număr de inventar **100***	X	FIAP	X	FIAP
*Computer înregistrat cu număr de inventar **150***	X	FIAP	X	FIAP
*Computer înregistrat cu număr de inventar **200***	X	X	X	FIAP
*Computer înregistrat cu număr de inventar **250***	X	X	X	FIAP

Data: 18.09.2009

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICA
Serviciul Audit Intern

FISĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 6.1.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 13.09.2009
Avizat: Dumitru Daniel Data: 13.09.2009

Problema	Utilizarea în cadrul entităţii publice a unor programe software fără licenţă.
Constatarea	Cu toate că entitatea publică a achiziţionat licenţe pentru pachetul de programe Lotus, s-au constatat că în cadrul unor departamente se folosesc programe aferente pachetului Microsoft Office fără ca pentru acestea entitatea publică să fi achiziţionat licenţe. Practic salariaţii au instalat programe utilizând CD-uri piratate. La nivelul sistemului IT al entităţii publice s-a constatat inexistenţa controalelor de sistem ce alertează administratorul în cazul utilizării de soft-uri pentru care nu s-au achiziţionat licenţe.
Cauza	Salariaţii entităţii publice au observat că deşi programele existente permit realizarea sarcinilor de serviciu, totuşi programele din pachetul Microsoft Office sunt mai fiabile, mai flexibile şi permit realizarea unui număr mai mare de operaţiuni, cu care sunt deja familiarizaţi. De asemenea această situaţie a fost generată şi de primirea de la alte entităţi publice a unor fişiere electronice create cu programele din pachetul Microsoft Office, şi care nu au putut fi prelucrate în continuare folosind programele Lotus.
Consecinţa	Entitatea publică este pasibilă de sancţiuni din partea Oficiului Român pentru Drepturi de Autor, pentru utilizarea unor programe fără licenţă; Soft-urile nelicenţiate instalate de utilizatori pot conţine viruşi, troieni sau alte programe ce ar putea afecta în mod grav subsistemele IT la care au acces aceşti utilizatori, sau chiar sistemul IT în ansamblul său;
Recomandarea	Inventarierea tuturor staţiilor de lucru pentru a stabili situaţia reală privind utilizarea programelor fără licenţă; Dezinstalarea tuturor programelor nelicenţiate din pachetul Microsoft Office; Realizarea unei analize complexe în urma căreia managementul entităţii publice să decidă asupra oportunităţii schimbării programelor existente şi achiziţionarea unui număr adecvat de licenţe Microsoft Office.

Auditor intern,	**Supervizor,**	**Pentru conformitate,**
Radu George	Dumitru Daniel	Structură auditată

ENTITATEA PUBLICĂ
Serviciul Audit Intern

LISTA DE VERIFICARE NR. 7

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01. 2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 19.09.2009
Avizat: Dumitru Daniel Data: 19.09.2009

Obiectivul 7.

PROIECTAREA, IMPLEMENTAREA ŞI MENŢINEREA ÎN FUNCŢIUNE A UNEI REŢELE

Nr. crt.	Activitatea de audit	Da	Nu	Observaţii
A	**Proiectarea, instalarea şi administrarea reţelei de calculatoare**			
1.	**Asigurarea bunei funcţionări a sistemelor bazate pe existenţa şi funcţionarea reţelei de calculatoare**			
1.1.	Verificaţi dacă resursele materiale necesare pentru urmărirea performanţelor şi menţinerea în funcţiune a reţelei de calculatoare sunt stabilite corect pe componente, respectiv server, client, echipament de conectare la reţea;	X		
1.2.	Verificaţi dacă resursele umane sunt identificate şi stabilite ca dimensiune atât numeric, cât şi în raport de competenţele necesare;	X		
1.3.	Verificaţi dacă echipamentele din reţea sunt administrate centralizat;	X		
1.4.	Verificaţi dacă pentru fiecare echipament din reţea îi sunt asociate proceduri, operaţii şi termene de efectuare;	X		
1.5.	Verificaţi dacă subsistemele existente pot fi configurate şi supravegheate individual;	X		
1.6.	Verificaţi dacă configurarea reţelei, conectarea componentelor în reţea, distribuirea serviciilor conduc la creşterea productivităţii muncii în organizaţie;	X		
1.7.	Verificaţi dacă numărul componentelor de tip server şi al celor de tip client se stabileşte în conformitate cu activităţile desfăşurate în organizaţie;	X		
1.8.	Verificaţi dacă serverele şi staţiile client sunt amplasate în reţea şi configurate conform regulilor impuse prin strategia de securitate;	X		
1.9.	Verificaţi dacă riscul apariţiei erorilor previzibile este corect evaluat;	X		
1.10.	Verificaţi dacă la apariţia incidentelor neprevăzute, sunt puse în practică proceduri de răspuns special prevăzute;	X		
1.11.	Verificaţi dacă regulile stabilite şi implementate asigură accesul controlat şi sigur al utilizatorilor numai la acele resurse de care au nevoie pentru îndeplinirea sarcinilor de serviciu conform fişei postului;	X		
1.12.	Verificaţi dacă datele disponibile şi folosite în reţea sunt corecte, sigure şi obţinute la timp;	X		
1.13.	Verificaţi dacă regulile stabilite şi implementate pentru urmărirea traficului de informaţii în reţea, a încărcării reţelei, a performanţelor serverelor şi serviciilor sunt folosite numai pentru evaluarea corectă a stării de funcţionare a reţelei şi a componentelor ei;	X		
1.14.	Verificaţi dacă dezvoltarea, adaptarea sau reconfigurarea reţelei se realizează pe baza evaluării modului de funcţionare şi au drept scop creşterea performanţelor serviciilor şi diminuarea încărcării reţelei în anumite puncte;	X		
1.15.	Verificaţi dacă lista parametrilor de referinţă şi valorile etalon folosite pentru evaluarea performanţelor echipamentelor hardware şi ale componentelor software respectă specificaţiile producătorilor şi se încadrează în standarde;	X		

1.16.	Verificaţi dacă pentru fiecare echipament este stabilit un set propriu de parametri şi valori acceptate, conform standardelor de funcţionare;	X		
1.17.	Verificaţi dacă regulile, procedurile şi criteriile folosite pentru evaluarea performanţelor nu conduc la ambiguităţi şi identifică din timp posibilitatea apariţiei unor erori de funcţionare.	X		
1.18.	Verificaţi dacă jurnalele cu valorile măsurate ale parametrilor de referinţă sunt păstrate şi analizate periodic, în vederea stabilirii corecţiilor suplimentare pentru preîntâmpinarea apariţiei erorilor de funcţionare;	X		
1.19.	Verificaţi dacă erorile, nefuncţionalităţile sunt evaluate şi sunt elaborate soluţii de remediere;	X		
1.20.	Verificaţi dacă vulnerabilităţile sunt identificate şi corectate;	X		
1.21.	Verificaţi dacă fiecare componentă a reţelei este evaluată conform unui etalon standard.	X		
2.	**Administrarea serverelor**			
2.1.	Verificaţi dacă resursele hardware instalate respectă indicaţiile producătorului;	X		
2.2.	Verificaţi dacă resursele hardware instalate şi configurate respectă cerinţele IT implementate în organizaţie;	X		
2.3.	Verificaţi dacă accesul şi utilizarea resurselor serverului respectă strategia de securitate a reţelei;	X		
2.4.	Verificaţi dacă programele sunt instalate şi configurate conform specificaţiei producătorilor;	X		
2.5.	Verificaţi dacă permisiunea de administrare a unui program este acordată numai personalului calificat şi cu respectarea strategiei de securitate a reţelei;	X		
2.6.	Verificaţi dacă administrarea programelor se face de la distanţă folosind instrumente specifice;	X		
2.7.	Verificaţi dacă activităţile de întreţinere hardware sau software sunt planificate conform cerinţelor din instrucţiunile de utilizare;	X		
2.8.	Verificaţi dacă soluţiile de salvare ale unui program sunt corecte şi eficiente;	X		
2.9.	Verificaţi dacă jurnalele obţinute prin monitorizarea programelor sunt păstrate pentru a fi periodic consultate;	X		
2.10.	Verificaţi dacă jurnalele identifică utilizatorii care au avut acces la program, în limita permisiunilor ce le-au fost acordate;	X		
2.11.	Verificaţi dacă jurnalele identifică tentativele nereuşite ale utilizatorilor de a avea acces la programe;	X		
2.12	Verificaţi dacă intruşii din interior sau exterior pot fi identificaţi prin informaţiile păstrate în jurnale.	X		
B.	**Interconectarea şi securitatea reţelei**			
1.	**Interconectarea reţelelor**			
1.1.	Verificaţi dacă conexiunile dintre reţele sunt conforme cu arhitectura generală şi respectă standardele de interconectare;	X		
1.2.	Verificaţi dacă componentele hardware şi software ale echipamentelor de legătură sunt configurate respectând regulile de securitate a transmisiilor de date din strategia de securitate a organizaţiei;	X		
1.3.	Verificaţi dacă tabelele de rutare sunt corect configurate şi indică adresele reţelelor accesibile;	X		
1.4.	Verificaţi dacă instalarea şi configurarea echipamentelor de legătură între reţele respectă instrucţiunile din documentaţia tehnică;	X		
1.5.	Verificaţi dacă instalarea şi configurarea componentelor software respectă indicaţiile producătorilor şi sunt conforme strategiei de securitate;	X		
1.6.	Verificaţi dacă cerinţele de conectare la Internet sunt identificate în conformitate cu fişa postului pentru fiecare categorie de personal şi respectă strategia de securitate;	X		
1.7.	Verificaţi dacă accesul permis din reţeaua Internet la programele şi aplicaţiile organizaţiei respectă strategia de securitate privitoare la accesul la informaţiile organizaţiei;	X		

1.8.	Verificaţi dacă conectarea la Internet se realizează în conformitate cu standardele de securitate în vigoare;	X		
1.9.	Verificaţi dacă sunt implementate reguli de securitate pentru accesul la şi din reţeaua Internet în conformitate cu strategia de securitate a organizaţiei;	X		
1.10.	Verificaţi dacă accesul prin intermediul Internet-ului la programe este strict monitorizat pentru detectarea tentativelor de acces neautorizat;	X		
1.11.	Verificaţi dacă tentativele de acces neautorizat sunt urmate de declanşarea procedurilor de securitate.	X		
2.	**Proiectarea şi asigurarea securităţii reţelei**			
2.1.	Verificaţi dacă cerinţele de asigurare a securităţii reţelei sunt identificate în funcţie de activităţile desfăşurate;	X		
2.2.	Verificaţi dacă cerinţele de asigurare a securităţii transmisiilor de date sunt stabilite în funcţie de activităţile desfăşurate;	X		
2.3.	Verificaţi dacă vulnerabilităţile şi ameninţările sunt corect identificate şi prioritizate;	X		
2.4.	Verificaţi dacă obiectivele activităţii de management al riscurilor sunt eliminarea, atenuarea sau transferul riscurilor;	X		
2.5.	Verificaţi dacă fiecărui risc identificat îi corespunde un set de proceduri a căror aplicare conduce la atenuarea sau eliminarea pagubelor;	X		
2.6.	Verificaţi dacă procedurile de securitate respectă principiul apărării / imunizării procesului vizat de eventuale atacuri informatice;	X		
2.7.	Verificaţi dacă procedurile de securitate elaborate pentru protecţia datelor, aplicaţiilor, sistemelor de operare şi echipamentelor sunt eficiente;	X		
2.8.	Verificaţi dacă procedurile de securitate ce trebuie implementate sunt aduse operativ la cunoştinţa personalului;	X		
2.9.	Verificaţi dacă sistemele de operare şi aplicaţiile sunt configurate astfel încât să aplice automat procedurile de securitate;	X		
2.10.	Verificaţi dacă transmisiile de date şi comunicaţiile în reţea sunt configurate astfel încât să aplice automat procedurile de securitate;	X		
2.11.	Verificaţi dacă jurnalele de evenimente sunt analizate periodic pentru identificarea potenţialelor lipsuri de securitate;	X		
2.12.	Verificaţi dacă reacţiile managerilor şi ale personalului faţă de securitatea reţelei sunt periodic şi atent evaluate;	X		
2.13.	Verificaţi dacă aplicarea procedurilor de securitate împiedică buna desfăşurare a activităţilor organizaţiei;	X		
2.14.	Verificaţi dacă detectarea unui incident neprevăzut determină o reacţie prestabilită.	X		
2.15.	Verificaţi modul de implementare a măsurilor privind siguranţa accesului utilizatorilor în reţea conform procedurilor;	X		
2.16.	Verificaţi modul de alocare a numelui de utilizator şi parolei aferente pentru accesul la reţea;		X	Test nr. 7.1. Foaie de lucru nr. 7.1. Listă de control 7.1. FIAP nr. 7.1.
2.17.	Verificarea monitorizării siguranţei accesului utilizatorilor în reţea			
2.18.	Analizaţi dacă a fost elaborată documentaţia tehnică adecvată privind conectarea la Internet.	X		
2.19.	Verificaţi dacă această documentaţie este adecvată şi actualizată	X		
2.20.	Determinaţi dacă manualele privind utilizarea reţelei au în vedere asigurarea securităţii comunicării datelor în reţea.	X		
2.21.	Analizaţi acţiunile întreprinse în cazurile în care a fost ameninţată integritatea şi eficacitatea transmiterii datelor în reţea.	X		
2.22.	Verificaţi existenţa procedurilor şi desemnarea responsabilităţilor pentru monitorizarea controalelor fizice;	X		
2.23.	Verificaţi efectuarea controalelor fizice conform procedurilor;	X		
2.24.	Analiza siguranţei accesului la reţea şi a comunicării datelor în reţea	X		
2.25	Monitorizarea conectării la reţea conform listei de logare;	X		
2.26.	Analizaţi rapoartele de monitorizare a traficului datelor în reţea.	X		
2.27.	Verificaţi existenţa procedurilor şi desemnarea responsabilităţilor pentru monitorizarea accesului utilizatorilor în reţea;	X		

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICA
Serviciul Audit Intern

TEST nr. 7.1.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 19.09.2009
Avizat: Dumitru Daniel Data: 19.09.2009

Obiectul testului	Proiectarea şi asigurarea securităţii reţelei
Obiectivele testului	Siguranţa accesului la reţea şi a comunicării datelor în reţea
Descrierea testului	Populaţia statistică a fost constituită din cele 250 de calculatoare existente la nivelul entităţii publice, conform Listei de inventariere a calculatoarelor personale. Eşantionul pentru realizarea testării siguranţei accesului la reţea a fost stabilit pe baza unui procent de 2%, din totalul populaţiei statistice, respectiv 5 calculatoare personale, conform Foii de lucru nr. 4.5. Testarea a constat în examinarea următoarelor elemente stabilite prin Lista de verificare nr. 4, poz. 4.5, şi anume: - Verificaţi modul de alocare a numelui de utilizator şi parolei aferente pentru accesul la reţea ; - Monitorizarea conectării la reţea conform listei de log-are. Testarea s-a concretizat în elaborarea Listei de control nr. ….. privind accesul şi comunicarea datelor în reţea.
Constatări	Din analiza *Listei de control* rezultate, s-au constatat următoarele: a. majoritatea salariaţilor din cadrul entităţii publice, prin natura sarcinilor de serviciu, trebuie să acceseze mai multe subsisteme IT care folosesc nume de utilizator şi parole diferite. Sistemul IT este conceput astfel încât pentru accesul la fiecare subsistem IT trebuie folosite nume de utilizator şi parolă diferite, în loc să se folosească acelaşi nume de utilizator şi parolă indiferent de subsistemul IT la care se conectează angajatul. b. datorită numărului mare de parole ce trebuiesc utilizate de salariaţi, deseori aceştia notează parolele pe documente lăsate pe birou. Astfel salariaţii cunosc parolele colegilor de serviciu, putându-se conecta la subsistemele IT folosindu-le datele de identificare şi prin urmare putând să vizualizeze şi/sau modifice date aflate în acele subsisteme IT. c. practic, sistemul de parole nu mai are funcţii principale de restricţionare a accesului persoanelor nepotrivite, ci îngreunează funcţionarea sistemului. d. în situaţia apariţiei unor incidente nu se pot stabili responsabilităţile aferente.
Concluzii	Sistemul de parole este stabilit si utiliza in mod neadecvat

Auditor,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICA
Serviciul Audit Intern

FOAIE DE LUCRU NR. 7.1.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009

Obiectiv: Siguranţa accesului la reţea şi a comunicării datelor în reţea

Testarea se va realiza pe un eşantion care a fost constituit astfel:

- populaţia totală este de 250 calculatoare personale;
- eşantionul va fi de 2%, respectiv 250 x 2% = 5 calculatoare personale;
- pasul de selecţie va fi 250 : 5 = 50;
- eşantionul se va constitui din calculatoarele existente în Lista IP-urilor calculatoarelor ce se conectează la reţeaua entităţii publice la poziţiile:
  35, 85, 135, 185, 235
- eşantionul constituit va fi verificat integral;
- în urma verificării se va întocmi un test.

Data: 19.09.2009

Auditor,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICA
Serviciul Audit Intern

Lista control nr. 7.1.
Privind accesul şi comunicarea datelor în reţea

Elemente Testate / Eşantion	Verificaţi modul de alocare a numelui de utilizator şi parolei aferente pentru accesul la reţea	Monitorizarea conectării la reţea conform listei de log-are
*Computer aflat la poziţia **35***	FIAP	X
*Computer aflat la poziţia **85***	X	X
*Computer aflat la poziţia **135***	FIAP	X
*Computer aflat la poziţia **185***	FIAP	X
*Computer aflat la poziţia **235***	X	X

Data: 19.09.2009

Auditor,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICA
Serviciul Audit Intern

FISĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI nr. 7.1.

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 19.09.2009
Avizat: Dumitru Daniel Data: 19.09.2009

Problema	Neutilizarea unui singur nume de utilizator şi unei singure parole pentru accesul la sistemul IT.
Constatarea	Din evaluare s-a constatat că majoritatea salariaţilor din cadrul entităţii publice, prin natura sarcinilor de serviciu, trebuie să acceseze mai multe subsisteme IT care folosesc nume de utilizator şi parole diferite. Sistemul IT este conceput astfel încât pentru accesul la fiecare subsistem IT trebuiesc folosite: nume de utilizator şi parolă diferite, în loc să se folosească acelaşi nume de utilizator şi parolă indiferent de subsistemul IT la care se conectează angajatul.
Cauza	Inexistenţa unor proceduri de lucru adecvate potrivit cărora sa fie reglementat modul de conectare a echipamentelor la reţea sau programe si aplicaţii.
Consecinţa	Datorită numărului mare de parole ce trebuiesc utilizate de salariaţi, deseori aceştia notează parolele pe documente lăsate pe birou. Astfel salariaţii cunosc parolele colegilor de serviciu, putându-se conecta la subsistemele IT folosindu-le datele de identificare şi prin urmare putând să vizualizeze şi/sau modifice date aflate în acele subsisteme IT. În situaţia apariţiei unor incidente nu se pot stabili responsabilităţile adecvate.
Recomandarea	Realizarea unui proces de reenginering la nivelul sistemului IT din cadrul entităţii publice, astfel încât salariaţii să poată accesa subsistemele IT de care au nevoie utilizând un singur nume de utilizator şi o singură parolă;

Auditor,	Supervizor,	Pentru conformitate
Radu George	Dumitru Daniel	Structura auditată

Procedura – P10: REVIZUIREA DOCUMENTELOR DE LUCRU

Entitatea Publică
Serviciul de Audit Intern

CONSTITUIREA DOSARELOR DE AUDIT INTERN

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 20.09.2009
Avizat: Dumitru Daniel Data: 20.09.2009

După finalizarea intervenţiei la faţa locului, se constituie *Dosarele de audit intern* în vederea asigurării unei legături între obiectivele stabilite prin programul de audit, intervenţia la faţa locului şi raportul de audit public intern. Documentele culese şi/sau întocmite pe timpul misiunii de audit se constituie în următoarele dosare:

A. ***Dosarul permanent,*** care cuprinde:

a) *Secţiunea A – Raportul de audit intern şi anexele acestuia:*
- Ordinul de serviciu;
- Declaraţia de independenţă;
- Rapoartele de audit intern (intermediar, final, sinteza Raportului de audit intern);
- teste;
- Fişele de identificare şi analiză a problemelor;
- Formularele de constatare a iregularităţilor;
- Programul intervenţiei la faţa locului.

b) *Secţiunea B – administrativă:*
- Notificarea privind declanşarea misiunii de audit;
- Minuta şedinţei de deschidere;
- Minuta reuniunii de conciliere;
- Minuta şedinţei de închidere;
- Corespondenţa cu entitatea structurii auditate;

c) *Secţiunea C - documentaţia misiunii de audit public intern:*
- strategii interne;
- reguli, regulamente şi legi aplicabile;
- proceduri de lucru;
- materiale despre entitatea/structura auditată;
- rapoarte de audit public intern anterioare;
- informaţii privind fluxul de informaţii;
- documentaţia analizei riscului;
- documentaţia privind sistemul de control (aprobări, autorizări, separarea sarcinilor, supervizarea, reconcilierea, rapoarte etc.);

d) *Secţiunea D - supervizarea şi revizuirea desfăşurării misiunii* şi a rezultatelor acesteia şi cuprinde Lista de supervizare a documentelor;

B. *Dosarul documentelor de lucru* cuprinde copii xerox a documentelor justificative, care confirmă şi sprijină concluziile. Dosarul se indexează prin atribuirea de litere şi cifre pentru fiecare secţiune/obiectiv din cadrul programului.

Dosarele de audit public intern sunt proprietatea entităţii publice şi sunt confidenţiale şi *se păstrează până la îndeplinirea recomandărilor din raportul de audit intern*, după care se arhivează potrivit reglementarilor legale privind arhivarea.

Notă:

Constituirea dosarelor de audit intern se realizează în finalul intervenţiei la faţa locului şi are ca scop de a asigura o legătură între obiectivele misiunii de audit stabilite prin programul de audit, constatările efectuate în etapa de intervenţie la faţa locului şi raportul de audit public intern.

Documentele de lucru trebuie organizate astfel încât să faciliteze trecerea în revistă a dosarului şi să permită o comparaţie rapidă între constatările şi probele de audit.

Este necesară clasificarea tuturor documentelor de lucru, în funcţie de etapa de activitate căreia îi corespund.

Sursa de informaţie trebuie indicată clar şi precis, pentru a păstra şi a verifica ulterior fiabilitatea ei.

Procedura P10:	**REVIZUIREA DOCUMENTELOR DE LUCRU**

Entitatea publică
Serviciul Audit Intern

NOTA CENTRALIZATOARE A DOCUMENTELOR DE LUCRU

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 10.10..2009
Avizat: Dumitru Daniel Data: 10.10.2009

Constatarea	***Document justificativ***	***Există***		***Auditori***
		Da	***Nu***	
Secţiunea E – Strategia şi planificarea sistemelor informatice				
Analiza proceselor-verbale ale Comisiei numite la nivelul entităţii cu responsabilităţi în dezvoltarea IT, a direcţiilor de acţiune strategice şi a deciziilor luate în vederea implementării strategiei a pus în evidenţă unele disfuncţionalităţi, legate de faptul că anumite proiecte de dezvoltare IT derulate în cadrul entităţii nu au fost supuse analizei şi evaluării comisiei.	Proces verbal 3242/23.01.2009 Proces verbal 4321/22.02.2009 …… Proces verbal 5434/22.07.2011	X		Popescu Sorin Radu George
Obiectivele specifice ale structurii funcţionale, definite în cadrul strategiei, nu au fost corelate cu posibilităţile efective ale organizaţiei, cu factorii interni şi factori externi.	Listă obiective specifice Listă obiective generale	X		Popescu Sorin Radu George
……..				
Secţiunea F- Organizarea şi funcţionarea departamentului IT				
Atribuţiile definite in sarcina salariaţilor nu sunt întotdeauna conforme şi nu asigură competenţa de realizare a activităţilor şi acţiunilor, acestea fiind definite în multe cazuri la modul general, nu indică, prin modul de formulare o acţiune, nu asigură un conţinut clar, fiind definite sub forma unei relaţii funcţionale sau având caracter de activitate.	Fişele posturilor pentru eşantionul constituit	X		Popescu Sorin Radu George
Organigrama ca document prin care se relevă grafic structura organizaţiei şi substructurile acesteia nu pune în evidenţă organizarea şi funcţionarea departamentului. Compartimentele aflate în subordinea departamentului nu sunt nominalizate în	Organigrama departamentului	X		Popescu Sorin Radu George

totalitate în cadrul organigramei şi nu este precizat nici nivelul de subordonare al departamentului în cadrul organizaţiei.				
……				
Secţiunea G - Operaţii ale sistemului informatic				
Analiza implementării subsistemelor IT, potrivit planului anual întocmit şi aprobat, a pus în evidenta faptul ca termenele stabilite pentru implementarea programelor nu sunt respectate, iar departamentele ce ar trebui să utilizeze deja noile aplicaţii IT întâmpină deficienţe în transmiterea datelor în format electronic celorlalte departamente care au nevoie de aceste informaţii şi unde funcţionează deja de programe performante.	Planul anual de dezvoltare a sistemului IT Procesele verbale privind punerea în funcţiune a aplicaţiilor	X		Popescu Sorin Radu George
……				
Secţiunea H- Securitatea informaţiilor				
Inexistenţa unui sistem de stabilire de către fiecare utilizator a parolelor şi a unui responsabil cu verificarea schimbării periodice a parolelor de acces.	Procedura privind schimbarea parolelor	X		Popescu Sorin Radu George
……				
Secţiunea H – Achiziţionarea şi testarea aplicaţiilor				
Organizarea datelor în fişierele de date prezintă următoarele disfuncţii: redundanţă mare, acces dificil la date, izolarea datelor, actualizarea datelor prin adăugare, modificare, ştergerea generează erori atunci când mai mulţi utilizatori doresc să modifice simultan aceleaşi date, dependenţa programelor, descrierea independentă a datelor în toate fişierele în care apar.	Procedura privind organizarea datelor în fişiere Fişele de intervenţie la fiecare aplicaţie	X		Popescu Sorin Radu George
……				
Secţiunea I – Elaborarea şi implementarea proiectelor IT				
Cu toate că entitatea publică a achiziţionat licenţe pentru pachetul de programe Lotus, s-au constatat că în cadrul unor departamente se folosesc programe aferente pachetului Microsoft Office fără ca pentru acestea entitatea publică să fi achiziţionat licenţe.	Lista staţiilor de lucru pe care erau instalate programe aferente Microsoft Office, fără licenţă	X		Popescu Sorin Radu George

…….				
Secţiunea K – Proiectarea şi menţinerea în funcţiune a unei reţele				
Sistemul IT este conceput astfel încât pentru accesul la fiecare subsistem IT trebuiesc folosite: nume de utilizator şi parolă diferite, în loc să se folosească acelaşi nume de utilizator şi parolă indiferent de subsistemul IT la care se conectează angajatul.	Lista staţiilor de lucru la care accesul se realizează cu aceleaşi nume de utilizator şi parolă	X		Popescu Sorin Radu George
…….				

Auditori,
Popescu Sorin
Radu George

Notă:

Revizuirea documentelor asigură că documentele de lucru sunt pregătite în mod corespunzător şi că acestea furnizează un sprijin adecvat pentru munca efectuată şi pentru dovezile adunate în timpul misiunii de audit intern.

Auditorii revăd documentele procedurale şi documentele de lucru din punct de vedere al formei şi al conţinutului, se asigură că dovezile de audit prezentate în susţinerea constatărilor sunt justificative, respectiv sunt suficiente, concludente şi relevante.

Procedura P11:	**ŞEDINŢA DE ÎNCHIDERE**

Entitatea Publică
Serviciul de Audit Intern

MINUTA ŞEDINŢEI DE ÎNCHIDERE

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 15.10..2009
Avizat: Dumitru Daniel Data: 15.10.2009

Lista participanţilor:

Numele	**Funcţia**	**Direcţia/ Serviciul**	**Nr. telefon**	**E-mail**	**Semnătura**
Dumitru Daniel	Sef serviciu	SAI			
Popescu Sorin	Auditor intern	SAI			
Radu George	Auditor intern	SAI			
Mincă Cristian	Director	Direcţia IT			
Negru Adrian	Sef serviciu	Serviciul 1 IT			
Ciobanu Vasile	Şef serviciu	Serviciul 2 IT			
Butnaru Lenuţa	Şef serviciu	Serviciul 3 IT			
Vasilescu George	Şef serviciu	Serviciul 4 IT			
Toma Eugen	Consilier	Serviciul 2 IT			
Stănescu Ioana	Consilier	Serviciul 3 IT			
Istrate Viorica	Consilier	Serviciul 4 IT			

B. Concluzii:

În cadrul şedinţei au fost prezentate obiectivele auditate şi constatările pentru fiecare obiect auditat. De asemenea, au fost discutate constatările, au fost analizate cauzele care au contribuit la realizarea disfuncţionalităţilor şi au fost comentate recomandările care urmează a fi implementate pentru eliminarea deficienţelor constatate.

In cadrul *Şedinţei de închidere*, structura auditată si-a însuşit în totalitate constatările şi recomandările formulate de echipa de auditori si, în acest sens, au prezentat *Planul de acţiune şi Calendarul de implementare al recomandărilor,* cu termenele de realizare şi persoanele responsabile, vor fi urmărite de echipa de auditori, pana la implementarea acestora.

În consecinţă, *proiectul Raportului de audit intern* devine *Raport de audit intern final* care va fi pregătit pentru aprobare şi transmitere structurii auditate. Raportul de audit intern va fi însoţit de o SINTEZA care va conţine concluziile echipei de auditori interni cu prezentarea principalelor recomandări şi opinia generala a acesteia.

Structura auditată se angajează sa completeze *Planul de acţiune şi calendarul implementării recomandărilor*, cu termenele de realizare şi persoanele responsabile cu implementare acestora, pe care îl vor discuta cu echipa de auditori.

Notă:

Şedinţa de închidere a intervenţiei la faţa locului are ca scop prezentarea opiniei auditorilor interni, a constatărilor şi recomandărilor finale, precum şi discutarea unui plan de acţiune însoţit de un calendar de implementare a recomandărilor.

În cadrul acestei şedinţe se urmăreşte ca atât constatările, cât şi recomandările, să fie uşor de înţeles, să nu permită interpretări şi să nu fie părtinitoare. Constatările trebuie să aibă la bază documente doveditoare, iar recomandările trebuie să ajute managementul entităţii auditate în luarea deciziilor manageriale în vederea eliminării deficienţelor constatate.

Entitatea Publică
Serviciul de Audit Intern

LISTA DE SUPERVIZARE A DOCUMENTELOR

Misiunea de audit: *Activitatea IT*
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/ Radu George Data: 18.10..2009
Avizat: Dumitru Daniel Data: 18.10.2009

Nr. crt.	***Lucrarea***	***Propunerea şefului structurii de audit/ supervizorului misiunii, ca urmare a revizuirii documentului***	***Răspunsul auditorilor***	***Revizuirea răspunsurilor auditorilor de către şeful structurii de audit/supervizor***
1.	Declaraţia de independenţă	Nu există incompatibilitate		De acord
2	Colectarea informaţiilor	Nu exista un centralizator al documentelor colectate şi prelucrate	Se va întocmi şi elabora documentul procedura de lucru privind documentele colectate şi prelucrate	De acord
3.	Programul de audit intern	In programul de audit nu apare obiectivul cu privire la definirea structurilor organizatorice	Programul de audit a fost refăcut, obiectivul privind definirea structurilor organizatorice a fost cuprins în program	De acord
4	Constatarea şi raportarea iregularităţilor	Nu s-a întocmit şi elaborat fisa de constatare şi raportare a iregularităţilor pentru constatarea cu privire la necalcularea taxei pentru eliberarea autorizaţiilor de construire	Se va întocmi şi elabora FCRI în acest caz	De acord
5	Nota centralizatoare a documentelor de lucru	Nu s-a întocmit şi elaborat nota centralizatoare a documentelor de lucru	Se va elabora şi întocmi şi elabora nota centralizatoare a documentelor de lucru	De acord
…. …. ….		……..	…….	……..
n	Raportul de audit	Raportul de audit nu prezintă cauzele şi consecinţele constatărilor efectuate	Raportul de audit va fi completat cu precizarea cauzelor şi consecinţelor aferente constatărilor efectuate	De acord

Supervizor,
Georgescu Cristian

Notă:

Supervizarea reprezintă activitatea de îndrumare, consiliere, supraveghere şi verificare efectuată de către supervizor asupra activităţii echipei de audit, se realizată pe tot parcursul derulării misiunii de audit intern prin semnarea documentelor întocmite.

Scopul activităţii de supervizare este asigurarea că obiectivele misiunii de audit intern au fost atinse în condiţii de calitate.

Documentele de audit elaborate (procedurale sau întocmite de auditor cu privire la constatări efectuate) trebuie supervizate pentru a se asigura că acestea vin în sprijinul raportului de audit şi că toate procedurile de audit necesare au fost efectuate.

Entitatea Publică
Serviciul de Audit Intern

PROIECT
DE RAPORT DE AUDIT INTERN

MISIUNEA DE AUDIT INTERN

ACTIVITATEA IT

BUCUREŞTI
2009

CAPITOLUL I

DATE DE IDENTIFICARE A MISIUNII DE AUDIT INTERN

Echipa de auditare - *a fost formată din:*

Popescu Sorin, auditor superior, coordonator
Radu George, auditor superior

Ordinul de efectuare a misiunii de audit - auditarea activităţilor cuprinse în Planul de audit intern pe anul 2010, s-a făcut în baza Ordinului de serviciu nr. 11/12.08.2009.

Baza legală a acţiunii de auditare*:*

Planul de audit intern pentru anul 2009, aprobat de conducerea entităţii publice;

Legea nr. 672/2002 privind auditul public intern;

OMFP nr. 38/15.01.2003 pentru aprobarea Normelor generale de privind exercitarea activităţii de audit public intern.

Normele proprii de audit public intern ale entităţii, avizate şi aprobate de conducere, privind exercitarea activităţii de audit intern în cadrul entităţii.

Durata misiunii de audit: 01.09.2009 – 20.10.2009.

Perioada auditată: 01.01.2008 - 31.08.2009

Scopul acţiunii de auditare *constă în:*

- asigurarea conducerii asupra funcţionării echipamentelor, aplicaţiilor şi programelor în concordanţă cu cerinţele stabilite;
- asigurarea aplicării corecte a măsurilor de testarea şi implementarea noilor aplicaţii, de a soluţiona problemele apărute în funcţionarea aplicaţiilor.

Obiectivele acţiunii de auditare au urmărit:

- *Strategia şi planificarea sistemelor informatice;*
- *Organizarea şi funcţionarea departamentului IT;*
- *Operaţii ale sistemului informatic;*
- *Securitatea informaţiilor;*
- *Proiectarea şi testarea programelor şi aplicaţiilor;*
- *Elaborarea şi implementarea proiectelor IT;*
- *Proiectarea şi menţinerea în funcţiune a unei reţele.*

Tipul de auditare - *audit de conformitate/regularitate.*

Tehnici de audit intern utilizate:

- verificarea se realizează în vederea asigurării validităţii, realităţii şi acurateţei înregistrărilor în contabilitate a documentelor şi a concordanţei cu legile şi regulamentele în vigoare, precum şi a eficacităţii controlului intern prin cu ajutorul următoarele *tehnici de verificare:*

a) comparaţia: pentru confirmarea identităţii unor informaţii, după obţinerea lor din două sau mai multe surse diferite;

b) examinarea: pentru detectarea erorilor şi/sau iregularităţilor;

c) recalcularea: verificarea algoritmilor de calcul şi a calculelor matematice;

d) punerea de acord: pentru realizarea procesului de potrivire a doua categorii diferite de înregistrări;

e) confirmarea: pentru solicitarea informaţiilor din mai multe surse independente cu scopul validării acestora;

f) garantarea: pentru verificarea realităţii tranzacţiilor înregistrate pornind de la examinarea înregistrărilor spre documentele justificative;

*g) urmărire*a: pentru verificarea modului în care au fost elaborate procedurile, pentru verificarea documentelor justificative spre articolul contabil în vederea verificării dacă toate operaţiunile au fost înregistrate.

- observarea fizică: constă în urmărirea unui proces sau a unei proceduri, prin care auditorul îşi formează o imagine de ansamblu asupra structurii auditate;

- interviul, notele de relaţii: se realizează de către auditorii interni prin intervievarea persoanelor auditate, implicate şi interesate şi informaţiile primite, care trebuie să fie susţinute de documente. Pentru eventualele explicaţii suplimentare se solicită note de relaţii;

***- analiza*:** constă în descompunerea unei entităţi în elemente, care pot fi izolate, identificate, cuantificate şi măsurate distinct.

Instrumentele de audit intern utilizate:

- Chestionarul de luare la cunoştinţă - CLC: pentru obţinerea unor informaţii referitoare la contextul socio-economic, organizare internă, funcţionarea entităţii/structurii auditate;

- Chestionarul de control intern - CCI: orientează auditorii interni în activitatea de identificare obiectivă a disfuncţiunilor şi cauzelor reale ale acestora. Acesta a fost utilizat pentru evaluarea instrumentelor de control existente, împreună cu alte informaţii relevante pentru audit, pe parcursul desfăşurării misiunii de audit intern;

- Listă de verificare - LV: pentru stabilirea condiţiilor de regularitate pe care trebuie să le îndeplinească fiecare domeniu auditabil. Cuprinde un set de operaţii ce trebuie parcurse de auditor pentru a analiza activităţile de control intern încorporate în proceduri, existenţa responsabilităţilor pentru efectuarea acestora şi permite stabilirea testelor de conformitate atunci când sunt semnalate diferite disfuncţionalităţi;

- Fişa de identificare şi analiză a problemelor – FIAP: întocmită pentru fiecare disfuncţionalitate constatată;

- Formularul de constatare şi raportare a iregularităţilor –FCRI: întocmit cu scopul de a informa conducerea direcţiei cu privire la iregularitatea constată.

Documente şi materiale examinate în cadrul Direcţiei IT *- verificarea la faţa locului a vizat documentaţia aferentă perioadei auditate, respectiv 01.01.2008 – 30.06.2009, care a cuprins următoarele:*

- legi şi regulamente aplicabile structurii auditate;
- strategia în domeniul IT;
- organigrama Direcţiei IT;
- Regulamentul de Organizare şi Funcţionare;
- Fişele posturilor;
- Proceduri operaţionale de lucru;
- Rapoarte de evaluare;
- Liste de achiziţii în domeniul IT;
- aplicaţii informatic;
- programe informatice achiziţionate;
- Planul privind continuitatea activităţilor, etc.

Documente şi materiale întocmite pe timpul auditării:

- documentaţia aferentă analizei riscurilor;
- tabelul puncte tari şi puncte slabe;
- tematica în detaliu a misiunii de audit intern;
- programul de audit intern;
- programul intervenţiei la faţa locului;
- liste de verificare structurate pe obiective;
- foi de lucru pentru stabilirea eşantioanelor;
- chestionare de control intern;
- teste;
- liste de control;
- fişe de identificare şi analiză a problemelor constatate - FIAP-uri;

- formulare de constatare şi raportare a iregularităţilor - FCRI-uri;
- proiectul raportul de audit intern;
- minutele şedinţelor de deschidere, de închidere şi de conciliere;
- Raportul de audit intern;
- planul de acţiune şi calendarul de implementare a recomandărilor;
- fişa de urmărire a implementărilor recomandărilor.
- foi de lucru privind descrierea activităţilor auditate;
- documente de lucru;
- note de relaţii;
- interviuri.

Organizarea Direcţiei IT

Direcţia IT a funcţionat în perioada supusă auditării cu un număr de 32 salariaţi, din care un 4 posturi de conducere – un director, şi 4 şefi de serviciu. Organizarea şi funcţionarea direcţiei se desfăşoară conform organigramei şi Regulamentului de organizare şi funcţionare.

Pentru toţi salariaţii au fost întocmite fişe ale posturilor prin care s-au stabilit relaţiile ierarhice de subordonare şi de colaborare, precum şi sarcinile de serviciu.

II. CONSTATĂRI

II. CONSTATĂRI ŞI RECOMANDĂRI

Prezentam principalele constatări, consecinţele care s-au produs sau care ar putea sa apară în perioada imediat următoare, precum şi recomandările formulate în vederea corectării disfuncţionalităţilor semnalate sau ale celor care pot să survină, diminuării riscurilor existente şi îmbunătăţirii sistemelor de management şi control intern al activităţilor auditate cu scopul facilitării atingerii obiectivelor prestabilite.

Obiectivul I.

1. STRATEGIA ŞI PLANIFICAREA SISTEMELOR INFORMATICE

1.1. Strategia IT este concordanţă cu scopurile organizaţiei

1.1.1. Strategia IT defineşte necesităţile şi priorităţile

Nerealizarea în termen a procedurilor de achiziţie şi implementare a programelor şi aplicaţiilor informatice.

Cu privire la armonizarea strategiei în domeniul IT cu strategia entităţii, s-a constatat că aceasta derivă şi este elaborată în conformitate cu direcţiile şi principiile de dezvoltare ale entităţii, contribuie la dezvoltarea şi eficientizarea activităţilor entităţii şi prin implementare se urmăreşte realizarea unui sistem informatic integrat, care să asigure integrarea tuturor informaţiilor şi datelor la nivelul entităţii, respectiv juridice, economice, comerciale, tehnice, financiar-contabile, de personal, sociale şi patrimoniale.

Din analiza atribuţiilor stabilite Comisiei numită la nivelul entităţii cu responsabilităţi în domeniul dezvoltării IT, s-a constatat că acestea sunt, în general, de natură metodologică, respectiv planificarea şi elaborarea strategiei în domeniul IT şi armonizarea acesteia cu strategia şi mandatul entităţii. Totuşi, această comisie are şi atribuţii cu privire la monitorizarea activităţilor privind implementarea strategiei, însă analiza realizării acestor activităţi este rezumată doar la raportările periodice realizate de departamentul IT, cu privire la stadiul implementării proiectelor IT. Limitarea exercitării acestor atribuţii, doar la analiza raportărilor efectuate de departamentul IT, fără o evaluare fizică, din partea comisiei, a modului de implementare a programelor informatice, conduce la formularea unor constatări şi concluzii insuficiente, care au influenţă în decizia managerială şi dezvoltarea strategică.

Analiza proceselor-verbale ale Comisiei numite la nivelul entităţii cu responsabilităţi în dezvoltarea IT, a direcţiilor de acţiune strategice şi a deciziilor luate în vederea implementării strategiei a pus în evidenţă

unele disfuncţionalităţi, legate de faptul că anumite proiecte de dezvoltare IT derulate în cadrul entităţii nu au fost supuse analizei şi evaluării comisiei. Astfel, în cursul anului 2009, discuţiile în cadrul comisiei au privit, în general, analiza progreselor proiectelor IT stabilite şi aprobate la nivelul entităţii, însă potrivit proceselor verbale întocmite în urma şedinţelor, a rezultat că discuţiile s-au derulat doar cu privire la proiectele pentru care au fost înaintate de către departamentul IT, rapoarte privind stadiul implementării, astfel că propunerile formulate de comisie cu privire la dezvoltarea IT, inclusiv cu privire la asigurarea resursele financiare, au fost legate doar de aceste aspecte.

În urma examinării şi analizelor efectuate s-a constatat că anumite proiecte nu au fost implementate sau sunt întârzieri în implementarea acestora, respectiv:

a) aplicaţia privind evidenţa documentelor intrate ieşite din cadrul organizaţiei, inclusiv stadiul soluţionării lor, a fost aprobată a fi implementată, inclusiv au fost asigurate resursele financiare încă din cursul anului anterior, dar până în prezent nu s-a realizat nici o procedură legată de stabilire a condiţiilor tehnice ale aplicaţiei, demararea acţiunilor de realizare a caietului de sarcini, sau a procedurilor de realizare a achiziţiei, cu toate că prin buget au fost alocate fondurile necesare.

Din discuţiile purtate cu responsabilii IT în domeniul dezvoltării şi informatizării entităţii, a rezultat că acest program informatic nu a fost demarat, deoarece la nivelul departamentului IT nu existau specialişti în testarea şi implementarea programului, iar fondurile aprobate permiteau doar achiziţia aplicaţiei.

În condiţiile în care atribuţiile comisiei permiteau şi o evaluare fizică a modului de implementare a proiectelor, greutăţile întâmpinate se puteau cunoaşte şi se puteau găsi soluţiile necesare, respectiv, în acest caz a condiţiilor de pregătire a personalului în vederea utilizării programului informatic.

b) pentru proiectul „Implementarea unei infrastructuri IT care să asigure integrarea datelor la nivelul organizaţiei", a fost raportat stadiul de implementare la comisie, însă nu şi termenele de realizare. În urma evaluării s-a constatat că au fost demarate procedurile pentru achiziţia acestuia, însă până în prezent acestea s-au limitat la studiul pieţei şi alocarea banilor în cadrul bugetului. Proiectul se află în întârziere şi nu va putea fi realizat în timp util. Aceasta va avea consecinţe negative în implementarea altor aplicaţii, care au legătură cu acesta, în acest sens va trebui decalat termenul de începere a procedurilor privind implementarea proiectului „Crearea unei structuri IT care să permită urmărirea circuitului unui document, stadiul de realizare şi persoanele care au intervenit asupra acestuia, autorizarea pe niveluri ierarhice prestabilite". Întârzierea implementării acestui program a determinat decalarea termenul planificat a obiectivului strategic „Modernizarea infrastructurii IT din cadrul entităţii".

Pentru deficienţele constatate s-a recomanda reanalizarea atribuţiilor Comisiei de planificare strategică în domeniul IT şi redefinirea acestora astfel încât să poată realiza şi monitorizarea implementării proiectelor informatice şi informarea periodică a conducerii asupra realizării acestora.

Referitor la nerespectarea procedurii de elaborare şi fundamentare a strategiei şi a politicilor de dezvoltare s-a constat, din analiza sistemului de fundamentare a strategiei, rezultă că s-au realizat următoarele etape:

*e) stabilirea rolului*ui IT în cadrul organizaţiei, fiind identificată şi definită importanţa acesteia;

f) definirea misiunii structurii funcţionale în concordanţă cu obiectivele strategice şi direcţiile de acţiune stabilite la nivelul organizaţiei;

g) identificarea şi provenienţa resurselor financiare, materiale şi umane necesare aplicării şi implementării strategiei;

h) implementarea strategiei, fiind fixate termenele necesare atingerii obiectivelor în raport cu care se urmăresc asigurarea şi repartizarea resurselor precum şi concentrarea eforturilor umane şi materiale.

Tot din analiză rezultă că la elaborarea strategiei, la nivelul structurii funcţionale, nu s-au avut în vedere următoarelor etape:

d) Evaluarea situaţiei actuale pe baza analizei diagnostic, respectiv orientarea activităţii pentru o anumită perioadă, prin strategie, presupune ca, în prealabil, să fie cunoscută situaţia actuală, pe baza unei analize diagnostic, pentru a avea o imagine cât mai completă asupra domeniului de activitate al organizaţiei. Analiza diagnostic trebuia elaborată în baza unor studii privind potenţialului intern, folosind metode statistice, matematice, analiza pe bază de bilanţ etc. care să surprindă evoluţia proceselor şi fenomenelor specifice domeniului de activitate. Informaţiile de intrare nu fac referire la aspecte cum sunt: dimensiunea structurii funcţionale, resursele umane, înzestrarea tehnică, managementul utilizat;

e) Identificarea punctelor tari şi a punctelor slabe ale entităţii în vederea determinării ameninţărilor şi oportunităţilor cu care se confruntă entitatea;

f) *Fundamentarea variantelor strategice* – obiectivele strategice stabilite pentru IT nu au fost corelate cu posibilităţile efective ale organizaţiei, cu factorii interni şi factori externi. Realizarea strategiei

implică fixarea şi respectarea termenelor necesare atingerii obiectivelor în raport cu care se urmăresc asigurarea şi repartizarea resurselor precum şi concentrarea eforturilor umane şi materiale. Totodată, trebuie avuta în vedere compatibilitatea variantei strategice elaborata teoretic cu realitatea şi modul în care s-a reuşit surprinderea acţiunii factorilor de influenta.

Strategia a fost elaborată fără a se evalua situata actuala, pe baza unei analize diagnostic, astfel încât să putem avea o imagine cât mai completa asupra organizaţiei, asupra rezultatelor pe care şi-a propus să le obţină, a potenţialului său financiar, cât şi a importanţei în cadrul realizării programului de guvernare.

Totodată nu au fost identificate nici punctele tari şi punctele slabe în vederea determinării ameninţărilor şi oportunităţilor cu care se confruntă entitatea.

De asemenea, obiectivele strategice ale structurii funcţionale, definite în cadrul strategiei, nu au fost corelate cu posibilităţile efective ale organizaţiei, cu factorii interni şi factori externi. Realizarea strategiei implica fixarea şi respectarea termenelor necesare atingerii obiectivelor în raport cu care se urmăresc asigurarea şi repartizarea resurselor precum şi concentrarea eforturilor umane şi materiale.

Pentru deficienţele constatate s-a recomandat pregătirea profesională anticipată a personalului implicat în elaborarea strategiei, de către managementul responsabil cu aceasta. Reanalizarea strategiei definite la nivelul structurii funcţionale în conformitate cu procedura operaţională aprobată şi actualizarea acesteia astfel încât implementarea sa să contribuie la realizarea unui management modern in domeniul de activitate şi la atingerea obiectivelor strategice ale organizaţiei.

În acelaşi timp s-a mai recomandat îmbunătăţirea procedurilor operaţionale de lucru privind sistemul de fundamentare a necesarului de resurse pentru elaborarea strategiei.

Referitor la faptul că obiectivelor strategice nu asigură acoperirea domeniului de activitate al structurii funcţionale şi nu contribuie la asigurarea realizării mandatului organizaţiei s-a constat că acestea reprezintă exprimările cantitative şi calitative ale scopului pentru care există şi funcţionează organizaţia.

În acelaşi timp din analiza modului de definire şi stabilire a obiectivelor strategice s-a constatat că acestea nu întrunesc următoarele caracteristici definitorii:

- nu sunt realiste şi nu au fost luate în calcul capacităţile şi posibilităţile efective de realizare de care dispune organizaţia în condiţiile actuale;
- nu sunt mobilizatoare şi nu implică eforturi de autodepăşire din partea salariaţilor;
- nu sunt comprehensibile şi nu sunt formulate şi prezentate într-o manieră care să permită înţelegerea conţinutului lor de către salariaţi;
- nu sunt antrenante şi nu asigură o abordare sistemică a intereselor organizaţiei şi componentelor sale organizatorice într-o viziune optimizantă pe termen mediu şi lung.

Aceşti factori trebuie să se regăsească la orice obiectiv strategic, indiferent de natura sa (economică, tehnică), deoarece aceste obiective reprezintă punctul de plecare în conturarea unui sistem unitar de obiective ce vizează toate componentele procesuale şi structurale ale organizaţiei.

Dimensiunea şi natura obiectivelor strategice generează direct sau indirect modalităţi şi opţiuni de realizare care condiţionează decisiv conţinutul şi funcţionalitatea strategiei, ceea ce impune ca la implementarea lor să se ia în considerare principalele variabile exogene ce influenţează comportamentul economic şi managerial al organizaţiei, cât şi capacitatea acesteia de adaptare la schimbare.

La fundamentarea necesarului de resurse solicitate de atingerea obiectivelor nu s-a realizat o dimensionare corectă a fondurilor de investiţii şi a mijloacelor circulante pe baza unor indicatori specifici, cantitativi şi calitativi.

De asemenea, nu în toate situaţiile, personalului i-au fost asigurate condiţiile de instruire pentru dobândirea aptitudinilor necesare realizării eficiente a obiectivelor individuale pentru a contribui astfel, în condiţii de performanţă, la obţinerea impactului definit de obiectivele strategice.

Pentru deficienţele constatate s-a recomandat evaluarea performanţelor actuale ale sistemului de organizare şi conducere a activităţilor desfăşurate în cadrul structurii funcţionale, ţinând cont de influenţa factorilor de mediu, interni şi externi, în vederea redefinirii obiectivelor strategice. Implicarea managementului pentru ca obiectivele strategice redefinite să întrunească caracteristicile de a fi realiste, mobilizatoare, stimulative şi să poată fi înţelese de salariaţi, stabilite de metodologie.

Totodată, la redefinirea acestora se va urmări asigurarea resurselor necesare implementării lor.

1.2. Planurile IT se adresează întregii organizaţii

1.2.1. Planurile IT ajută la îndeplinirea misiunii organizaţiei

Resursele nu sunt fundamentate corect în vederea implementării planului anual de activitate.

Din analiză s-a constatat că eforturile pentru elaborarea planului anual de activitate implică alocarea de fonduri şi resurse ridicate din partea organizaţiei care, în cele mai multe din cazuri, nu au ca referinţă atingerea scopului fundamental al acesteia.

În acelaşi timp, activităţile considerate prioritare ale planului anual nu au fost realizate sau implementate în totalitate, în mod corespunzător, deoarece nu au fost reanalizate şi repartizate atribuţiile în cadrul compartimentelor în corelaţie cu noile obiective şi activităţi stabilite în cadrul planului. Aceasta a însemnat că, în unele cazuri, obiectivele şi activităţile deşi erau cunoscute de personal, acesta nu avea competenţa necesară, în special a celor care erau realizate în colaborare cu alte structuri funcţionale, ceea ce a necesitat solicitarea unor competenţe pentru realizarea acestora, proces care a îngreunat implementarea obiectivelor şi realizarea activităţilor.

În alte cazuri, activităţile nu au fost comunicate salariaţilor, respectiv obiectivele individuale au rămas aceleaşi, în condiţiile în care obiectivele cuprinse în planul compartimentului au fost cu totul altele. Aceasta a însemnat stabilirea măsurilor în cursul anului, instruirea, sub diferite forme, a personalului pentru înţelegerea acestora şi stabilirea priorităţilor de implementare, ceea ce a condus la întârzieri în atingerea unor obiective ale planului.

Nevoia de îmbunătăţire a nivelului de competenţă în raport cu progresele tehnico-informaţionale şi organizatorice, pentru creşterea eficienţei şi reducerea costurilor, a presupus definirea în cadrul planului anual a unor asemenea obiective şi activităţi, însă pentru implementarea acestora nu a fost corelat necesarul de mijloace şi echipamente cu necesităţile pentru atingerea obiectivelor planului.

În cadrul planului reducerea costurilor a fost definită şi prin reducerea personalului, prin care s-au pierdut o serie de competenţe care, din motive financiare, nu au fost înlocuite, prin dezvoltarea altor angajaţi, ceea ce a condus la realizarea activităţilor, dar nu au fost atinse condiţiile de performanţă stabilite.

Monitorizarea resursele financiare utilizate în derulare obiectivelor planului anual a fost de multe ori deficitară, ceea ce a contribuit la realizarea de costuri suplimentare faţă de cele planificate pentru implementarea obiectivelor stabilite.

În cadrul entităţii nu a fost comunicată eficient şi nu a fost conştientizată nevoia de cunoaştere a normelor, legislaţiei şi metodologiei în domeniile de activitate, a diferitelor culturi din cadrul organizaţiei, importanţa obiectivelor stabilite spre îndeplinire şi modul cum acestea contribuie la atingerea obiectivelor generale şi a obiectivelor strategice, şi înţelegerea comportamentului competitiv ca un sistem în care oamenii şi resursele interacţionează continuu.

Activităţile considerate prioritare ale planului anual nu au fost realizate sau implementate corespunzător deoarece nu s-au reanalizat şi repartizat atribuţiile compartimentelor pentru a asigura competenţa necesară realizării obiectivelor şi activităţilor stabilite în cadrul planului.

De asemenea, nu au fost stabilite şi comunicate salariaţilor obiectivele individuale care derivă din noile obiective stabilite în cadrul planului de activitate şi care se aflau în competenţa compartimentului funcţional.

Definirea în cadrul planului anual a obiectivelor şi activităţilor s-a realizat fără să se asigure: nevoia de îmbunătăţire a nivelului de competenţă în raport cu progresele tehnico-informaţionale şi organizatorice;creşterea eficienţei şi reducerea costurilor; corelarea necesarul de echipamente cu necesităţile de atingere a obiectivelor planului.

Pentru deficientele constatate s-a recomandat dezvoltarea unui sistem de instruire şi pregătire a salariaţilor astfel încât metodologia specifică domeniului de activitate, normativă şi procedurală, să fie aplicată corespunzător pentru dezvoltarea şi implementarea planurilor anuale. În baza planurilor elaborate să se identifice toate atribuţiile necesare pentru atingerea obiectivelor stabilite, iar acestea să fie repartizate corespunzător în cadrul compartimentelor.

Totodată, s-a mai recomandat promovarea dezvoltării resurselor umane pentru a obţine competenţele necesare creşterii economice în condiţiile în care au loc reduceri de personal, precum şi evaluarea cuprinzătoare a resurselor (financiare, instituţionale, programe, personal) necesare implementării planurilor anuale de activitate şi monitorizarea eficientă pentru a se asigura încadrarea în limitele stabilite.

1.2.2. Planurile IT oferă asigurare cu privire la faptul că resursele IT sunt alocate în concordanţă cu necesităţile

Unele departamente din cadrul entităţii nu dispun de subsisteme IT specifice activităţilor care se desfăşoară în cadrul acestora.

Din analiză s-a constatat că în cadrul entităţii publice există structuri nou-înfiinţate ca urmare a recomandărilor Comisiei Europene şi a schimbărilor legislative, care nu au notificat departamentul IT în privinţa nevoilor lor de aplicaţii informatice specifice. În acelaşi timp, s-au constatat şi departamente nou înfiinţate care şi-au exprimat nevoile pentru realizarea subsistemelor IT specifice activităţii lor, dar care nu au beneficiat de implementarea acestora, conform planificării, datorită întârzierilor în realizarea achiziţiilor.

Pentru deficienţele constatate s-a recomandat coroborarea atribuţiilor prezentate prin proceduri cu cele stabilite prin fişele posturilor şi inventarierea stadiului implementării subsistemelor IT la nivelul departamentelor entităţii publice şi stabilirea necesităţilor IT care trebuie incluse în strategia IT.

1.3. Obiectivele IT îndeplinesc obiectivele organizaţiei

1.3.1. Strategia IT este concordantă cu scopurile organizaţiei

……

1.4. Comitetul IT determină strategia IT

1.4.1. Comitetul IT transpune strategia în planuri pe termen scurt şi pe termen mediu

…….

1.4.2. Comitetul IT stabileşte prioritătile proiectelor între dezvoltarea sistemelor şi activităţilor realizate

…….

1.5. Organizarea IT corespunde necesităţilor organizaţiei

1.5.1. Organizarea adecvată a funcţiei IT

……

1.5.2. Adecvarea practicilor şi procedurilor IT la procesele existente

……..

1.6. Elaborarea strategiei IT corespunde strategiei entităţii

1.6.1. Dotarea actuală cu tehnică de calcul a stat la baza strategiei IT

……..

2. ORGANIYAREA ŞI FUNC'IONAREA DEPARTAMENTULUI IT

2.1. Definirea atribuţiilor şi activităţilor

2.1.1. Definirea atribuţiilor şi responsabilităţilor în cadrul Departamentului IT

Atribuţiile stabilite pentru posturile din cadrul Departamentului IT nu asigură întotdeauna aria de competenţă privind realizarea activităţilor şi acţiunilor repartizate.

Atribuţiile definite in sarcina salariaţilor nu sunt întotdeauna conforme şi nu asigură competenţa de realizare a activităţilor şi acţiunilor, acestea fiind definite în multe cazuri la modul general, nu indică, prin modul de formulare o acţiune, nu asigură un conţinut clar, fiind definite sub forma unei relaţii funcţionale sau având caracter de activitate.

În acest sens s-a recomandat conştientizarea managementului responsabil cu procesul de stabilire şi definire a atribuţiilor prin informări şi consilieri pentru clarificarea modalităţilor practice de definire a

unei atribuţii sau unui set de atribuţii pentru asigurarea ariei de competenţă necesară pentru realizarea activităţilor.

2.1.2. Definirea activităţilor în cadrul structurii organizatorice

Activităţile nu sunt definite omogen în cadrul structurii funcţionale, iar stabilirea complexităţii acestora nu se realizează în funcţie de nivelurile de calificare ale posturilor existente.

La definirea activităţilor se are în vedere complexitatea acestora, respectiv gradul de diferenţiere a muncii pe orizontală şi pe verticală. Diferenţierea pe orizontală constă în numărul de activităţi (specializări) şi de subunităţi funcţionale (birouri, servicii). Diferenţierea pe verticală se referă la numărul de niveluri ierarhice de-a lungul cărora se exercită autoritatea în organizaţie.

Analiza conţinutului şi modului de definire a activităţilor necesare pentru realizarea fiecărui obiectiv specific a pus în evidenţă următoarele:

– unele activităţi sunt definite sub forma unor relaţii de colaborare care fie nu indică acţiuni concrete de realizare a acestora, fie indică o acţiune comună de realizare;

– altele sunt definite sub forma unor relaţii de colaborare, în condiţiile în care sunt exercitate acţiuni concrete de realizare şi pentru care există rezultate aşteptate stabilite;

– nu sunt identificate toate activităţile care contribuie la realizarea obiectivelor specifice şi care asigură conformitatea cu reglementările legale.

Prin modul de organizare a activităţilor structurilor organizatorice ale direcţiei nu se asigură evitarea dublării acţiunilor, respectiv există activităţi identice sau similare, desfăşurate de mai multe departamente şi probleme semnificative de suprapunere şi de coordonare.

De asemenea, pentru realizarea unor activităţi, nu se respectă principiul convergenţei în definirea şi stabilirea conţinutului activităţilor care sunt necesare pentru realizarea unui obiectiv.

Pentru reglementarea deficienţelor constatate s-a recomandat realizarea unei analize riguroase a sarcinilor şi responsabilităţilor fiecărui angajat, care să stea la baza oricărei iniţiative de organizare a activităţii. Constituirea unei echipe, pe baza deciziei managementului general, care să analizeze şi să redefinească activităţile şi acţiunile realizate în cadrul compartimentelor şi serviciilor, astfel încât să se asigure că obiectivele vor fi realizate în totalitate.

La stabilirea obiectivelor se va urmări dacă sunt ataşate toate activităţile necesare obţinerii rezultatelor stabilite, realizate efectiv în cadrul compartimentului, formulate ca acţiuni concrete.

2.2. Stabilirea structurii organizatorice

2.2.1. Organizarea funcţională a Departamentului IT

Organigrama ca document prin care se relevă grafic structura organizaţiei şi substructurile acesteia nu pune în evidenţă organizarea şi funcţionarea departamentului. Compartimentele aflate în subordinea departamentului nu sunt nominalizate în totalitate în cadrul organigramei şi nu este precizat nici nivelul de subordonare al departamentului în cadrul organizaţiei.

Organigrama nu furnizează o înţelegere a raporturilor de subordonare şi de evitare a suprapunerilor de competenţe. Astfel, cu privire la raporturile de subordonare, potrivit organigramei, Serviciul Programare este organizat sub forma unui compartiment care se află în directa subordonare a directorului general adjunct al departamentului, dar în realitate acest compartiment este organizat la nivel de serviciu şi subordonat directorul general. Postul de director general adjunct a fost desfiinţat în anul 2008 urmare a reorganizărilor efectuate.

Definirea relaţiilor ierarhice aşa cum a fost precizat mai sus, nu asigură o integrare corespunzătoare a departamentului în structura organizatorică a organizaţiei şi nu se asigură operativitatea fluxului de informaţii şi date între structurile implicate în fluxul tehnologic al activităţilor.

În structura organizatorică a departamentului, definită în cadrul organigramei, nu se precizează în cadrul serviciilor numărul de posturi şi responsabilii structurilor funcţionale corespunzător fiecărui nivel ierarhic şi/sau cine coordonează aceste servicii şi compartimente, ceea ce nu permite identificarea nivelurilor şi relaţiilor ierarhice.

Pentru remedierea deficienţelor constatate s-a recomandat analiza actului normativ de organizare şi funcţionare a organizaţiei şi urmărirea atribuţiilor definite departamentului astfel încât să acopere în totalitate activităţile desfăşurate.

Totodată, din evaluare s-a mai constat că persoanele responsabilizate în posturile de conducere nu au coordonat în nici un fel activităţile care erau realizate zilnic de către salariaţi, nu au îndrumat în nici un fel salariaţii cu privire la modul în care în care să realizeze activităţile şi nici nu au realizat o monitorizare cu privire la modul de realizare a acestora. Salariaţii, în baza sarcinilor stabilite prin fişa postului, au realizat activităţile în funcţie de cunoştinţele şi aptitudinile pe care le deţineau.

Examinarea fişelor posturilor pentru posturile de execuţie ocupate de persoanele care au fost numite cu delegaţie în posturi de conducere s-a constatat că acestea nu prevedeau nici o aptitudine managerială.

La nivelul celor două servicii în această perioadă nu a fost luată nici o decizie cu privire la îmbunătăţirea activităţilor sau la dezvoltarea acestora.

Pentru aceste nereguli s-a recomandat desfăşurarea procesului de selecţie şi recrutarea în vederea ocupării posturilor de conducere existente la nivelul departamentului IT. În acelaşi timp se va urmări dacă persoanele selectate deţin abilităţile şi aptitudinile manageriale necesare realizării activităţilor specifice celor două servicii şi dacă au pregătirea de bază, de nivel superior, în domeniul IT.

2.2.2. Examinarea sistemului de gestionare a riscurilor generale la nivelul Departamentului IT

Din analiză s-a constatat că riscurile nu sunt identificate şi gestionate la nivelul departamentului şi nu este condus Registrul riscurilor cuprinzând riscurile potenţiale şi istoricul acestora, precum şi instrumentele de control intern implementate pentru limitarea acestora.

Pentru această deficienţă s-a recomandat elaborarea mecanismelor procedurale şi metodologice privind identificarea riscurilor şi gestionarea acestora, evaluarea riscurilor identificate şi diferenţierea acestora în riscuri inerente şi riscuri acceptabile, precum şi implementarea de instrumente de control pentru riscurile inerente, astfel încât manifestarea acestora să fie limitată şi nivelul acestora să devină unul acceptabil.

Sistemul de control intern definit la nivelul organizaţiei nu cuprinde toate activităţile de control ce trebuie alocate în vederea atingerii obiectivelor.

Din analiza sistemului de control intern instituit la nivelul departamentului IT a rezultat că unele activităţi de control relevante nu au fost cuprinse în politicile şi procedurile de control instituite, astfel:

- revizuiri ale performanţei - aceste activităţi de control trebuie să includă revizuiri şi analize ale performanţei efective în comparaţie cu bugetele, previziunile şi performanţa perioadelor precedente;
- procesarea informaţiilor – acestea trebuie să includă cele două grupări de activităţi de control ale sistemelor informaţionale, respectiv controalele asupra aplicaţiilor individuale şi controalele generale asupra tehnologiei informaţiei, care sunt de fapt politici şi proceduri care se referă la mai multe aplicaţii şi contribuie la asigurarea funcţionării adecvate continue a sistemelor informaţionale.

Anumite activităţi de control care nu sunt de rutină şi care depind de existenţa unor politici adecvate stabilite de conducere sau de cei însărcinaţi cu guvernanţa nu au o aprobare de la aceste niveluri şi nici nu au fost delegate în responsabilitatea unor posturi inferioare.

Pentru remedierea acestor deficienţe s-a constatat stabilirea controalelor interne aferente riscurilor identificate şi determinarea gradului de funcţionalitate al acestora şi proiectarea de instrumente sau măsuri de introducere de controale interne, fie individuale, fie în combinaţie cu alte controale, capabile să prevină, detecteze şi să corecteze în mod eficient denaturările semnificative.

În acelaşi timp din analiza efectuată a mai rezultat că la nivelul departamentului nu este organizat şi nu se conduce registrul riscurilor. Riscurile cu care se confruntă organizaţia nu sunt identificate şi nu sunt monitorizate în vederea stăpânirii şi menţinerii lor la un nivel acceptabil.

Pentru soluţionarea acestei deficienţe s-a recomandat instituirea şi conducerea Registrului riscurilor la nivelul organizaţiei.

2.3. Stabilirea responsabilităţilor

2.3.1. Definirea sarcinilor prin fişa postului

Studiile de specialitate aferente unui post sunt definite în cadrul fişei postului fără a se ţine cont de scopul postului şi cunoştinţele de bază necesare pentru realizarea atribuţiilor alocate acestuia. Din analiza fişelor posturilor s-a constatat că la concursul organizat pentru ocuparea postului respectiv poate participa orice persoană care are o diplomă, deoarece nu se specifică tipul de studii şi nivelul acestora, respectiv în

domeniul IT, studii superioare de lungă durată absolvite cu diplomă de licenţă etc.

La stabilirea sarcinilor în fişele posturilor nu se urmăreşte asigurarea unui echilibru între sarcinile şi competenţele titularului postului. Din analiza eşantionului selectat a rezultat că pentru posturile cu un nivel al studiilor medii sunt alocate aceleaşi atribuţii şi responsabilităţi ca şi pentru posturile cu un nivel al studiilor superiore. Acestea creează probleme în gestionarea aplicaţiilor şi programelor, deoarece persoanelor încadrate în cadrul departamentului pe studii medii le-au fost date în responsabilitate întreţinerea de aplicaţii şi programe complexe şi chiar realizarea de astfel de aplicaţii pentru organizaţie, care necesită cunoştinţe IT de nivel superior şi chiar anumite specializări.

Pentru aceasta s-a recomandat analiza sarcinilor şi atribuţiilor definite în fişele posturilor şi stabilirea acestora în funcţie de caracteristicile postului, respectiv nivelul postului şi urmărirea definirii aceluiaşi gen de sarcini şi atribuţii numai dacă posturile sunt de acelaşi nivel.

Totodată, atribuţiile definite în sarcina compartimentelor funcţionale nu sunt întotdeauna conforme şi nu asigură competenţa de realizare a activităţilor şi acţiunilor, acestea fiind definite în multe cazuri la modul general, nu indică, prin modul de formulare, o acţiune, nu asigura un conţinut clar, fiind sub forma unei relaţii funcţionale sau având caracter de activitate sau sarcină.

Nu sunt definite în cadrul ROF-ului la capitolul privind departamentul IT relaţiile cu celelalte structuri funcţionale cu care are sau ar trebui să aibă relaţii funcţionale, respectiv nu este definită relaţia funcţională care reglementează asigurarea conformităţii informaţiilor cu privire la asistarea utilizatorilor în realizarea activităţilor de introducere a datelor şi informaţiilor în cadrul aplicaţiilor şi programelor derulate la nivelul celorlalte departamente funcţionale din cadrul organizaţiei, precum şi cu privire la asistarea în utilizarea echipamentelor din dotare.

Totodată, nu sunt prezentate relaţiile ierarhice între posturile de conducere şi posturile de execuţie, ci numai relaţia ierarhică între posturile de conducere situate la niveluri ierarhice diferite din cadrul departamentului IT.

În vederea remedierii acestor deficienţe s-a recomandat identificarea şi definirea corectă în cadrul documentului de organizare şi funcţionare, a atribuţiilor specifice departamentului, a relaţiilor funcţionale pe care compartimentul la are cu alte structuri funcţionale din cadrul organizaţiei.

3. OPERAŢII ALE SISTEMULUI INFORMATIC

3.1. Managementul operaţiunilor

3.1.1. Performanţa, capacitatea şi disponibilitatea sistemelor informatice este monitorizată de administratori

Existenţa unor controale interne slabe privind managementul operaţiunilor IT, reflectate în disfuncţii legate de gestionarea acestora, astfel:

- în urma analizei modului de alocare şi utilizare efectivă a resurselor IT disponibile, echipa de auditori a constatat că unele departamente dispun de resurse insuficiente (departamentul IT), în timp ce altele dispun de resurse excedentare (Direcţia Generală de Investiţii, Achiziţii Publice şi Servicii Interne), fiind utilizate în proporţie de max. 10-15%.
- echipa de auditori a constatat că listele generate în urma prelucrărilor pe un anumit computer puteau fi vizualizate şi modificate de pe toate celelalte computere din reţea, accesul la ele nefiind restricţionat.
- în urma inventarierii intervenţiilor efectuate asupra computerelor, imprimantelor şi copiatoarelor aflate în cadrul biroului Multiplicare, s-a constatat că procedurile privind mentenanţa nu au fost realizate cu respectarea specificaţiilor producătorului, de către personal autorizat, fapt ce a condus, în majoritatea cazurilor, la pierderea garanţiei, dar a fost afectată şi performanţa echipamentelor respective.
- analizând modul de soluţionare a unui număr de 6 probleme de ordin tehnic apărute în cadrul proceselor, echipa de auditori a constatat că au fost efectuate intervenţii punctuale din partea personalului specializat din cadrul departamentului IT al entităţii, urmărindu-se strict remedierea respectivelor probleme şi fără a se avea în vedere etapele premergătoare apariţiei problemei, cauzele şi modul de propagare etc.
- Analizând modul de efectuare a verificărilor asupra prelucrărilor, implementării funcţiilor şi programelor, asupra modului de iniţiere a unor proceduri sau a timpului de execuţie, echipa de auditori a constatat că o anumită parte din aceste verificări se realizează manual.

Pentru deficienţele constatate s-a recomandat următoarele:

- implementarea unei aplicaţii care să monitorizeze alocarea şi utilizarea resurselor în funcţie de gradul de complexitate al operaţiilor efectuate. Urmărirea în permanenţă a echilibrului între necesităţile IT şi resursele alocate acestor scopuri.

- mediile sau locaţiile de stocare să fie protejate împotriva deteriorării sau accesului neautorizat.

- procedurile de mentenanţă a echipamentelor să fie realizate corect şi la intervale de timp stabilite în funcţie de specificul fiecărei componente, numai de către personal autorizat în acest sens.

- constituirea în cadrul departamentului IT a unui colectiv specializat în raportarea şi rezolvarea operativă a problemelor de ordin tehnic (Help Desk), care să asigure şi acordarea suportului tehnic de specialitate către utilizatori, fie prin linii telefonice dedicate, fie prin e-mail sau deplasări ale echipelor specializate.

- elaborarea şi implementarea unor programe care să automatizeze pe cât posibil verificările efectuate asupra operaţiilor informatice.

3.1.2. Responsabilitatea pentru supravegherea sarcinilor pe seturi de programe revine administratorilor

……

3.1.3. Elaborarea planului anual de activitate

……..

3.2. Managementul problemelor

3.2.1. Programele antivirus asigură protecţia aplicaţiilor

Din analiză s-a constatat neaplicarea în mod unitar a politicii de securitate IT, care a condus la infectarea cu viruşi a unor staţii de lucru din sistemul IT al entităţii publice. Astfel, echipa de auditori a verificat 5 de staţii de lucru, selectate în mod aleator, din cadrul tuturor departamentelor şi a constatat că în 2 departamente din cadrul entităţii publice configuraţia programului anti-virus pentru un număr de doua calculatoare a fost modificată pentru a întrerupe monitorizarea întregii activităţi şi verificarea e-mail-ului şi, în special, a fişierelor anexate. Acest lucru s-a realizat la cererea conducătorului departamentului, deoarece se considera că programul anti-virus are un efect negativ asupra performanţei sistemului. Urmare acestei constatări, am verificat respectivele staţii de lucru pentru a descoperi prezenţa viruşilor şi am descoperit că toate erau infectate cu viruşi.

Pentru deficienţele constatate s-a recomandat constituirea unor echipe pentru efectuarea de verificări anti-virus la nivelul tuturor staţiilor de lucru din cadrul entităţii publice, configurarea corecta în cazurile în care aceste programe au fost dezactivate, stabilirea de responsabilităţi în cazul în care acestea sunt dezactivate şi produc disfuncţii în cadrul organizaţiei.

3.2.2. Implementarea subsistemelor IT

Din analiza efectuată a rezultat că, subsistemele IT nu au fost realizate la termenele stabilite. Astfel, analiza implementării subsistemelor IT, potrivit planului anual întocmit şi aprobat, a pus în evidenta faptul ca termenele stabilite pentru implementarea programelor nu sunt respectate, iar departamentele ce ar trebui să utilizeze deja noile aplicaţii IT întâmpină deficienţe în transmiterea datelor în format electronic celorlalte departamente care au nevoie de aceste informaţii şi unde funcţionează deja de programe performante.

Resursele financiare alocate pentru implementarea acestor aplicaţii în cadrul programelor deja existente au fost utilizate pentru finalizarea unor aplicaţii şi programe deja începute şi nefinalizate.

Întârzieri în realizarea activităţilor planificate atât în cadrul departamentului IT cât şi în cadrul altor departamente, deoarece datele şi informaţiile sunt reluate şi introduse manual.

Pentru deficienţele constatate s-a recomandat analiza tuturor aplicaţiilor şi programelor începute şi nefinalizate, identificarea resurselor financiare necesare pentru finalizarea acestora, stabilirea de termene de finalizare şi urmărirea respectării acestora. Noile aplicaţii şi programe vor fi aprobate şi achiziţionate numai dacă sunt compatibile cu cele deja implementate sau aflate în faza de implementare şi numai dacă exista resursele necesare aprobate prin buget.

3.3. Funcţionalitatea Departamentului IT

3.3.1. Organizarea funcţională a Departamentului IT

…….

3.3.2. Asigurarea caracterului secret al datelor

…….

3.4. Mentenanţa echipamentelor

3.4.1. Întreţinerea calculatorului şi a echipamentelor

……

3.4.2. Instalarea şi configurarea calculatorului

…….

3.5. Utilizarea echipamentelor

3.5.1. Realizarea eficientă a operaţiilor în cadrul Departamentului IT

…….

3.5.2. Administrarea eficientă a aplicaţiilor şi programelor

…….

3.5.3. Evaluarea problemelor şi soluţionarea acestora

Din evaluare, auditorii interni au mai constatat că nu există un sistem de controale generale care să fie avute în vedere în cadrul procesului de proiectare, realizare, testare şi implementare a tuturor subsistemelor IT ce rulează pe echipamentele entităţii publice, astfel:

- Controlul datelor introduse în aplicaţii;
- Controlul pe parcursul procesării datelor şi rapoartele produse în caz de nerealizarea procesării (întreruperi, transfer);
- Controlul datelor rezultate în urma procesării, astfel încât să se asigure că aceste date sunt complete;
- Controlul privind validarea datelor transferate din alte aplicaţii;
- Controlul privind tranzacţiile efectuate.

Pentru deficienţele constatate s-a recomandat identificarea riscurilor care guvernează toate subsistemele IT, stabilirea controalelor interne care ar trebui să existe pentru ca acestea să funcţioneze corect, urmărirea controalelor interne care există şi funcţionează, identificarea şi implementarea de instrumente de control pentru controalele interne care nu sunt implementate sau nu funcţionează.

4. SECURITATEA INFORMAŢIEI

4.1. Organizarea securităţii informaţiilor

4.1.1. Elaborarea politicii privind securitatea informaţiei

……

4.1.2. Stabilirea responsabilităţilor în cadrul politicii de securitate

…….

4.1.3. Securitatea datelor asigură disponibilitatea acestora doar pentru utilizatorii autorizaţi

…….

4.2. Disponibilitatea datelor

4.2.1. Protejarea datelor împotriva virusilor

…….

4.2.2. Asigurarea continuităţii activităţilor

……

4.2.3. Recuperarea datelor în caz de dezastru

……

4.3. Asigurarea funcţionării programelor şi aplicaţiilor

4.3.1. Asigurarea introducerii corecte a datelor

……..

4.3.2. Prelucrarea datelor

……

4.3.3. Asigurarea securităţii datelor şi documentelor

PROBLEMA

Din analiza efectuată s-a constatat că la nivelul Departamentului IT nu se respectă procedurile specifice privind asigurarea securităţii reţelelor, astfel:

- la nivelul departamentului IT au fost întocmite hărţi privind infrastructura reţelelor IT, însă una din cele 3 hărţi cuprinse în eşantion nu fusese actualizată, astfel încât aplicaţiile copiate pe un număr de 4 sisteme nu au fost protejate prin intermediul programelor antivirus. De asemenea, aplicaţiile contabile au fost copiate de pe unul din calculatoarele existente, fără a se proceda la instalarea acestora de către personalul specializat din cadrul departamentului IT, ocazie cu care nu au putut fi asigurata integritatea tuturor modulelor.

- deşi există o clasificare a sistemelor hardware, în funcţie de importanţa fiecărei categorii în parte, în ceea ce priveşte aplicaţiile informatice, nu a fost avută în vedere o prioritizare a importanţei acestora în vederea alocării corespunzătoare a resurselor de securitate.

- la nivelul entităţii s-a procedat la identificarea şi înlăturarea celor mai critice vulnerabilităţi ale reţelelor, însă nu a fost avut în vedere un sistem de management al vulnerabilităţilor, la cel mai profund nivel, actualizat, care să permită identificarea precisă şi cuprinzătoare a ultimilor vulnerabilităţi ale sistemului sau a greşelilor de configurare, bazându-se pe informaţii precise şi configuraţii de sistem şi de reţea adecvate.

- administratorii de sistem au procedat la întocmirea de rapoarte care detaliază nivelul critic al vulnerabilităţilor şi au furnizat soluţii de remediere însă informaţiile nu au fost strânse, adaptate şi prezentate acelor persoane care decid asupra situaţiei securităţii în cadrul entităţii publice. Astfel, conducerea entităţii nu a avut la dispoziţie informaţiile necesare cuantificării efortului necesar pentru asigurarea securităţii reţelelor.

Pentru remedierea deficienţelor constatate au fost formulate următoarele recomandări:

1. Implementarea procedurilor operaţionale de lucru cu elemente care să asigure actualizarea în timp util a situaţiilor privind reţelele IT; Tratarea securităţii reţelelor ca pe un proces continuu, astfel încât schimbările în cadrul utilizatorilor, echipamentelor sau aplicaţiilor să se realizeze evitând expunerile la riscuri;

2. Prioritizare şi a aplicaţiilor informatice, în funcţie de importanţa acestora, în vederea alocării corespunzătoare a măsurilor de securitate, având în vedere că acestea necesită de cele mai multe ori resurse considerabile, care trebuie să fie direct proporţionale cu valoarea datelor sau echipamentelor de protejat;

3. Implementarea unui sistem de management al vulnerabilităţilor, care să identifice precis, cuprinzător şi actualizat la zi, ultimele vulnerabilităţi ale sistemului sau a greşelilor de configurare.

4. Toate rapoartele întocmite în urma identificării şi soluţionării vulnerabilităţilor reţelelor să fie corelate şi aduse la cunoştinţa conducerii entităţii publice.

4.4. Implementarea instrumentelor de control

4.4.1. Accesul la aplicaţie este oferit pe baza necesităţilor utilizatorului

Posturile de lucru dotate cu computer nu sunt evidenţiate la nivelul Departamentului IT, neasigurându-se o intervenţie promptă şi rapidă, iar securitatea datelor şi informaţiilor nu este asigurată pe baza unui sistem de autorizare a accesului şi unui sistem adecvat de parole.

La nivelul entităţii au fost elaborate harţi privind reţele informatice existente. În acest sens, au fost stabilite locaţiile serverelor, sistemelor desktop, sistemelor laptop, a routerelor, a punctelor de acces, a imprimantelor şi a celorlalte dispozitive conectate la reţea. Aceste hărţi au stat la baza elaborării sistemului de management al securităţii reţelelor din cadrul entităţii.

Analiza celor 3 reţele care a constituit eşantionul, a pus în evidenţă faptul că pentru două reţele hărţile erau corespunzătoare, însă referitor la reţeaua care deservea direcţia generală buget-finanţe s-a constatat că, au fost achiziţionate şi conectate 4 noi computere şi o imprimantă de reţea, toate deservite prin intermediul unui nou router, care nu au fost consemnate în cadrul hărţii.

De asemenea, pe cele 3 computere au fost copiate aplicaţiile contabile utilizate la nivelul direcţiei, fără a fi luate măsuri pentru asigurarea securităţii datelor şi informaţiilor prin controlarea accesului şi implementarea de programe antivirus adecvate.

La nivelul departamentului IT există o clasificare a sistemelor hardware, în funcţie de importanţa fiecărei categorii pentru buna desfăşurare a activităţii în cadrul entităţii. În acest sens, dispozitivele din reţea au fost grupate în funcţie de priorităţi, de la sisteme cu importanţă redusă, cum sunt sistemele de test sau care sunt folosite independent pentru asigurarea funcţiilor mai puţin importante ale entităţii şi sistemele de importanţă medie, cum sunt sistemele laptop folosite de unii angajaţi în cadrul delegaţiilor sau pentru lucrul acasă, la sisteme de importanţă majoră pentru asigurarea continuităţii activităţilor organizaţiei, cum ar fi sistemele care gestionează bazele de date, serverele care deservesc compartimentele cheie ale entităţii (tranzacţii, operaţiuni financiare etc.).

Deşi există o clasificare a sistemelor hardware, în funcţie de importanţa fiecărei categorii în parte, în ceea ce priveşte aplicaţiile informatice, nu a fost avută în vedere o prioritizare a importanţei acestora în vederea alocării corespunzătoare a resurselor de securitate. Ex. - aplicaţia informatică utilizată la nivelul serviciului secretariat pentru urmărirea circuitului documentelor beneficiază de aceleaşi măsuri de securitate ca şi sistemul integrat privind conducerea organizaţiei.

Administratorii de reţea au procedat la întocmirea de rapoarte prin care detaliază nivelul vulnerabilităţilor şi furnizează soluţii de remediere, însă informaţiile nu sunt adaptate şi prezentate persoanelor cu responsabilităţi decizionale asupra securităţii informaţionale.

Recomandările formulate au făcut referire la prioritizarea aplicaţiilor informatice, în funcţie de importanţa acestora, în vederea alocării corespunzătoare a măsurilor de securitate şi tratarea securităţii reţelelor ca pe un proces continuu. Implementarea unui sistem de management al vulnerabilităţilor, care să identifice vulnerabilităţile şi greşelile de configurare şi să dispună măsurile operative de soluţionare. Rapoartele întocmite în urma identificării şi soluţionării vulnerabilităţilor reţelelor să fie corelate şi aduse la cunoştinţa conducerii organizaţiei.

4.4.2. Introducerea instrumentelor de control fizic asupra echipamentelor IT al aplicaţiilor

Controalele fizice nu sunt implementate in mod eficient pentru a asigura securitatea echipamentelor.

Din examinarea efectuata si observarea la fata locului s-a constatat unele disfuncţii legate de accesul necontrolat la cele trei locaţii selectate atât a persoanelor din cadrul altor departamente cât şi a altor persoane din afara entităţii publice;

Totodată, deşi au fost instalate camere de supraveghere, acestea nu sunt permanent monitorizate. Deseori, camerele în care sunt localizate servere-le sunt lăsate descuiate şi nesupravegheate, deşi sunt echipate cu încuietori adecvate;

La scoaterea echipamentelor din cadrul organizaţiei nu există obligativitatea prezentării unei autorizaţii scrise.

*Pentru deficienţele constatate s-a recomandat introducerea de instrumente de control adecvate astfel incit orice acces la echipamentele sau datele si informaţiile organizaţiei sa fie limitat, sau in cazurile in care acesta este permis sa fie supravegheat in totalitat*e.

4.5. Securitatea reţelei

4.5.1. Monitorizarea securităţii reţelelor

……

4.6. Gestionarea parolelor

4.6.1. Utilizatori au parole de acces individuale

Inexistenţa unui sistem de stabilire de către fiecare utilizator a parolelor şi a unui responsabil cu verificarea schimbării periodice a parolelor de acces.

Analiza interviului a scos în evidenţă, de asemenea, faptul că nu există un sistem de securitate a sistemului informatic şi un responsabil cu administrarea acestui sistem.

Recomandarea s-a referit la schimbarea sistematică a parolelor de acces de către utilizatorii sistemului informatic, precum şi stabilirea unei persoane care să aibă în responsabilitate atribuţii şi competenţe de verificare a schimbării periodice a parolelor de acces.

4.6.2. Schimbarea periodică a parolelor

……..

4.6.3. Protejarea parolelor

……

4.6.4. Persoanele autorizate au acces la sistemul de operare

……

4.7. Securitatea logică

4.7.1. Asigurarea securităţii funcţionării programelor şi aplicaţiilor

……

5. PROIECTAREA ŞI TESTAREA PROGRAMELOR ŞI APLICAŢIILOR

5.1. Proiectarea şi elaborarea programelor şi aplicaţiilor

5.1.1. Achiziţia programelor informatice

…….

5.1.2. Proiectarea programului informatic

…….

5.1.3. Elaborarea programului informatic

…….

5.2. Testarea şi implementarea programelor şi aplicaţiilor

5.2.1. Testarea programului şi aplicaţiei

……

5.2.2. Asigurarea corectitudini rezultatelor

Organizarea datelor şi stocarea acestora nu asigură o utilizare şi exploatare eficientă a acestora. Accesul la o înregistrare din fişierul de date se obţine prin parcurgerea înregistrărilor fişierului în secvenţa în care au fost stocate sau pe bază unui cod de identificare care să permită regăsirea rapidă a înregistrării.

Accesul direct se obţine prin indexarea fişierelor, adică prin crearea unor tabele de indecşi care pentru fiecare valoare atributului care permite identificarea în mod unic a unei înregistrări din fişier.

Organizarea datelor în fişierele de date prezintă următoarele disfuncţii:

- redundanţă mare – stocarea datelor în mai multe fişiere;
- acces dificil la date – exploatarea multiutilizator a datelor necesită operaţii suplimentare de sortare, fuziune, ventilare;
- izolarea datelor – imposibilitatea realizării de programe pe calculator care să acceseze datele într-o manieră globală;
- actualizarea datelor prin adăugare, modificare, ştergere generează erori atunci când mai mulţi utilizatori doresc să modifice simultan aceleaşi date;
- dependenţa programelor faţă de date – modificările din structura datelor obligă la efectuarea de corecturi în programele de calculator;
- fiecare dată este descrisă independent în toate fişierele în care apar – dacă într-un fişier se modifică formatul şi valoarea unei date, acea modificare nu se transmite automat, pentru aceeaşi dată, în toate fişierele de date.

Pentru remedierea acestor deficiente s-a recomandat organizarea datelor în baze de date, respectiv un fişier format din înregistrări, care conţin câmpuri şi operaţii de căutare, sortare sau recombinare. Pentru aceasta este necesar realizarea următoarelor: definirea, structurarea, ordonarea şi gruparea datelor în colecţii de date omogene; stabilirea legăturilor între date, între elementele unei colecţii de date şi între colecţiile de date, după o ierarhie bine precizată, precum şi memorarea datelor pe un suport informaţional prelucrabil într-un sistem de calcul.

6. ELABORAREA ŞI IMPLEMENTAREA PROIECTELOR IT

6.1. Dezvoltarea proiectelor IT

6.1.1. Iniţierea şi elaborarea proiectelor IT

……

6.2. Implementarea şi funcţionarea programelor şi aplicaţiilor

6.2.1. Reproiectarea soluţiilor IT pentru programe şi aplicaţii

…….

6.2.2. Întreţinerea aplicaţiilor garantează funcţionarea proceselor la parametri optimi

Din evaluarea realizată s-a constatat utilizarea în cadrul entităţii publice a unor programe software fără licenţă. Astfel, cu toate că entitatea publică a achiziţionat licenţe pentru pachetul de programe Lotus, s-au constatat că în cadrul unor departamente se folosesc programe aferente pachetului Microsoft Office fără ca pentru acestea entitatea publică să fi achiziţionat licenţe. Practic salariaţii au instalat programe utilizând CD-uri piratate.

La nivelul sistemului IT al entităţii publice s-a constatat inexistenţa controalelor de sistem ce alertează administratorul în cazul utilizării de soft-uri pentru care nu s-au achiziţionat licenţe.

Pentru remedierea deficienţelor constatate s-a recomandat inventarierea tuturor staţiilor de lucru pentru a stabili situaţia reală privind utilizarea programelor fără licenţă şi dezinstalarea tuturor programelor nelicenţiate din pachetul Microsoft Office. Totodată, s-a recomandat şi realizarea unei analize complexe în urma căreia managementul entităţii publice să decidă asupra oportunităţii schimbării programelor existente şi achiziţionarea unui număr adecvat de licenţe Microsoft Office.

7. PROIECTAREA, IMPLEMENTAREA ŞI MENŢINEREA ÎN FUNCŢIE A UNEI REŢELE

7.1. Proiectarea, instalarea şi administrarea reţelei de calculatoare

7.1.1. Asigurarea bunei funcţionări a sistemelor bazate pe existenţa şi funcţionarea reţelei de calculatoare

……..

7.1.2. Administrarea serverelor

…….

7.2. Interconectarea şi securitatea reţelei

7.2.1. Interconectarea reţelelor

……

7.2.2. Proiectarea şi asigurarea securităţii reţelei

Din evaluare s-a constatat neutilizarea unui singur nume de utilizator şi unei singure parole pentru accesul la sistemul IT, în condiţiile în care majoritatea salariaţilor din cadrul entităţii publice, prin natura sarcinilor de serviciu, trebuie să acceseze mai multe subsisteme IT care folosesc nume de utilizator şi parole diferite. Sistemul IT este conceput astfel încât pentru accesul la fiecare subsistem IT trebuiesc folosite: nume de utilizator şi parolă diferite, în loc să se folosească acelaşi nume de utilizator şi parolă indiferent de subsistemul IT la care se conectează angajatul.

Pentru aceasta s-a recomandat realizarea unui proces de reenginering la nivelul sistemului IT din cadrul entităţii publice, astfel încât salariaţii să poată accesa subsistemele IT de care au nevoie utilizând un singur nume de utilizator şi o singură parolă;

* *
*

Precizăm faptul că, constatările prezentate au la bază probe de audit, obţinute pe baza testelor efectuate, consemnate în documentele de lucru întocmite de către echipa de auditori şi însuşite de către factorii de management ai entităţii. Aceste evaluări au fost discutate şi recomandările auditorilor au fost acceptate în şedinţa de închidere a misiunii şi au fost apreciate de către participanţi ca fiind realiste şi fezabile.

Considerăm că rezultatele evaluării auditorilor interni privind **Activitatea IT** se înscriu în parametri normali pentru această perioadă de consolidare a implementării activităţii de audit intern în cadrul entităţilor. De asemenea, prin implementarea recomandărilor echipei de auditori activitatea Direcţiei IT va cunoaşte o ameliorare semnificativă.

Structura auditată are obligaţia să respecte **Programul de acţiune şi Calendarul implementării recomandărilor** şi să raporteze periodic echipei de auditori interni stadiul implementării acestora.

Prezentul proiect de **Raport de audit intern** a fost întocmit în baza tematicii în detaliu a obiectelor auditabile selectate, a Programului de audit şi a Programului de intervenţie la faţa locului, a constatărilor efectuate în procedurile de colectare a dovezilor, din timpul intervenţiei pe teren, şi s-au materializat în elaborarea de FIAP-uri şi FCRI-uri care au fost preluate în Raportul de audit intern.

Data: 18.10.2009

Auditori interni,	***Supervizor,***	***Pentru conformitate,***
Popescu Sorin	Dumitru Daniel	Director , Direcţia IT
Radu George		……..

Notă:

Proiectul de raport de audit intern concretizează activitatea auditorilor interni prin prezentarea cadrului general de desfăşurare a activităţii entităţii, obiectivelor, constatărilor, concluziilor şi recomandărilor obţinute în urma misiunii realizate, cât şi aria şi metodologia de audit, tehnicile de colectare şi de analiză a dovezilor de audit utilizate.

La elaborarea Proiectului de raportul de audit intern, auditorul foloseşte dovezile de audit raportate în Fişele de Identificare şi Analiza a Problemelor şi în Formularul de Constatare şi Raportare a Iregularităţilor şi în celelalte documente de lucru.

Entitatea Publică
Serviciul de audit public intern

MINUTA ŞEDINŢEI DE CONCILIERE

Misiunea de audit: Tehnologia informaţiei
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 10.09.2009
Avizat: Dumitru Daniel Data: 10.09.2009

A. Lista participanţilor:

Numele	Funcţia	Direcţia/ Serviciul	Nr. telefon	E-mail	Semnătura
Dumitru Daniel	Coordonator	CAPI			
Popescu Sorin	Auditor	SAPI			
Radu George	Auditor	SAPI			
Pătrulescu George	Director	DIT			
Voiculescu Alin	Sef	STDAM			
Boerescu Ilie	Sef	SCD			
Teodorescu Rodica	Sef	SEE			
Eleodor Darius	Sef	SAPP			
Iordache Camelia	Sef	SRC			
Păun Elena	Sef	SSD			
Badea Ştefan	Sef	SAT			

B. Stenograma şedinţei

În cadrul şedinţei de conciliere s-a discutat asupra constatărilor şi recomandărilor cuprinse în proiectul Raportului de audit, iar reprezentanţii structurii auditate au reiterat o parte din problemele cu care se confruntă şi anume:

- lipsa fondurilor necesare privind achiziţia de echipamente performante;
- programe şi aplicaţii vechi care se adaptează foarte greu nevoilor actuale de lucru şi necesităţilor utilizatorilor;
- personal insuficient;
- participarea foarte slabă şi restrânsă la instruiri, datorită lipsei resurselor financiare.

Cu privire la constatările şi recomandările formulate, conducerea entităţii a formulat un singur punct de vedere, respectiv existenţa sistemului potrivit căruia fiecare utilizator poate stabili şi introduce propria parolă, în vederea protejării echipamentului şi a aplicaţiilor pe care le utilizează. În acelaşi timp există responsabilizată persoană care verifică dacă parolele de acces au fost schimbate periodic şi au prezentat în acest sens documente justificative.

Auditori interni au reţinut acest aspect, au evaluat documentele prezentate şi au concluzionat că raportul de audit va fi revizuit în mod corespunzător referitor la această informaţie, iar recomandarea şi termenele de implementare vor ţine seama acţiunile planificate de entitate pentru implementarea acestui program.

Pentru implementarea recomandărilor şi remedierea problemelor constatate structura auditată a întocmit

şi ne-a prezentat planul de acţiune şi calendarul de implementare al recomandărilor, prin care s-au stabilit persoanele responsabile pentru implementare, etapele şi termenele de realizare.
Pentru toate celelalte constatări, structura auditată nu a formulat obiecţii fiind de acord cu acestea, recunoscând deficienţele din activitatea specifică.

Notă:
Scopul şedinţei de conciliere este de a analiza constatările şi concluziile şi de a valida definitiv recomandările şi planul de acţiune elaborat pentru implementarea acestora, modalităţile de punere în practică, responsabilii şi calendarul de implementare.
Participanţi vor fi persoanele prezente la şedinţa de închidere, conducătorul structurii auditate şi persoanele responsabile cu punerea în practică a acţiunilor stabilite.
Şedinţa de conciliere trebuie organizată în termen de 10 zile de la data primirii punctului de vedere al auditatului.

Entitatea Publică
Serviciul de Audit Intern

RAPORT DE AUDIT INTERN

MISIUNEA DE AUDIT INTERN

ACTIVITATEA IT

BUCUREŞTI
2009

CAPITOLUL I

DATE DE IDENTIFICARE A MISIUNII DE AUDIT INTERN

Echipa de auditare - *a fost formată din:*

Popescu Sorin, auditor superior, coordonator

Radu George, auditor superior

Ordinul de efectuare a misiunii de audit - auditarea activităţilor cuprinse în Planul de audit intern pe anul 2010, s-a făcut în baza Ordinului de serviciu nr. 11/12.08.2009.

Baza legală a acţiunii de auditare*:*

Planul de audit intern pentru anul 2009, aprobat de conducerea entităţii publice;

Legea nr. 672/2002 privind auditul public intern;

OMFP nr. 38/15.01.2003 pentru aprobarea Normelor generale de privind exercitarea activităţii de audit public intern.

Normele proprii de audit public intern ale entităţii, avizate şi aprobate de conducere, privind exercitarea activităţii de audit intern în cadrul entităţii.

Durata misiunii de audit: 01.09.2009 – 20.10.2009.

Perioada auditată: 01.01.2008 - 31.08.2009

Scopul acţiunii de auditare *constă în:*

- asigurarea conducerii asupra funcţionării echipamentelor, aplicaţiilor şi programelor în concordanţă cu cerinţele stabilite;
- asigurarea aplicării corecte a măsurilor de testarea şi implementarea noilor aplicaţii, de a soluţiona problemele apărute în funcţionarea aplicaţiilor.

Obiectivele acţiunii de auditare au urmărit:

- *Strategia şi planificarea sistemelor informatice;*
- *Organizarea şi funcţionarea departamentului IT;*
- *Operaţii ale sistemului informatic;*
- *Securitatea informaţiilor;*
- *Proiectarea şi testarea programelor şi aplicaţiilor;*
- *Elaborarea şi implementarea proiectelor IT;*
- *Proiectarea şi menţinerea în funcţiune a unei reţele.*

Tipul de auditare - *audit de conformitate/regularitate.*

Tehnici de audit intern utilizate:

- verificarea se realizează în vederea asigurării validităţii, realităţii şi acurateţei înregistrărilor în contabilitate a documentelor şi a concordanţei cu legile şi regulamentele în vigoare, precum şi a eficacităţii controlului intern prin cu ajutorul următoarele *tehnici de verificare:*

a) comparaţia: pentru confirmarea identităţii unor informaţii, după obţinerea lor din două sau mai multe surse diferite;

b) examinarea: pentru detectarea erorilor şi/sau iregularităţilor;

c) recalcularea: verificarea algoritmilor de calcul şi a calculelor matematice;

d) punerea de acord: pentru realizarea procesului de potrivire a doua categorii diferite de înregistrări;

e) confirmarea: pentru solicitarea informaţiilor din mai multe surse independente cu scopul validării acestora;

f) garantarea: pentru verificarea realităţii tranzacţiilor înregistrate pornind de la examinarea

înregistrărilor spre documentele justificative;

*g) urmărire*a: pentru verificarea modului în care au fost elaborate procedurile, pentru verificarea documentelor justificative spre articolul contabil în vederea verificării dacă toate operaţiunile au fost înregistrate.

- observarea fizică: constă în urmărirea unui proces sau a unei proceduri, prin care auditorul îşi formează o imagine de ansamblu asupra structurii auditate;

- interviul, notele de relaţii: se realizează de către auditorii interni prin intervievarea persoanelor auditate, implicate şi interesate şi informaţiile primite, care trebuie să fie susţinute de documente. Pentru eventualele explicaţii suplimentare se solicită note de relaţii;

***- analiza*:** constă în descompunerea unei entităţi în elemente, care pot fi izolate, identificate, cuantificate şi măsurate distinct.

Instrumentele de audit intern utilizate:

- Chestionarul de luare la cunoştinţă - CLC: pentru obţinerea unor informaţii referitoare la contextul socio-economic, organizare internă, funcţionarea entităţii/structurii auditate;

- Chestionarul de control intern - CCI: orientează auditorii interni în activitatea de identificare obiectivă a disfuncţiunilor şi cauzelor reale ale acestora. Acesta a fost utilizat pentru evaluarea instrumentelor de control existente, împreună cu alte informaţii relevante pentru audit, pe parcursul desfăşurării misiunii de audit intern;

- Listă de verificare - LV: pentru stabilirea condiţiilor de regularitate pe care trebuie să le îndeplinească fiecare domeniu auditabil. Cuprinde un set de operaţii ce trebuie parcurse de auditor pentru a analiza activităţile de control intern încorporate în proceduri, existenţa responsabilităţilor pentru efectuarea acestora şi permite stabilirea testelor de conformitate atunci când sunt semnalate diferite disfuncţionalităţi;

- Fişa de identificare şi analiză a problemelor – FIAP: întocmită pentru fiecare disfuncţionalitate constatată;

- Formularul de constatare şi raportare a iregularităţilor –FCRI: întocmit cu scopul de a informa conducerea direcţiei cu privire la iregularitatea constată.

Documente şi materiale examinate în cadrul Direcţiei IT *- verificarea la faţa locului a vizat documentaţia aferentă perioadei auditate, respectiv 01.01.2008 – 30.06.2009, care a cuprins următoarele:*

- legi şi regulamente aplicabile structurii auditate;
- strategia în domeniul IT;
- organigrama Direcţiei IT;
- Regulamentul de Organizare şi Funcţionare;
- Fişele posturilor;
- Proceduri operaţionale de lucru;
- Rapoarte de evaluare;
- Liste de achiziţii în domeniul IT;
- aplicaţii informatic;
- programe informatice achiziţionate;
- Planul privind continuitatea activităţilor, etc.

Documente şi materiale întocmite pe timpul auditării:

- documentaţia aferentă analizei riscurilor;
- tabelul puncte tari şi puncte slabe;
- tematica în detaliu a misiunii de audit intern;
- programul de audit intern;
- programul intervenţiei la faţa locului;
- liste de verificare structurate pe obiective;
- foi de lucru pentru stabilirea eşantioanelor;
- chestionare de control intern;
- teste;
- liste de control;
- fişe de identificare şi analiză a problemelor constatate - FIAP-uri;
- formulare de constatare şi raportare a iregularităţilor - FCRI-uri;
- proiectul raportul de audit intern;

- minutele şedinţelor de deschidere, de închidere şi de conciliere;
- Raportul de audit intern;
- planul de acţiune şi calendarul de implementare a recomandărilor;
- fişa de urmărire a implementărilor recomandărilor.
- foi de lucru privind descrierea activităţilor auditate;
- documente de lucru;
- note de relaţii;
- interviuri.

Organizarea Direcţiei IT

Direcţia IT a funcţionat în perioada supusă auditării cu un număr de 32 salariaţi, din care un 4 posturi de conducere – un director, şi 4 şefi de serviciu. Organizarea şi funcţionarea direcţiei se desfăşoară conform organigramei şi Regulamentului de organizare şi funcţionare.

Pentru toţi salariaţii au fost întocmite fişe ale posturilor prin care s-au stabilit relaţiile ierarhice de subordonare şi de colaborare, precum şi sarcinile de serviciu.

II. CONSTATĂRI

II. CONSTATĂRI ŞI RECOMANDĂRI

Prezentam principalele constatări, consecinţele care s-au produs sau care ar putea sa apară în perioada imediat următoare, precum şi recomandările formulate în vederea corectării disfuncţionalităţilor semnalate sau ale celor care pot să survină, diminuării riscurilor existente şi îmbunătăţirii sistemelor de management şi control intern al activităţilor auditate cu scopul facilitării atingerii obiectivelor prestabilite.

Obiectivul I.

1. STRATEGIA ŞI PLANIFICAREA SISTEMELOR INFORMATICE

1.1. Strategia IT este concordanţă cu scopurile organizaţiei

1.1.1. Strategia IT defineşte necesităţile şi priorităţile

Nerealizarea în termen a procedurilor de achiziţie şi implementare a programelor şi aplicaţiilor informatice.

Cu privire la armonizarea strategiei în domeniul IT cu strategia entităţii, s-a constatat că aceasta derivă şi este elaborată în conformitate cu direcţiile şi principiile de dezvoltare ale entităţii, contribuie la dezvoltarea şi eficientizarea activităţilor entităţii şi prin implementare se urmăreşte realizarea unui sistem informatic integrat, care să asigure integrarea tuturor informaţiilor şi datelor la nivelul entităţii, respectiv juridice, economice, comerciale, tehnice, financiar-contabile, de personal, sociale şi patrimoniale.

Din analiza atribuţiilor stabilite Comisiei numită la nivelul entităţii cu responsabilităţi în domeniul dezvoltării IT, s-a constatat că acestea sunt, în general, de natură metodologică, respectiv planificarea şi elaborarea strategiei în domeniul IT şi armonizarea acesteia cu strategia şi mandatul entităţii. Totuşi, această comisie are şi atribuţii cu privire la monitorizarea activităţilor privind implementarea strategiei, însă analiza realizării acestor activităţi este rezumată doar la raportările periodice realizate de departamentul IT, cu privire la stadiul implementării proiectelor IT. Limitarea exercitării acestor atribuţii, doar la analiza raportărilor efectuate de departamentul IT, fără o evaluare fizică, din partea comisiei, a modului de implementare a programelor informatice, conduce la formularea unor constatări şi concluzii insuficiente, care au influenţă în decizia managerială şi dezvoltarea strategică.

Analiza proceselor-verbale ale Comisiei numite la nivelul entităţii cu responsabilităţi în dezvoltarea IT, a direcţiilor de acţiune strategice şi a deciziilor luate în vederea implementării strategiei a pus în evidenţă unele disfuncţionalităţi, legate de faptul că anumite proiecte de dezvoltare IT derulate în cadrul entităţii nu au fost supuse analizei şi evaluării comisiei. Astfel, în cursul anului 2009, discuţiile în cadrul comisiei au

privit, în general, analiza progreselor proiectelor IT stabilite şi aprobate la nivelul entităţii, însă potrivit proceselor verbale întocmite în urma şedinţelor, a rezultat că discuţiile s-au derulat doar cu privire la proiectele pentru care au fost înaintate de către departamentul IT, rapoarte privind stadiul implementării, astfel că propunerile formulate de comisie cu privire la dezvoltarea IT, inclusiv cu privire la asigurarea resursele financiare, au fost legate doar de aceste aspecte.
În urma examinării şi analizelor efectuate s-a constatat că anumite proiecte nu au fost implementate sau sunt întârzieri în implementarea acestora, respectiv:

a) aplicaţia privind evidenţa documentelor intrate ieşite din cadrul organizaţiei, inclusiv stadiul soluţionării lor, a fost aprobată a fi implementată, inclusiv au fost asigurate resursele financiare încă din cursul anului anterior, dar până în prezent nu s-a realizat nici o procedură legată de stabilire a condiţiilor tehnice ale aplicaţiei, demararea acţiunilor de realizare a caietului de sarcini, sau a procedurilor de realizare a achiziţiei, cu toate că prin buget au fost alocate fondurile necesare.
Din discuţiile purtate cu responsabilii IT în domeniul dezvoltării şi informatizării entităţii, a rezultat că acest program informatic nu a fost demarat, deoarece la nivelul departamentului IT nu existau specialişti în testarea şi implementarea programului, iar fondurile aprobate permiteau doar achiziţia aplicaţiei.
În condiţiile în care atribuţiile comisiei permiteau şi o evaluare fizică a modului de implementare a proiectelor, greutăţile întâmpinate se puteau cunoaşte şi se puteau găsi soluţiile necesare, respectiv, în acest caz a condiţiilor de pregătire a personalului în vederea utilizării programului informatic.

b) pentru proiectul „Implementarea unei infrastructuri IT care să asigure integrarea datelor la nivelul organizaţiei", a fost raportat stadiul de implementare la comisie, însă nu şi termenele de realizare. În urma evaluării s-a constatat că au fost demarate procedurile pentru achiziţia acestuia, însă până în prezent acestea s-au limitat la studiul pieţei şi alocarea banilor în cadrul bugetului. Proiectul se află în întârziere şi nu va putea fi realizat în timp util. Aceasta va avea consecinţe negative în implementarea altor aplicaţii, care au legătură cu acesta, în acest sens va trebui decalat termenul de începere a procedurilor privind implementarea proiectului „Crearea unei structuri IT care să permită urmărirea circuitului unui document, stadiul de realizare şi persoanele care au intervenit asupra acestuia, autorizarea pe niveluri ierarhice prestabilite". Întârzierea implementării acestui program a determinat decalarea termenul planificat a obiectivului strategic „Modernizarea infrastructurii IT din cadrul entităţii".

Pentru deficienţele constatate s-a recomanda reanalizarea atribuţiilor Comisiei de planificare strategică în domeniul IT şi redefinirea acestora astfel încât să poată realiza şi monitorizarea implementării proiectelor informatice şi informarea periodică a conducerii asupra realizării acestora.

Referitor la nerespectarea procedurii de elaborare şi fundamentare a strategiei şi a politicilor de dezvoltare s-a constat, din analiza sistemului de fundamentare a strategiei, rezultă că s-au realizat următoarele etape:

*i) stabilirea rolului*i IT în cadrul organizaţiei, fiind identificată şi definită importanţa acesteia;

j) definirea misiunii structurii funcţionale în concordanţă cu obiectivele strategice şi direcţiile de acţiune stabilite la nivelul organizaţiei;

k) identificarea şi provenienţa resurselor financiare, materiale şi umane necesare aplicării şi implementării strategiei;

l) implementarea strategiei, fiind fixate termenele necesare atingerii obiectivelor în raport cu care se urmăresc asigurarea şi repartizarea resurselor precum şi concentrarea eforturilor umane şi materiale.

Tot din analiză rezultă că la elaborarea strategiei, la nivelul structurii funcţionale, nu s-au avut în vedere următoarelor etape:

g) Evaluarea situaţiei actuale pe baza analizei diagnostic, respectiv orientarea activităţii pentru o anumită perioadă, prin strategie, presupune ca, în prealabil, să fie cunoscută situaţia actuală, pe baza unei analize diagnostic, pentru a avea o imagine cât mai completă asupra domeniului de activitate al organizaţiei. Analiza diagnostic trebuia elaborată în baza unor studii privind potenţialului intern, folosind metode statistice, matematice, analiza pe bază de bilanţ etc. care să surprindă evoluţia proceselor şi fenomenelor specifice domeniului de activitate. Informaţiile de intrare nu fac referire la aspecte cum sunt: dimensiunea structurii funcţionale, resursele umane, înzestrarea tehnică, managementul utilizat;

h) Identificarea punctelor tari şi a punctelor slabe ale entităţii în vederea determinării ameninţărilor şi oportunităţilor cu care se confruntă entitatea;

i) Fundamentarea variantelor strategice – obiectivele strategice stabilite pentru IT nu au fost corelate cu posibilităţile efective ale organizaţiei, cu factorii interni şi factori externi. Realizarea strategiei implică fixarea şi respectarea termenelor necesare atingerii obiectivelor în raport cu care se urmăresc asigurarea şi repartizarea resurselor precum şi concentrarea eforturilor umane şi materiale. Totodată, trebuie

avuta în vedere compatibilitatea variantei strategice elaborata teoretic cu realitatea şi modul în care s-a reuşit surprinderea acţiunii factorilor de influenta.

Strategia a fost elaborată fără a se evalua situata actuala, pe baza unei analize diagnostic, astfel încât să putem avea o imagine cât mai completa asupra organizaţiei, asupra rezultatelor pe care şi-a propus să le obţină, a potenţialului său financiar, cât şi a importanţei în cadrul realizării programului de guvernare.

Totodată nu au fost identificate nici punctele tari şi punctele slabe în vederea determinării ameninţărilor şi oportunităţilor cu care se confruntă entitatea.

De asemenea, obiectivele strategice ale structurii funcţionale, definite în cadrul strategiei, nu au fost corelate cu posibilităţile efective ale organizaţiei, cu factorii interni şi factori externi. Realizarea strategiei implica fixarea şi respectarea termenelor necesare atingerii obiectivelor în raport cu care se urmăresc asigurarea şi repartizarea resurselor precum şi concentrarea eforturilor umane şi materiale.

Pentru deficienţele constatate s-a recomandat pregătirea profesională anticipată a personalului implicat în elaborarea strategiei, de către managementul responsabil cu aceasta. Reanalizarea strategiei definite la nivelul structurii funcţionale în conformitate cu procedura operaţională aprobată şi actualizarea acesteia astfel încât implementarea sa să contribuie la realizarea unui management modern in domeniul de activitate şi la atingerea obiectivelor strategice ale organizaţiei.

În acelaşi timp s-a mai recomandat îmbunătăţirea procedurilor operaţionale de lucru privind sistemul de fundamentare a necesarului de resurse pentru elaborarea strategiei.

Referitor la faptul că obiectivelor strategice nu asigură acoperirea domeniului de activitate al structurii funcţionale şi nu contribuie la asigurarea realizării mandatului organizaţiei s-a constat că acestea reprezintă exprimările cantitative şi calitative ale scopului pentru care există şi funcţionează organizaţia.

În acelaşi timp din analiza modului de definire şi stabilire a obiectivelor strategice s-a constatat că acestea nu întrunesc următoarele caracteristici definitorii:

- nu sunt realiste şi nu au fost luate în calcul capacităţile şi posibilităţile efective de realizare de care dispune organizaţia în condiţiile actuale;
- nu sunt mobilizatoare şi nu implică eforturi de autodepăşire din partea salariaţilor;
- nu sunt comprehensibile şi nu sunt formulate şi prezentate într-o manieră care să permită înţelegerea conţinutului lor de către salariaţi;
- nu sunt antrenante şi nu asigură o abordare sistemică a intereselor organizaţiei şi componentelor sale organizatorice într-o viziune optimizantă pe termen mediu şi lung.

Aceşti factori trebuie să se regăsească la orice obiectiv strategic, indiferent de natura sa (economică, tehnică), deoarece aceste obiective reprezintă punctul de plecare în conturarea unui sistem unitar de obiective ce vizează toate componentele procesuale şi structurale ale organizaţiei.

Dimensiunea şi natura obiectivelor strategice generează direct sau indirect modalităţi şi opţiuni de realizare care condiţionează decisiv conţinutul şi funcţionalitatea strategiei, ceea ce impune ca la implementarea lor să se ia în considerare principalele variabile exogene ce influenţează comportamentul economic şi managerial al organizaţiei, cât şi capacitatea acesteia de adaptare la schimbare.

La fundamentarea necesarului de resurse solicitate de atingerea obiectivelor nu s-a realizat o dimensionare corectă a fondurilor de investiţii şi a mijloacelor circulante pe baza unor indicatori specifici, cantitativi şi calitativi.

De asemenea, nu în toate situaţiile, personalului i-au fost asigurate condiţiile de instruire pentru dobândirea aptitudinilor necesare realizării eficiente a obiectivelor individuale pentru a contribui astfel, în condiţii de performanţă, la obţinerea impactului definit de obiectivele strategice.

Pentru deficienţele constatate s-a recomandat evaluarea performanţelor actuale ale sistemului de organizare şi conducere a activităţilor desfăşurate în cadrul structurii funcţionale, ţinând cont de influenţa factorilor de mediu, interni şi externi, în vederea redefinirii obiectivelor strategice. Implicarea managementului pentru ca obiectivele strategice redefinite să întrunească caracteristicile de a fi realiste, mobilizatoare, stimulative şi să poată fi înţelese de salariaţi, stabilite de metodologie.

Totodată, la redefinirea acestora se va urmări asigurarea resurselor necesare implementării lor.

1.2. Planurile IT se adresează întregii organizaţii

1.2.1. Planurile IT ajută la îndeplinirea misiunii organizaţiei

Resursele nu sunt fundamentate corect în vederea implementării planului anual de activitate.

Din analiză s-a constatat că eforturile pentru elaborarea planului anual de activitate implică alocarea

de fonduri şi resurse ridicate din partea organizaţiei care, în cele mai multe din cazuri, nu au ca referinţă atingerea scopului fundamental al acesteia.

În acelaşi timp, activităţile considerate prioritare ale planului anual nu au fost realizate sau implementate în totalitate, în mod corespunzător, deoarece nu au fost reanalizate şi repartizate atribuţiile în cadrul compartimentelor în corelaţie cu noile obiective şi activităţi stabilite în cadrul planului. Aceasta a însemnat că, în unele cazuri, obiectivele şi activităţile deşi erau cunoscute de personal, acesta nu avea competenţa necesară, în special a celor care erau realizate în colaborare cu alte structuri funcţionale, ceea ce a necesitat solicitarea unor competenţe pentru realizarea acestora, proces care a îngreunat implementarea obiectivelor şi realizarea activităţilor.

În alte cazuri, activităţile nu au fost comunicate salariaţilor, respectiv obiectivele individuale au rămas aceleaşi, în condiţiile în care obiectivele cuprinse în planul compartimentului au fost cu totul altele. Aceasta a însemnat stabilirea măsurilor în cursul anului, instruirea, sub diferite forme, a personalului pentru înţelegerea acestora şi stabilirea priorităţilor de implementare, ceea ce a condus la întârzieri în atingerea unor obiective ale planului.

Nevoia de îmbunătăţire a nivelului de competenţă în raport cu progresele tehnico-informaţionale şi organizatorice, pentru creşterea eficienţei şi reducerea costurilor, a presupus definirea în cadrul planului anual a unor asemenea obiective şi activităţi, însă pentru implementarea acestora nu a fost corelat necesarul de mijloace şi echipamente cu necesităţile pentru atingerea obiectivelor planului.

În cadrul planului reducerea costurilor a fost definită şi prin reducerea personalului, prin care s-au pierdut o serie de competenţe care, din motive financiare, nu au fost înlocuite, prin dezvoltarea altor angajaţi, ceea ce a condus la realizarea activităţilor, dar nu au fost atinse condiţiile de performanţă stabilite.

Monitorizarea resursele financiare utilizate în derulare obiectivelor planului anual a fost de multe ori deficitară, ceea ce a contribuit la realizarea de costuri suplimentare faţă de cele planificate pentru implementarea obiectivelor stabilite.

În cadrul entităţii nu a fost comunicată eficient şi nu a fost conştientizată nevoia de cunoaştere a normelor, legislaţiei şi metodologiei în domeniile de activitate, a diferitelor culturi din cadrul organizaţiei, importanţa obiectivelor stabilite spre îndeplinire şi modul cum acestea contribuie la atingerea obiectivelor generale şi a obiectivelor strategice, şi înţelegerea comportamentului competitiv ca un sistem în care oamenii şi resursele interacţionează continuu.

Activităţile considerate prioritare ale planului anual nu au fost realizate sau implementate corespunzător deoarece nu s-au reanalizat şi repartizat atribuţiile compartimentelor pentru a asigura competenţa necesară realizării obiectivelor şi activităţilor stabilite în cadrul planului.

De asemenea, nu au fost stabilite şi comunicate salariaţilor obiectivele individuale care derivă din noile obiective stabilite în cadrul planului de activitate şi care se aflau în competenţa compartimentului funcţional.

Definirea în cadrul planului anual a obiectivelor şi activităţilor s-a realizat fără să se asigure: nevoia de îmbunătăţire a nivelului de competenţă în raport cu progresele tehnico-informaţionale şi organizatorice;creşterea eficienţei şi reducerea costurilor; corelarea necesarul de echipamente cu necesităţile de atingere a obiectivelor planului.

Pentru deficientele constatate s-a recomandat dezvoltarea unui sistem de instruire şi pregătire a salariaţilor astfel încât metodologia specifică domeniului de activitate, normativă şi procedurală, să fie aplicată corespunzător pentru dezvoltarea şi implementarea planurilor anuale. În baza planurilor elaborate să se identifice toate atribuţiile necesare pentru atingerea obiectivelor stabilite, iar acestea să fie repartizate corespunzător în cadrul compartimentelor.

Totodată, s-a mai recomandat promovarea dezvoltării resurselor umane pentru a obţine competenţele necesare creşterii economice în condiţiile în care au loc reduceri de personal, precum şi evaluarea cuprinzătoare a resurselor (financiare, instituţionale, programe, personal) necesare implementării planurilor anuale de activitate şi monitorizarea eficientă pentru a se asigura încadrarea în limitele stabilite.

1.2.2. Planurile IT oferă asigurare cu privire la faptul că resursele IT sunt alocate în concordanţă cu necesităţile

Unele departamente din cadrul entităţii nu dispun de subsisteme IT specifice activităţilor care se desfăşoară în cadrul acestora.

Din analiză s-a constatat că în cadrul entităţii publice există structuri nou-înfiinţate ca urmare a recomandărilor Comisiei Europene şi a schimbărilor legislative, care nu au notificat departamentul IT în privinţa nevoilor lor de aplicaţii informatice specifice. În acelaşi timp, s-au constatat şi departamente nou înfiinţate care şi-au exprimat nevoile pentru realizarea subsistemelor IT specifice activităţii lor, dar care nu

au beneficiat de implementarea acestora, conform planificării, datorită întârzierilor în realizarea achiziţiilor.

Pentru deficienţele constatate s-a recomandat coroborarea atribuţiilor prezentate prin proceduri cu cele stabilite prin fişele posturilor şi inventarierea stadiului implementării subsistemelor IT la nivelul departamentelor entităţii publice şi stabilirea necesităţilor IT care trebuie incluse în strategia IT.

1.3. Obiectivele IT îndeplinesc obiectivele organizaţiei

1.3.1. Strategia IT este concordantă cu scopurile organizaţiei

……

1.4. Comitetul IT determină strategia IT

1.4.1. Comitetul IT transpune strategia în planuri pe termen scurt şi pe termen mediu

…….

1.4.2. Comitetul IT stabileşte prioritătile proiectelor între dezvoltarea sistemelor şi activităţilor realizate

…….

1.5. Organizarea IT corespunde necesităţilor organizaţiei

1.5.1. Organizarea adecvată a funcţiei IT

……

1.5.2. Adecvarea practicilor şi procedurilor IT la procesele existente

……..

1.6. Elaborarea strategiei IT corespunde strategiei entităţii

1.6.1. Dotarea actuală cu tehnică de calcul a stat la baza strategiei IT

……..

2. ORGANIYAREA ŞI FUNC'IONAREA DEPARTAMENTULUI IT

2.1. Definirea atribuţiilor şi activităţilor

2.1.1. Definirea atribuţiilor şi responsabilităţilor în cadrul Departamentului IT

Atribuţiile stabilite pentru posturile din cadrul Departamentului IT nu asigură întotdeauna aria de competenţă privind realizarea activităţilor şi acţiunilor repartizate.

Atribuţiile definite in sarcina salariaţilor nu sunt întotdeauna conforme şi nu asigură competenţa de realizare a activităţilor şi acţiunilor, acestea fiind definite în multe cazuri la modul general, nu indică, prin modul de formulare o acţiune, nu asigură un conţinut clar, fiind definite sub forma unei relaţii funcţionale sau având caracter de activitate.

În acest sens s-a recomandat conştientizarea managementului responsabil cu procesul de stabilire şi definire a atribuţiilor prin informări şi consilieri pentru clarificarea modalităţilor practice de definire a unei atribuţii sau unui set de atribuţii pentru asigurarea ariei de competenţă necesară pentru realizarea activităţilor.

2.1.2. Definirea activităţilor în cadrul structurii organizatorice

Activităţile nu sunt definite omogen în cadrul structurii funcţionale, iar stabilirea complexităţii acestora nu se realizează în funcţie de nivelurile de calificare ale posturilor existente.

La definirea activităţilor se are în vedere complexitatea acestora, respectiv gradul de diferenţiere a muncii pe orizontală şi pe verticală. Diferenţierea pe orizontală constă în numărul de activităţi (specializări) şi de subunităţi funcţionale (birouri, servicii). Diferenţierea pe verticală se referă la numărul de niveluri ierarhice de-a lungul cărora se exercită autoritatea în organizaţie.

Analiza conţinutului şi modului de definire a activităţilor necesare pentru realizarea fiecărui obiectiv specific a pus în evidenţă următoarele:

– unele activităţi sunt definite sub forma unor relaţii de colaborare care fie nu indică acţiuni concrete de realizare a acestora, fie indică o acţiune comună de realizare;

– altele sunt definite sub forma unor relaţii de colaborare, în condiţiile în care sunt exercitate acţiuni concrete de realizare şi pentru care există rezultate aşteptate stabilite;

– nu sunt identificate toate activităţile care contribuie la realizarea obiectivelor specifice şi care asigură conformitatea cu reglementările legale.

Prin modul de organizare a activităţilor structurilor organizatorice ale direcţiei nu se asigură evitarea dublării acţiunilor, respectiv există activităţi identice sau similare, desfăşurate de mai multe departamente şi probleme semnificative de suprapunere şi de coordonare.

De asemenea, pentru realizarea unor activităţi, nu se respectă principiul convergenţei în definirea şi stabilirea conţinutului activităţilor care sunt necesare pentru realizarea unui obiectiv.

Pentru reglementarea deficienţelor constatate s-a recomandat realizarea unei analize riguroase a sarcinilor şi responsabilităţilor fiecărui angajat, care să stea la baza oricărei iniţiative de organizare a activităţii. Constituirea unei echipe, pe baza deciziei managementului general, care să analizeze şi să redefinească activităţile şi acţiunile realizate în cadrul compartimentelor şi serviciilor, astfel încât să se asigure că obiectivele vor fi realizate în totalitate.

La stabilirea obiectivelor se va urmări dacă sunt ataşate toate activităţile necesare obţinerii rezultatelor stabilite, realizate efectiv în cadrul compartimentului, formulate ca acţiuni concrete.

2.2. Stabilirea structurii organizatorice

2.2.1. Organizarea funcţională a Departamentului IT

Organigrama ca document prin care se relevă grafic structura organizaţiei şi substructurile acesteia nu pune în evidenţă organizarea şi funcţionarea departamentului. Compartimentele aflate în subordinea departamentului nu sunt nominalizate în totalitate în cadrul organigramei şi nu este precizat nici nivelul de subordonare al departamentului în cadrul organizaţiei.

Organigrama nu furnizează o înţelegere a raporturilor de subordonare şi de evitare a suprapunerilor de competenţe. Astfel, cu privire la raporturile de subordonare, potrivit organigramei, Serviciul Programare este organizat sub forma unui compartiment care se află în directa subordonare a directorului general adjunct al departamentului, dar în realitate acest compartiment este organizat la nivel de serviciu şi subordonat directorul general. Postul de director general adjunct a fost desfiinţat în anul 2008 urmare a reorganizărilor efectuate.

Definirea relaţiilor ierarhice aşa cum a fost precizat mai sus, nu asigură o integrare corespunzătoare a departamentului în structura organizatorică a organizaţiei şi nu se asigură operativitatea fluxului de informaţii şi date între structurile implicate în fluxul tehnologic al activităţilor.

În structura organizatorică a departamentului, definită în cadrul organigramei, nu se precizează în cadrul serviciilor numărul de posturi şi responsabilii structurilor funcţionale corespunzător fiecărui nivel ierarhic şi/sau cine coordonează aceste servicii şi compartimente, ceea ce nu permite identificarea nivelurilor şi relaţiilor ierarhice.

Pentru remedierea deficienţelor constatate s-a recomandat analiza actului normativ de organizare şi funcţionare a organizaţiei şi urmărirea atribuţiilor definite departamentului astfel încât să acopere în totalitate activităţile desfăşurate.

Totodată, din evaluare s-a mai constat că persoanele responsabilizate în posturile de conducere nu au coordonat în nici un fel activităţile care erau realizate zilnic de către salariaţi, nu au îndrumat în nici un fel salariaţii cu privire la modul în care în care să realizeze activităţile şi nici nu au realizat o monitorizare cu privire la modul de realizare a acestora. Salariaţii, în baza sarcinilor stabilite prin fişa postului, au realizat

activităţile în funcţie de cunoştinţele şi aptitudinile pe care le deţineau.

Examinarea fişelor posturilor pentru posturile de execuţie ocupate de persoanele care au fost numite cu delegaţie în posturi de conducere s-a constatat că acestea nu prevedeau nici o aptitudine managerială.

La nivelul celor două servicii în această perioadă nu a fost luată nici o decizie cu privire la îmbunătăţirea activităţilor sau la dezvoltarea acestora.

Pentru aceste nereguli s-a recomandat desfăşurarea procesului de selecţie şi recrutarea în vederea ocupării posturilor de conducere existente la nivelul departamentului IT. În acelaşi timp se va urmări dacă persoanele selectate deţin abilităţile şi aptitudinile manageriale necesare realizării activităţilor specifice celor două servicii şi dacă au pregătirea de bază, de nivel superior, în domeniul IT.

2.2.2. Examinarea sistemului de gestionare a riscurilor generale la nivelul Departamentului IT

Din analiză s-a constatat că riscurile nu sunt identificate şi gestionate la nivelul departamentului şi nu este condus Registrul riscurilor cuprinzând riscurile potenţiale şi istoricul acestora, precum şi instrumentele de control intern implementate pentru limitarea acestora.

Pentru această deficienţă s-a recomandat elaborarea mecanismelor procedurale şi metodologice privind identificarea riscurilor şi gestionarea acestora, evaluarea riscurilor identificate şi diferenţierea acestora în riscuri inerente şi riscuri acceptabile, precum şi implementarea de instrumente de control pentru riscurile inerente, astfel încât manifestarea acestora să fie limitată şi nivelul acestora să devină unul acceptabil.

Sistemul de control intern definit la nivelul organizaţiei nu cuprinde toate activităţile de control ce trebuie alocate în vederea atingerii obiectivelor.

Din analiza sistemului de control intern instituit la nivelul departamentului IT a rezultat că unele activităţi de control relevante nu au fost cuprinse în politicile şi procedurile de control instituite, astfel:

- revizuiri ale performanţei - aceste activităţi de control trebuie să includă revizuiri şi analize ale performanţei efective în comparaţie cu bugetele, previziunile şi performanţa perioadelor precedente;
- procesarea informaţiilor – acestea trebuie să includă cele două grupări de activităţi de control ale sistemelor informaţionale, respectiv controalele asupra aplicaţiilor individuale şi controalele generale asupra tehnologiei informaţiei, care sunt de fapt politici şi proceduri care se referă la mai multe aplicaţii şi contribuie la asigurarea funcţionării adecvate continue a sistemelor informaţionale.

Anumite activităţi de control care nu sunt de rutină şi care depind de existenţa unor politici adecvate stabilite de conducere sau de cei însărcinaţi cu guvernanţa nu au o aprobare de la aceste niveluri şi nici nu au fost delegate în responsabilitatea unor posturi inferioare.

Pentru remedierea acestor deficienţe s-a constatat stabilirea controalelor interne aferente riscurilor identificate şi determinarea gradului de funcţionalitate al acestora şi proiectarea de instrumente sau măsuri de introducere de controale interne, fie individuale, fie în combinaţie cu alte controale, capabile să prevină, detecteze şi să corecteze în mod eficient denaturările semnificative.

În acelaşi timp din analiza efectuată a mai rezultat că la nivelul departamentului nu este organizat şi nu se conduce registrul riscurilor. Riscurile cu care se confruntă organizaţia nu sunt identificate şi nu sunt monitorizate în vederea stăpânirii şi menţinerii lor la un nivel acceptabil.

Pentru soluţionarea acestei deficienţe s-a recomandat instituirea şi conducerea Registrului riscurilor la nivelul organizaţiei.

2.3. Stabilirea responsabilităţilor

2.3.1. Definirea sarcinilor prin fişa postului

Studiile de specialitate aferente unui post sunt definite în cadrul fişei postului fără a se ţine cont de scopul postului şi cunoştinţele de bază necesare pentru realizarea atribuţiilor alocate acestuia. Din analiza fişelor posturilor s-a constatat că la concursul organizat pentru ocuparea postului respectiv poate participa orice persoană care are o diplomă, deoarece nu se specifică tipul de studii şi nivelul acestora, respectiv în domeniul IT, studii superioare de lungă durată absolvite cu diplomă de licenţă etc.

La stabilirea sarcinilor în fişele posturilor nu se urmăreşte asigurarea unui echilibru între sarcinile şi competenţele titularului postului. Din analiza eşantionului selectat a rezultat că pentru posturile cu un nivel al studiilor medii sunt alocate aceleaşi atribuţii şi responsabilităţi ca şi pentru posturile cu un nivel al

studiilor superiore. Acestea creează probleme în gestionarea aplicaţiilor şi programelor, deoarece persoanelor încadrate în cadrul departamentului pe studii medii le-au fost date în responsabilitate întreţinerea de aplicaţii şi programe complexe şi chiar realizarea de astfel de aplicaţii pentru organizaţie, care necesită cunoştinţe IT de nivel superior şi chiar anumite specializări.

Pentru aceasta s-a recomandat analiza sarcinilor şi atribuţiilor definite în fişele posturilor şi stabilirea acestora în funcţie de caracteristicile postului, respectiv nivelul postului şi urmărirea definirii aceluiaşi gen de sarcini şi atribuţii numai dacă posturile sunt de acelaşi nivel.

Totodată, atribuţiile definite în sarcina compartimentelor funcţionale nu sunt întotdeauna conforme şi nu asigură competenţa de realizare a activităţilor şi acţiunilor, acestea fiind definite în multe cazuri la modul general, nu indică, prin modul de formulare, o acţiune, nu asigura un conţinut clar, fiind sub forma unei relaţii funcţionale sau având caracter de activitate sau sarcină.

Nu sunt definite în cadrul ROF-ului la capitolul privind departamentul IT relaţiile cu celelalte structuri funcţionale cu care are sau ar trebui să aibă relaţii funcţionale, respectiv nu este definită relaţia funcţională care reglementează asigurarea conformităţii informaţiilor cu privire la asistarea utilizatorilor în realizarea activităţilor de introducere a datelor şi informaţiilor în cadrul aplicaţiilor şi programelor derulate la nivelul celorlalte departamente funcţionale din cadrul organizaţiei, precum şi cu privire la asistarea în utilizarea echipamentelor din dotare.

Totodată, nu sunt prezentate relaţiile ierarhice între posturile de conducere şi posturile de execuţie, ci numai relaţia ierarhică între posturile de conducere situate la niveluri ierarhice diferite din cadrul departamentului IT.

În vederea remedierii acestor deficienţe s-a recomandat identificarea şi definirea corectă în cadrul documentului de organizare şi funcţionare, a atribuţiilor specifice departamentului, a relaţiilor funcţionale pe care compartimentul la are cu alte structuri funcţionale din cadrul organizaţiei.

3. OPERAŢII ALE SISTEMULUI INFORMATIC

3.1. Managementul operaţiunilor

3.1.1. Performanţa, capacitatea şi disponibilitatea sistemelor informatice este monitorizată de administratori

Existenţa unor controale interne slabe privind managementul operaţiunilor IT, reflectate în disfuncţii legate de gestionarea acestora, astfel:

- în urma analizei modului de alocare şi utilizare efectivă a resurselor IT disponibile, echipa de auditori a constatat că unele departamente dispun de resurse insuficiente (departamentul IT), în timp ce altele dispun de resurse excedentare (Direcţia Generală de Investiţii, Achiziţii Publice şi Servicii Interne), fiind utilizate în proporţie de max. 10-15%.

- echipa de auditori a constatat că listele generate în urma prelucrărilor pe un anumit computer puteau fi vizualizate şi modificate de pe toate celelalte computere din reţea, accesul la ele nefiind restricţionat.

- în urma inventarierii intervenţiilor efectuate asupra computerelor, imprimantelor şi copiatoarelor aflate în cadrul biroului Multiplicare, s-a constatat că procedurile privind mentenanţa nu au fost realizate cu respectarea specificaţiilor producătorului, de către personal autorizat, fapt ce a condus, în majoritatea cazurilor, la pierderea garanţiei, dar a fost afectată şi performanţa echipamentelor respective.

- analizând modul de soluţionare a unui număr de 6 probleme de ordin tehnic apărute în cadrul proceselor, echipa de auditori a constatat că au fost efectuate intervenţii punctuale din partea personalului specializat din cadrul departamentului IT al entităţii, urmărindu-se strict remedierea respectivelor probleme şi fără a se avea în vedere etapele premergătoare apariţiei problemei, cauzele şi modul de propagare etc.

- Analizând modul de efectuare a verificărilor asupra prelucrărilor, implementării funcţiilor şi programelor, asupra modului de iniţiere a unor proceduri sau a timpului de execuţie, echipa de auditori a constatat că o anumită parte din aceste verificări se realizează manual.

Pentru deficienţele constatate s-a recomandat următoarele:

- implementarea unei aplicaţii care să monitorizeze alocarea şi utilizarea resurselor în funcţie de gradul de complexitate al operaţiilor efectuate. Urmărirea în permanenţă a echilibrului între necesităţile IT şi resursele alocate acestor scopuri.

- mediile sau locaţiile de stocare să fie protejate împotriva deteriorării sau accesului neautorizat.

- procedurile de mentenanţă a echipamentelor să fie realizate corect şi la intervale de timp stabilite în funcţie de specificul fiecărei componente, numai de către personal autorizat în acest sens.

- constituirea în cadrul departamentului IT a unui colectiv specializat în raportarea şi rezolvarea operativă a problemelor de ordin tehnic (Help Desk), care să asigure şi acordarea suportului tehnic de specialitate către utilizatori, fie prin linii telefonice dedicate, fie prin e-mail sau deplasări ale echipelor specializate.

- elaborarea şi implementarea unor programe care să automatizeze pe cât posibil verificările efectuate asupra operaţiilor informatice.

3.1.2. Responsabilitatea pentru supravegherea sarcinilor pe seturi de programe revine administratorilor

……

3.1.3. Elaborarea planului anual de activitate

……..

3.2. Managementul problemelor

3.2.1. Programele antivirus asigură protecţia aplicaţiilor

Din analiză s-a constatat neaplicarea în mod unitar a politicii de securitate IT, care a condus la infectarea cu viruşi a unor staţii de lucru din sistemul IT al entităţii publice. Astfel, echipa de auditori a verificat 5 de staţii de lucru, selectate în mod aleator, din cadrul tuturor departamentelor şi a constatat că în 2 departamente din cadrul entităţii publice configuraţia programului anti-virus pentru un număr de doua calculatoare a fost modificată pentru a întrerupe monitorizarea întregii activităţi şi verificarea e-mail-ului şi, în special, a fişierelor anexate. Acest lucru s-a realizat la cererea conducătorului departamentului, deoarece se considera că programul anti-virus are un efect negativ asupra performanţei sistemului. Urmare acestei constatări, am verificat respectivele staţii de lucru pentru a descoperi prezenţa viruşilor şi am descoperit că toate erau infectate cu viruşi.

Pentru deficienţele constatate s-a recomandat constituirea unor echipe pentru efectuarea de verificări anti-virus la nivelul tuturor staţiilor de lucru din cadrul entităţii publice, configurarea corecta în cazurile în care aceste programe au fost dezactivate, stabilirea de responsabilităţi în cazul în care acestea sunt dezactivate şi produc disfuncţii în cadrul organizaţiei.

3.2.2. Implementarea subsistemelor IT

Din analiza efectuată a rezultat că, subsistemele IT nu au fost realizate la termenele stabilite. Astfel, analiza implementării subsistemelor IT, potrivit planului anual întocmit şi aprobat, a pus în evidenta faptul ca termenele stabilite pentru implementarea programelor nu sunt respectate, iar departamentele ce ar trebui să utilizeze deja noile aplicaţii IT întâmpină deficienţe în transmiterea datelor în format electronic celorlalte departamente care au nevoie de aceste informaţii şi unde funcţionează deja de programe performante.

Resursele financiare alocate pentru implementarea acestor aplicaţii în cadrul programelor deja existente au fost utilizate pentru finalizarea unor aplicaţii şi programe deja începute şi nefinalizate.

Întârzieri în realizarea activităţilor planificate atât în cadrul departamentului IT cât şi în cadrul altor departamente, deoarece datele şi informaţiile sunt reluate şi introduse manual.

Pentru deficienţele constatate s-a recomandat analiza tuturor aplicaţiilor şi programelor începute şi nefinalizate, identificarea resurselor financiare necesare pentru finalizarea acestora, stabilirea de termene de finalizare şi urmărirea respectării acestora. Noile aplicaţii şi programe vor fi aprobate şi achiziţionate numai dacă sunt compatibile cu cele deja implementate sau aflate în faza de implementare şi numai dacă exista resursele necesare aprobate prin buget.

3.3. Funcţionalitatea Departamentului IT

3.3.1. Organizarea funcţională a Departamentului IT

…….

3.3.2. Asigurarea caracterului secret al datelor

…….

3.4. Mentenanţa echipamentelor

3.4.1. Întreţinerea calculatorului şi a echipamentelor

……

3.4.2. Instalarea şi configurarea calculatorului

…….

3.5. Utilizarea echipamentelor

3.5.1. Realizarea eficientă a operaţiilor în cadrul Departamentului IT

…….

3.5.2. Administrarea eficientă a aplicaţiilor şi programelor

…….

3.5.3. Evaluarea problemelor şi soluţionarea acestora

Din evaluare, auditorii interni au mai constatat că nu există un sistem de controale generale care să fie avute în vedere în cadrul procesului de proiectare, realizare, testare şi implementare a tuturor subsistemelor IT ce rulează pe echipamentele entităţii publice, astfel:

- Controlul datelor introduse în aplicaţii;
- Controlul pe parcursul procesării datelor şi rapoartele produse în caz de nerealizarea procesării (întreruperi, transfer);
- Controlul datelor rezultate în urma procesării, astfel încât să se asigure că aceste date sunt complete;
- Controlul privind validarea datelor transferate din alte aplicaţii;
- Controlul privind tranzacţiile efectuate.

Pentru deficienţele constatate s-a recomandat identificarea riscurilor care guvernează toate subsistemele IT, stabilirea controalelor interne care ar trebui să existe pentru ca acestea să funcţioneze corect, urmărirea controalelor interne care există şi funcţionează, identificarea şi implementarea de instrumente de control pentru controalele interne care nu sunt implementate sau nu funcţionează.

4. SECURITATEA INFORMAŢIEI

4.1. Organizarea securităţii informaţiilor

4.1.1. Elaborarea politicii privind securitatea informaţiei

……

4.1.2. Stabilirea responsabilităţilor în cadrul politicii de securitate

…….

4.1.3. Securitatea datelor asigură disponibilitatea acestora doar pentru utilizatorii autorizaţi

…….

4.2. Disponibilitatea datelor

4.2.1. Protejarea datelor împotriva viruşilor

…….

4.2.2. Asigurarea continuităţii activităţilor

……

4.2.3. Recuperarea datelor în caz de dezastru

……

4.3. Asigurarea funcţionării programelor şi aplicaţiilor

4.3.1. Asigurarea introducerii corecte a datelor

……..

4.3.2. Prelucrarea datelor

……

4.3.3. Asigurarea securităţii datelor şi documentelor

Din analiza efectuată s-a constatat că la nivelul Departamentului IT nu se respectă procedurile specifice privind asigurarea securităţii reţelelor, astfel:

- la nivelul departamentului IT au fost întocmite hărţi privind infrastructura reţelelor IT, însă una din cele 3 hărţi cuprinse în eşantion nu fusese actualizată, astfel încât aplicaţiile copiate pe un număr de 4 sisteme nu au fost protejate prin intermediul programelor antivirus. De asemenea, aplicaţiile contabile au fost copiate de pe unul din calculatoarele existente, fără a se proceda la instalarea acestora de către personalul specializat din cadrul departamentului IT, ocazie cu care nu au putut fi asigurata integritatea tuturor modulelor.

- deşi există o clasificare a sistemelor hardware, în funcţie de importanţa fiecărei categorii în parte, în ceea ce priveşte aplicaţiile informatice, nu a fost avută în vedere o prioritizare a importanţei acestora în vederea alocării corespunzătoare a resurselor de securitate.

- la nivelul entităţii s-a procedat la identificarea şi înlăturarea celor mai critice vulnerabilităţi ale reţelelor, însă nu a fost avut în vedere un sistem de management al vulnerabilităţilor, la cel mai profund nivel, actualizat, care să permită identificarea precisă şi cuprinzătoare a ultimilor vulnerabilităţi ale sistemului sau a greşelilor de configurare, bazându-se pe informaţii precise şi configuraţii de sistem şi de reţea adecvate.

- administratorii de sistem au procedat la întocmirea de rapoarte care detaliază nivelul critic al vulnerabilităţilor şi au furnizat soluţii de remediere însă informaţiile nu au fost strânse, adaptate şi prezentate acelor persoane care decid asupra situaţiei securităţii în cadrul entităţii publice. Astfel, conducerea entităţii nu a avut la dispoziţie informaţiile necesare cuantificării efortului necesar pentru asigurarea securităţii reţelelor.

Pentru remedierea deficienţelor constatate au fost formulate următoarele recomandări:

1. Implementarea procedurilor operaţionale de lucru cu elemente care să asigure actualizarea în timp util a situaţiilor privind reţelele IT; Tratarea securităţii reţelelor ca pe un proces continuu, astfel încât schimbările în cadrul utilizatorilor, echipamentelor sau aplicaţiilor să se realizeze evitând expunerile la riscuri;

2. Prioritizare şi a aplicaţiilor informatice, în funcţie de importanţa acestora, în vederea alocării corespunzătoare a măsurilor de securitate, având în vedere că acestea necesită de cele mai multe ori resurse considerabile, care trebuie să fie direct proporţionale cu valoarea datelor sau echipamentelor de protejat;

3. Implementarea unui sistem de management al vulnerabilităţilor, care să identifice precis, cuprinzător şi actualizat la zi, ultimele vulnerabilităţi ale sistemului sau a greşelilor de configurare.

4. Toate rapoartele întocmite în urma identificării şi soluţionării vulnerabilităţilor reţelelor să fie corelate şi aduse la cunoştinţa conducerii entităţii publice.

4.4. Implementarea instrumentelor de control

4.4.1. Accesul la aplicaţie este oferit pe baza necesităţilor utilizatorului

Posturile de lucru dotate cu computer nu sunt evidenţiate la nivelul Departamentului IT, neasigurându-se o intervenţie promptă şi rapidă, iar securitatea datelor şi informaţiilor nu este asigurată pe baza unui sistem de autorizare a accesului şi unui sistem adecvat de parole.

La nivelul entităţii au fost elaborate harţi privind reţele informatice existente. În acest sens, au fost stabilite locaţiile serverelor, sistemelor desktop, sistemelor laptop, a routerelor, a punctelor de acces, a imprimantelor şi a celorlalte dispozitive conectate la reţea. Aceste hărţi au stat la baza elaborării sistemului de management al securităţii reţelelor din cadrul entităţii.

Analiza celor 3 reţele care a constituit eşantionul, a pus în evidenţă faptul că pentru două reţele hărţile erau corespunzătoare, însă referitor la reţeaua care deservea direcţia generală buget-finanţe s-a constatat că, au fost achiziţionate şi conectate 4 noi computere şi o imprimantă de reţea, toate deservite prin intermediul unui nou router, care nu au fost consemnate în cadrul hărţii.

De asemenea, pe cele 3 computere au fost copiate aplicaţiile contabile utilizate la nivelul direcţiei, fără a fi luate măsuri pentru asigurarea securităţii datelor şi informaţiilor prin controlarea accesului şi implementarea de programe antivirus adecvate.

La nivelul departamentului IT există o clasificare a sistemelor hardware, în funcţie de importanţa fiecărei categorii pentru buna desfăşurare a activităţii în cadrul entităţii. În acest sens, dispozitivele din reţea au fost grupate în funcţie de priorităţi, de la sisteme cu importanţă redusă, cum sunt sistemele de test sau care sunt folosite independent pentru asigurarea funcţiilor mai puţin importante ale entităţii şi sistemele de importanţă medie, cum sunt sistemele laptop folosite de unii angajaţi în cadrul delegaţiilor sau pentru lucrul acasă, la sisteme de importanţă majoră pentru asigurarea continuităţii activităţilor organizaţiei, cum ar fi sistemele care gestionează bazele de date, serverele care deservesc compartimentele cheie ale entităţii (tranzacţii, operaţiuni financiare etc.).

Deşi există o clasificare a sistemelor hardware, în funcţie de importanţa fiecărei categorii în parte, în ceea ce priveşte aplicaţiile informatice, nu a fost avută în vedere o prioritizare a importanţei acestora în vederea alocării corespunzătoare a resurselor de securitate. Ex. - aplicaţia informatică utilizată la nivelul serviciului secretariat pentru urmărirea circuitului documentelor beneficiază de aceleaşi măsuri de securitate ca şi sistemul integrat privind conducerea organizaţiei.

Administratorii de reţea au procedat la întocmirea de rapoarte prin care detaliază nivelul vulnerabilităţilor şi furnizează soluţii de remediere, însă informaţiile nu sunt adaptate şi prezentate persoanelor cu responsabilităţi decizionale asupra securităţii informaţionale.

Recomandările formulate au făcut referire la prioritizarea aplicaţiilor informatice, în funcţie de importanţa acestora, în vederea alocării corespunzătoare a măsurilor de securitate şi tratarea securităţii reţelelor ca pe un proces continuu. Implementarea unui sistem de management al vulnerabilităţilor, care să identifice vulnerabilităţile şi greşelile de configurare şi să dispună măsurile operative de soluţionare. Rapoartele întocmite în urma identificării şi soluţionării vulnerabilităţilor reţelelor să fie corelate şi aduse la cunoştinţa conducerii organizaţiei.

4.4.2. Introducerea instrumentelor de control fizic asupra echipamentelor IT al aplicaţiilor

Controalele fizice nu sunt implementate in mod eficient pentru a asigura securitatea echipamentelor.

Din examinarea efectuata si observarea la fata locului s-a constatat unele disfuncţii legate de accesul necontrolat la cele trei locaţii selectate atât a persoanelor din cadrul altor departamente cât şi a altor persoane din afara entităţii publice;

Totodată, deşi au fost instalate camere de supraveghere, acestea nu sunt permanent monitorizate. Deseori, camerele în care sunt localizate servere-le sunt lăsate descuiate şi nesupravegheate, deşi sunt echipate cu încuietori adecvate;

La scoaterea echipamentelor din cadrul organizaţiei nu există obligativitatea prezentării unei autorizaţii scrise.

*Pentru deficienţele constatate s-a recomandat introducerea de instrumente de control adecvate astfel incit orice acces la echipamentele sau datele si informaţiile organizaţiei sa fie limitat, sau in cazurile in care acesta este permis sa fie supravegheat in totalitat*e.

4.5. Securitatea reţelei

4.5.1. Monitorizarea securităţii reţelelor

……

4.6. Gestionarea parolelor

4.6.1. Utilizatori au parole de acces individuale

Din verificarea efectuata a rezultat că nu există o securitate a sistemului informatic şi un responsabil cu administrarea acestui sistem.

Recomandarea s-a referit la stabilirea unei persoane care să aibă în responsabilitate atribuţii şi competenţe de verificare a schimbării periodice a parolelor de acces.

4.6.2. Schimbarea periodică a parolelor

……..

4.6.3. Protejarea parolelor

……

4.6.4. Persoanele autorizate au acces la sistemul de operare

……

4.7. Securitatea logică

4.7.1. Asigurarea securităţii funcţionării programelor şi aplicaţiilor

……

5. PROIECTAREA ŞI TESTAREA PROGRAMELOR ŞI APLICAŢIILOR

5.1. Proiectarea şi elaborarea programelor şi aplicaţiilor

5.1.1. Achiziţia programelor informatice

…….

5.1.2. Proiectarea programului informatic

…….

5.1.3. Elaborarea programului informatic

…….

5.2. Testarea şi implementarea programelor şi aplicaţiilor

5.2.1. Testarea programului şi aplicaţiei

……

5.2.2. Asigurarea corectitudini rezultatelor

Organizarea datelor şi stocarea acestora nu asigură o utilizare şi exploatare eficientă a acestora. Accesul la o înregistrare din fişierul de date se obţine prin parcurgerea înregistrărilor fişierului în secvenţa în care au fost stocate sau pe bază unui cod de identificare care să permită regăsirea rapidă a înregistrării.

Accesul direct se obţine prin indexarea fişierelor, adică prin crearea unor tabele de indecşi care pentru fiecare valoare atributului care permite identificarea în mod unic a unei înregistrări din fişier.

Organizarea datelor în fişierele de date prezintă următoarele disfuncţii:

- redundanţă mare – stocarea datelor în mai multe fişiere;
- acces dificil la date – exploatarea multiutilizator a datelor necesită operaţii suplimentare de sortare, fuziune, ventilare;
- izolarea datelor – imposibilitatea realizării de programe pe calculator care să acceseze datele într-o manieră globală;

- actualizarea datelor prin adăugare, modificare, ştergere generează erori atunci când mai mulţi utilizatori doresc să modifice simultan aceleaşi date;

- dependenţa programelor faţă de date – modificările din structura datelor obligă la efectuarea de corecturi în programele de calculator;

- fiecare dată este descrisă independent în toate fişierele în care apar – dacă într-un fişier se modifică formatul şi valoarea unei date, acea modificare nu se transmite automat, pentru aceeaşi dată, în toate fişierele de date.

Pentru remedierea acestor deficiente s-a recomandat organizarea datelor în baze de date, respectiv un fişier format din înregistrări, care conţin câmpuri şi operaţii de căutare, sortare sau recombinare. Pentru aceasta este necesar realizarea următoarelor: definirea, structurarea, ordonarea şi gruparea datelor în colecţii de date omogene; stabilirea legăturilor între date, între elementele unei colecţii de date şi între colecţiile de date, după o ierarhie bine precizată, precum şi memorarea datelor pe un suport informaţional prelucrabil într-un sistem de calcul.

6. ELABORAREA ŞI IMPLEMENTAREA PROIECTELOR IT

6.1. Dezvoltarea proiectelor IT

6.1.1. Iniţierea şi elaborarea proiectelor IT

……

6.2. Implementarea şi funcţionarea programelor şi aplicaţiilor

6.2.1. Reproiectarea soluţiilor IT pentru programe şi aplicaţii

…….

6.2.2. Întreţinerea aplicaţiilor garantează funcţionarea proceselor la parametri optimi

Din evaluarea realizată s-a constatat utilizarea în cadrul entităţii publice a unor programe software fără licenţă. Astfel, cu toate că entitatea publică a achiziţionat licenţe pentru pachetul de programe Lotus, s-au constatat că în cadrul unor departamente se folosesc programe aferente pachetului Microsoft Office fără ca pentru acestea entitatea publică să fi achiziţionat licenţe. Practic salariaţii au instalat programe utilizând CD-uri piratate.

La nivelul sistemului IT al entităţii publice s-a constatat inexistenţa controalelor de sistem ce alertează administratorul în cazul utilizării de soft-uri pentru care nu s-au achiziţionat licenţe.

Pentru remedierea deficienţelor constatate s-a recomandat inventarierea tuturor staţiilor de lucru pentru a stabili situaţia reală privind utilizarea programelor fără licenţă şi dezinstalarea tuturor programelor nelicenţiate din pachetul Microsoft Office. Totodată, s-a recomandat şi realizarea unei analize complexe în urma căreia managementul entităţii publice să decidă asupra oportunităţii schimbării programelor existente şi achiziţionarea unui număr adecvat de licenţe Microsoft Office.

7. PROIECTAREA, IMPLEMENTAREA ŞI MENŢINEREA ÎN FUNCŢIE A UNEI REŢELE

7.1. Proiectarea, instalarea şi administrarea reţelei de calculatoare

7.1.1. Asigurarea bunei funcţionări a sistemelor bazate pe existenţa şi funcţionarea reţelei de calculatoare

……..

7.1.2. Administrarea serverelor

…….

7.2. Interconectarea şi securitatea reţelei

7.2.1. Interconectarea reţelelor

……

7.2.2. Proiectarea şi asigurarea securităţii reţelei

Din evaluare s-a constatat neutilizarea unui singur nume de utilizator şi unei singure parole pentru accesul la sistemul IT, în condiţiile în care majoritatea salariaţilor din cadrul entităţii publice, prin natura sarcinilor de serviciu, trebuie să acceseze mai multe subsisteme IT care folosesc nume de utilizator şi parole diferite. Sistemul IT este conceput astfel încât pentru accesul la fiecare subsistem IT trebuiesc folosite: nume de utilizator şi parolă diferite, în loc să se folosească acelaşi nume de utilizator şi parolă indiferent de subsistemul IT la care se conectează angajatul.

Pentru aceasta s-a recomandat realizarea unui proces de reenginering la nivelul sistemului IT din cadrul entităţii publice, astfel încât salariaţii să poată accesa subsistemele IT de care au nevoie utilizând un singur nume de utilizator şi o singură parolă;

III. CONCLUZII

Echipa de auditori pe baza testărilor şi analizelor efectuate evaluează **Activitatea de stabilire şi colectare a impozitelor şi taxelor locale** din entitatea auditată conform grilei:

Nr.. Crt.	OBIECTIVUL	APRECIERE		
		FUNCŢIONAL	DE ÎMBUNĂTĂŢIT	CRITIC
1.	Strategia şi planificarea sistemelor informatice;		X	
2.	Organizarea şi funcţionarea departamentului IT;			X
3.	Operaţii ale sistemului informatic;		X	
4.	Securitatea informaţiilor;		X	
5.	Testarea programelor şi aplicaţiilor;	X		
6.	Elaborarea şi implementarea proiectelor IT;		X	
7.	Proiectarea şi menţinerea în funcţiune a unei reţele.			X

Precizăm, faptul că constatările prezentate au la bază probe de audit obţinute pe baza testelor efectuate consemnate în documentele de lucru întocmite de către echipa de auditori şi însuşite de către factorii de management ai entităţii. Aceste evaluări au la bază discuţiile care au avut loc cu privire la recomandările auditorilor în şedinţele de închidere şi conciliere ale misiunii, apreciate de către participanţii la aceste şedinţe, ca fiind realiste şi fezabile, şi materializate în minutele şedinţelor de închidere şi conciliere.

Considerăm că rezultatele evaluării auditorilor interni privind **Activitatea privind tehnologia informaţiei** se înscrie în parametri normali pentru această perioadă de introducere a auditului intern în entităţi. De asemenea, prin implementarea recomandărilor echipei de auditori activitatea de stabilire şi colectare a impozitelor şi taxelor locale va cunoaşte o ameliorare semnificativă.

*Structura auditată are obligaţia să întocmească **Programul de acţiune şi Calendarul implementării recomandărilor** şi să raporteze periodic echipei de auditori stadiul implementării acestora.*

Prezentul Raport de audit intern a fost întocmit în baza Tematicii în detaliu a obiectelor auditabile selectate, a Programului de audit şi a Programului de intervenţie la faţa locului, a constatărilor efectuate în timpul etapei de colectării şi prelucrării informaţiilor şi în timpul Intervenţie la fata locului. Toate constatările efectuate au la bază probe de audit realizate prin teste, interviuri, liste de control, note de relaţii şi în urma analizei şi interpretării acestora s-au elaborat FIAP-uri şi FCRI-uri care au condus la concluziile cuprinse în Raportul de audit intern.

Data: 28.10.2009

Auditori interni,
Popescu Sorin
Radu George

Supervizor,
Dumitru Daniel

Notă:

Proiectul de raport de audit intern concretizează activitatea auditorilor interni prin prezentarea cadrului general de desfăşurare a activităţii entităţii, obiectivelor, constatărilor, concluziilor şi recomandărilor obţinute în urma misiunii realizate, cât şi aria şi metodologia de audit, tehnicile de colectare şi de analiză a dovezilor de audit utilizate.

La elaborarea Proiectului de raportul de audit intern, auditorul foloseşte dovezile de audit raportate în Fişele de Identificare şi Analiza a Problemelor şi în Formularul de Constatare şi Raportare a Iregularităţilor şi în celelalte documente de lucru.

S I N T E Z A

RAPORTULUI DE AUDIT INTERN

I. INTRODUCERE

Misiunea de audit intern privind *Activitatea de tehnologia informaţiei* din cadrul entităţii publice s-a desfăşurat conform prevederilor Legii nr. 672/2002 privind auditul public intern, cu modificările şi completările ulterioare, OMFP nr. 38/2003 de aprobare a Normelor generale privind exercitarea activităţii de audit intern, a Normelor specifice proprii de audit intern aprobate de conducere şi a Planului de audit intern pe anul 2009, şi a fost realizata de:

Popescu Sorin - auditor superior, coordonator echipă
Radu George - auditor superior
Dumitru Daniel - supervizor.

II. CONCLUZII

Nr.. Crt.	OBIECTIVUL	APRECIERE		
		FUNCŢIONAL	DE ÎMBUNĂTĂŢIT	CRITIC
1.	**Strategia şi planificarea sistemelor informatice;**		X	
2.	**Organizarea şi funcţionarea departamentului IT;**			X
3.	**Operaţii ale sistemului informatic;**		X	
4.	**Securitatea informaţiilor;**		X	
5.	**Testarea programelor şi aplicaţiilor;**	X		
6.	**Elaborarea şi implementarea proiectelor IT;**		X	
7.	**Proiectarea şi menţinerea în funcţiune a unei reţele.**			X

III. CONSTATĂRI şi RECOMANDĂRI

Principalele constatări şi recomandări rezultate în urma evaluării:

1. Constatări: Nerealizarea în termen a procedurilor de achiziţie şi implementare a programelor şi aplicaţiilor informatice.
Recomandare: Reanalizarea atribuţiilor Comisiei de planificare strategică în domeniul IT şi redefinirea acestora astfel încât să poată realiza şi monitorizarea implementării proiectelor informatice şi informarea periodică a conducerii asupra realizării acestora.

2. Constatări: La elaborarea strategiei, la nivelul structurii funcţionale, nu s-au avut în vedere evaluarea situaţiei actuale pe baza analizei diagnostic, identificarea punctelor tari şi a punctelor slabe ale entităţii şi fundamentarea variantelor strategice
Recomandări: Pregătirea profesională anticipată a personalului implicat în elaborarea strategiei, de către managementul responsabil cu aceasta. Reanalizarea strategiei definite la nivelul structurii funcţionale în conformitate cu procedura operaţională aprobată şi actualizarea acesteia astfel încât implementarea sa să contribuie la realizarea unui management modern in domeniul de activitate şi la atingerea obiectivelor strategice ale organizaţiei. În acelaşi timp s-a mai recomandat îmbunătăţirea procedurilor operaţionale de lucru privind sistemul de fundamentare a necesarului de resurse pentru elaborarea strategiei.

3. Constatări: Obiectivelor strategice nu asigură acoperirea domeniului de activitate al structurii funcţionale şi nu contribuie la asigurarea realizării mandatului organizaţiei. Acestea reprezintă exprimările cantitative şi calitative ale scopului pentru care există şi funcţionează organizaţia.
Recomandări: Pentru deficienţele constatate s-a recomandat evaluarea performanţelor actuale ale sistemului de organizare şi conducere a activităţilor desfăşurate în cadrul structurii funcţionale, ţinând cont de influenţa factorilor de mediu, interni şi externi, în vederea redefinirii obiectivelor strategice. Implicarea managementului pentru ca obiectivele strategice redefinite să întrunească caracteristicile de a fi realiste, mobilizatoare, stimulative şi să poată fi înţelese de salariaţi, stabilite de metodologie.

4. Constatări: Resursele nu sunt fundamentate corect în vederea implementării planului anual de activitate. Activităţile considerate prioritare ale planului anual nu au fost realizate sau implementate în totalitate, în mod corespunzător, deoarece nu au fost reanalizate şi repartizate atribuţiile în cadrul compartimentelor în corelaţie cu noile obiective şi activităţi stabilite în cadrul planului. Aceasta a însemnat că, în unele cazuri, obiectivele şi activităţile deşi erau cunoscute de personal, acesta nu avea competenţa necesară, în special a celor care erau realizate în colaborare cu alte structuri funcţionale, ceea ce a necesitat solicitarea unor competenţe pentru realizarea acestora, proces care a îngreunat implementarea obiectivelor şi realizarea activităţilor. Activităţile nu au fost comunicate salariaţilor, respectiv obiectivele individuale au rămas aceleaşi, în condiţiile în care obiectivele cuprinse în planul compartimentului au fost cu totul altele. Aceasta a însemnat stabilirea măsurilor în cursul anului, instruirea, sub diferite forme, a personalului pentru înţelegerea acestora şi stabilirea priorităţilor de implementare, ceea ce a condus la întârzieri în atingerea unor obiective ale planului.
Recomandări: Dezvoltarea unui sistem de instruire şi pregătire a salariaţilor astfel încât metodologia specifică domeniului de activitate, normativă şi procedurală, să fie aplicată corespunzător pentru dezvoltarea şi implementarea planurilor anuale. În baza planurilor elaborate să se identifice toate atribuţiile necesare pentru atingerea obiectivelor stabilite, iar acestea să fie repartizate corespunzător în cadrul compartimentelor. Promovarea dezvoltării resurselor umane pentru a obţine competenţele necesare creşterii economice în condiţiile în care au loc reduceri de personal, precum şi evaluarea cuprinzătoare a resurselor necesare implementării planurilor anuale de activitate şi monitorizarea eficientă pentru a se asigura încadrarea în limitele stabilite.

5. Constatări: Departamente din cadrul entităţii nu dispun de subsisteme IT specifice activităţilor care se desfăşoară în cadrul acestora.
Recomandare: Pentru deficienţele constatate s-a recomandat coroborarea atribuţiilor prezentate prin proceduri cu cele stabilite prin fişele posturilor şi inventarierea stadiului implementării subsistemelor IT la nivelul departamentelor entităţii publice şi stabilirea necesităţilor IT care trebuie incluse în strategia IT.

6. Constatări: Atribuţiile stabilite pentru posturile din cadrul Departamentului IT nu asigură întotdeauna aria de competenţă privind realizarea activităţilor şi acţiunilor repartizate.
Recomandare: Conştientizarea managementului responsabil cu procesul de stabilire şi definire a atribuţiilor prin informări şi consilieri pentru clarificarea modalităţilor practice de definire a unei atribuţii sau unui set de atribuţii pentru asigurarea ariei de competenţă necesară pentru realizarea activităţilor.

7. Constatări: Activităţile nu sunt definite omogen în cadrul structurii funcţionale, iar stabilirea complexităţii acestora nu se realizează în funcţie de nivelurile de calificare ale posturilor existente.
Recomandări: Realizarea unei analize riguroase a sarcinilor şi responsabilităţilor fiecărui angajat, care să stea la baza oricărei iniţiative de organizare a activităţii. Constituirea unei echipe, pe baza deciziei managementului general, care să analizeze şi să redefinească activităţile şi acţiunile realizate în cadrul compartimentelor şi serviciilor, astfel încât să se asigure că obiectivele vor fi realizate în totalitate.

8. Constatări: Organigrama ca document prin care se relevă grafic structura organizaţiei şi substructurile acesteia nu pune în evidenţă organizarea şi funcţionarea departamentului. Compartimentele aflate în subordinea departamentului nu sunt nominalizate în totalitate în cadrul organigramei şi nu este precizat nici nivelul de subordonare al departamentului în cadrul organizaţiei. Organigrama nu furnizează o înţelegere a raporturilor de subordonare şi de evitare a suprapunerilor de competenţe. Astfel, cu privire la raporturile de subordonare, potrivit organigramei, **Recomandare:** Pentru remedierea deficienţelor constatate s-a recomandat analiza actului normativ de organizare şi funcţionare a organizaţiei şi urmărirea atribuţiilor definite departamentului astfel încât să acopere în totalitate activităţile desfăşurate.

9. Constatări: Persoanele responsabilizate în posturile de conducere nu au coordonat în nici un fel activităţile care erau realizate zilnic de către salariaţi, nu au îndrumat în nici un fel salariaţii cu privire la modul în care în care să realizeze activităţile şi nici nu au realizat o monitorizare cu privire la modul de realizare a acestora. Salariaţii, în baza sarcinilor stabilite prin fişa postului, au realizat activităţile în funcţie de cunoştinţele şi aptitudinile pe care le deţineau.
Recomandare: Desfăşurarea procesului de selecţie şi recrutarea în vederea ocupării posturilor de conducere existente la nivelul departamentului IT. În acelaşi timp se va urmări dacă persoanele selectate deţin abilităţile şi aptitudinile manageriale necesare realizării activităţilor specifice celor două servicii şi dacă au pregătirea de bază, de nivel superior, în domeniul IT.

10. Constatare: Riscurile nu sunt identificate şi gestionate la nivelul departamentului şi nu este condus Registrul riscurilor cuprinzând riscurile potenţiale şi istoricul acestora, precum şi instrumentele de control intern implementate pentru limitarea acestora.
Recomandare: Elaborarea mecanismelor procedurale şi metodologice privind identificarea riscurilor şi gestionarea acestora, evaluarea riscurilor identificate şi diferenţierea acestora în riscuri inerente şi riscuri acceptabile, precum şi implementarea de instrumente de control pentru riscurile inerente, astfel încât manifestarea acestora să fie limitată şi nivelul acestora să devină unul acceptabil.

11. Constatare: Sistemul de control intern definit la nivelul organizaţiei nu cuprinde toate activităţile de control ce trebuie alocate în vederea atingerii obiectivelor.
Recomandare: Pentru remedierea acestor deficienţe s-a constatat stabilirea controalelor interne aferente riscurilor identificate şi determinarea gradului de funcţionalitate al acestora şi proiectarea de instrumente sau măsuri de introducere de controale interne, fie individuale, fie în combinaţie cu alte controale, capabile să prevină, detecteze şi să corecteze în mod eficient denaturările semnificative.

12. Constatare: La nivelul departamentului nu este organizat şi nu se conduce registrul riscurilor. Riscurile cu care se confruntă organizaţia nu sunt identificate şi nu sunt monitorizate în vederea stăpânirii şi menţinerii lor la un nivel acceptabil.
Recomandare: Pentru soluţionarea acestei deficienţe s-a recomandat instituirea şi conducerea Registrului riscurilor la nivelul organizaţiei.

13. Constatare: Studiile de specialitate aferente unui post sunt definite în cadrul fişei postului fără a se ţine cont de scopul postului şi cunoştinţele de bază necesare pentru realizarea atribuţiilor alocate acestuia.
Recomandare: Pentru aceasta s-a recomandat analiza sarcinilor şi atribuţiilor definite în fişele posturilor şi stabilirea acestora în funcţie de caracteristicile postului, respectiv nivelul postului şi urmărirea definirii aceluiaşi gen de sarcini şi atribuţii numai dacă posturile sunt de acelaşi nivel.

13. Constatare: Atribuţiile definite în sarcina compartimentelor funcţionale nu sunt întotdeauna conforme şi nu asigură competenţa de realizare a activităţilor şi acţiunilor, acestea fiind definite în multe cazuri la modul general, nu indică, prin modul de formulare, o acţiune, nu asigura un conţinut clar, fiind sub forma unei relaţii funcţionale sau având caracter de activitate sau sarcină. Nu sunt definite în cadrul ROF-ului la capitolul privind departamentul IT relaţiile cu celelalte structuri funcţionale cu care are sau ar trebui să aibă relaţii funcţionale, respectiv nu este definită relaţia funcţională care reglementează asigurarea conformităţii informaţiilor cu privire la asistarea utilizatorilor în realizarea activităţilor de introducere a datelor şi informaţiilor în cadrul aplicaţiilor şi programelor derulate la nivelul celorlalte departamente funcţionale din cadrul organizaţiei, precum şi cu privire la asistarea în utilizarea echipamentelor din dotare.
Recomandare: În vederea remedierii acestor deficienţe s-a recomandat identificarea şi definirea corectă în cadrul documentului de organizare şi funcţionare, a atribuţiilor specifice departamentului, a relaţiilor funcţionale pe care compartimentul la are cu alte structuri funcţionale din cadrul organizaţiei.

14. Constatare: Existenţa unor controale interne slabe privind managementul operaţiunilor IT, reflectate în disfuncţii legate de gestionarea acestora.
Recomandare: Implementarea unei aplicaţii care să monitorizeze alocarea şi utilizarea resurselor în funcţie de gradul de complexitate al operaţiilor efectuate. Urmărirea în permanenţă a echilibrului între necesităţile IT şi resursele alocate acestor scopuri. Mediile sau locaţiile de stocare să fie protejate împotriva deteriorării sau accesului neautorizat. Constituirea în cadrul departamentului IT a unui colectiv specializat în raportarea şi rezolvarea operativă a problemelor de ordin tehnic, care să asigure şi acordarea suportului tehnic de specialitate către utilizatori, fie prin linii telefonice dedicate, fie prin e-mail sau deplasări ale echipelor specializate.

15. Constatare: Neaplicarea în mod unitar a politicii de securitate IT, care a condus la infectarea cu viruşi a unor staţii de lucru din sistemul IT al entităţii publice. Astfel, echipa de auditori a verificat 5 de staţii de lucru, selectate în mod aleator, din cadrul tuturor departamentelor şi a constatat că în 2 departamente din cadrul entităţii publice configuraţia programului anti-virus pentru un număr de doua calculatoare a fost modificată pentru a întrerupe monitorizarea întregii activităţi şi verificarea e-mail-ului şi, în special, a fişierelor anexate. Acest lucru s-a realizat la cererea conducătorului departamentului, deoarece se considera că programul anti-virus are un efect negativ asupra performanţei sistemului.
Recomandare: Pentru deficienţele constatate s-a recomandat constituirea unor echipe pentru efectuarea de verificări anti-virus la nivelul tuturor staţiilor de lucru din cadrul entităţii publice, configurarea corecta în cazurile în care aceste programe au fost dezactivate, stabilirea de responsabilităţi în cazul în care acestea sunt dezactivate şi produc disfuncţii în cadrul organizaţiei.

16. Constatare: Subsistemele IT nu au fost realizate la termenele stabilite. Astfel, analiza implementării subsistemelor IT, potrivit planului anual întocmit şi aprobat, a pus în evidenta faptul ca termenele stabilite pentru implementarea programelor nu sunt respectate, iar departamentele ce ar trebui să utilizeze deja noile aplicaţii IT întâmpină deficienţe în transmiterea datelor în format electronic celorlalte departamente care au nevoie de aceste informaţii şi unde funcţionează deja de programe performante.
Recomandare: Analiza tuturor aplicaţiilor şi programelor începute şi nefinalizate, identificarea resurselor financiare necesare pentru finalizarea acestora, stabilirea de termene de finalizare şi urmărirea respectării acestora. Noile aplicaţii şi programe vor fi aprobate şi achiziţionate numai dacă sunt compatibile cu cele deja implementate sau aflate în faza de implementare şi numai dacă exista resursele necesare aprobate prin buget.

17. Constatare: Nu există un sistem de controale generale care să fie avute în vedere în cadrul procesului de proiectare, realizare, testare şi implementare a tuturor subsistemelor IT ce rulează pe echipamentele entităţii publice.
Recomandare: Pentru deficienţele constatate s-a recomandat identificarea riscurilor care guvernează toate subsistemele IT, stabilirea controalelor interne care ar trebui să existe pentru ca acestea să funcţioneze corect, urmărirea controalelor interne care există şi funcţionează, identificarea şi implementarea de instrumente de control pentru controalele interne care nu sunt implementate sau nu funcţionează.

18. Constatare: Din analiza efectuată s-a constatat că la nivelul Departamentului IT nu se respectă procedurile specifice privind asigurarea securităţii reţelelor.
Recomandare: Implementarea procedurilor operaţionale de lucru cu elemente care să asigure actualizarea în timp util a situaţiilor privind reţelele IT. Tratarea securităţii reţelelor ca pe un proces continuu, astfel încât schimbările în cadrul utilizatorilor, echipamentelor sau aplicaţiilor să se realizeze evitând expunerile la riscuri. Implementarea unui sistem de management al vulnerabilităţilor, care să identifice precis, cuprinzător şi actualizat la zi, ultimele vulnerabilităţi ale sistemului sau a greşelilor de configurare.

19. Constatare: Posturile de lucru dotate cu computer nu sunt evidenţiate la nivelul Departamentului IT, neasigurându-se o intervenţie promptă şi rapidă, iar securitatea datelor şi informaţiilor nu este asigurată pe baza unui sistem de autorizare a accesului şi unui sistem adecvat de parole. La nivelul entităţii au fost elaborate harţi privind reţele informatice existente. În acest sens, au fost stabilite locaţiile serverelor, sistemelor desktop, sistemelor laptop, a routerelor, a punctelor de acces, a imprimantelor şi a celorlalte dispozitive conectate la reţea. Aceste hărţi au stat la baza elaborării sistemului de management al securităţii reţelelor din cadrul entităţii.
Recomandare: Prioritizarea aplicaţiilor informatice, în funcţie de importanţa acestora, în vederea alocării corespunzătoare a măsurilor de securitate şi tratarea securităţii reţelelor ca pe un proces continuu. Implementarea unui sistem de management al vulnerabilităţilor, care să identifice vulnerabilităţile şi

greşelile de configurare şi să dispună măsurile operative de soluţionare. Rapoartele întocmite în urma identificării şi soluţionării vulnerabilităţilor reţelelor să fie corelate şi aduse la cunoştinţa conducerii organizaţiei.

20. Constatări: Controalele fizice nu sunt implementate in mod eficient pentru a asigura securitatea echipamentelor.
Recomandare: Introducerea de instrumente de control adecvate astfel incit orice acces la echipamentele sau datele si informaţiile organizaţiei sa fie limitat, sau in cazurile in care acesta este permis sa fie supravegheat in totalitate.

21. Constatări: Inexistenţa unui sistem de stabilire de către fiecare utilizator a parolelor şi a unui responsabil cu verificarea schimbării periodice a parolelor de acces.
Recomandare: Schimbarea sistematică a parolelor de acces de către utilizatorii sistemului informatic, precum şi stabilirea unei persoane care să aibă în responsabilitate atribuţii şi competenţe de verificare a schimbării periodice a parolelor de acces.

22. Constatare: Organizarea datelor şi stocarea acestora nu asigură o utilizare şi exploatare eficientă a acestora. Accesul la o înregistrare din fişierul de date se obţine prin parcurgerea înregistrărilor fişierului în secvenţa în care au fost stocate sau pe bază unui cod de identificare care să permită regăsirea rapidă a înregistrării.
Recomandare: Organizarea datelor în baze de date, respectiv un fişier format din înregistrări, care conţin câmpuri şi operaţii de căutare, sortare sau recombinare. Pentru aceasta este necesar realizarea următoarelor: definirea, structurarea, ordonarea şi gruparea datelor în colecţii de date omogene; stabilirea legăturilor între date, între elementele unei colecţii de date şi între colecţiile de date, după o ierarhie bine precizată, precum şi memorarea datelor pe un suport informaţional prelucrabil într-un sistem de calcul.

23. Constatări: Utilizarea în cadrul entităţii publice a unor programe software fără licenţă. Astfel, cu toate că entitatea publică a achiziţionat licenţe pentru pachetul de programe Lotus, s-au constatat că în cadrul unor departamente se folosesc programe aferente pachetului Microsoft Office fără ca pentru acestea entitatea publică să fi achiziţionat licenţe. Practic salariaţii au instalat programe utilizând CD-uri piratate.
Recomandare: Inventarierea tuturor staţiilor de lucru pentru a stabili situaţia reală privind utilizarea programelor fără licenţă şi dezinstalarea tuturor programelor nelicenţiate din pachetul Microsoft Office. Totodată, s-a recomandat şi realizarea unei analize complexe în urma căreia managementul entităţii publice să decidă asupra oportunităţii schimbării programelor existente şi achiziţionarea unui număr adecvat de licenţe Microsoft Office.

24. Constatare: Neutilizarea unui singur nume de utilizator şi unei singure parole pentru accesul la sistemul IT, în condiţiile în care majoritatea salariaţilor din cadrul entităţii publice, prin natura sarcinilor de serviciu, trebuie să acceseze mai multe subsisteme IT care folosesc nume de utilizator şi parole diferite. Sistemul IT este conceput astfel încât pentru accesul la fiecare subsistem IT trebuiesc folosite: nume de utilizator şi parolă diferite, în loc să se folosească acelaşi nume de utilizator şi parolă indiferent de subsistemul IT la care se conectează angajatul.
Recomandare: Realizarea unui proces de reenginering la nivelul sistemului IT din cadrul entităţii publice, astfel încât salariaţii să poată accesa subsistemele IT de care au nevoie utilizând un singur nume de utilizator şi o singură parolă;

In încheiere, consideram necesara implicarea colectivului în analiza şi implementarea recomandărilor propuse şi a acţiunilor discutate şi informarea sistematica asupra evoluţiei acestora, atât a managementului general, cat şi a echipei de auditori interni.

Auditori interni,
Popescu Sorin
Radu George

Supervizor,
Dumitru Daniel

Entitatea Publică
Serviciul de Audit Intern

FIŞA DE URMĂRIRE A RECOMANDĂRILOR

Misiunea de audit: Tehnologia informaţiei
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 10.09.2009
Avizat: Dumitru Daniel Data: 10.09.2009

RECOMANDAREA		***Serviciul de Audit Intern***			***Sfârşit de lună***
		Misiunea de audit intern: Stabilirea şi colectarea impozitelor şi taxelor locale			***Raport de audit intern nr. 234532/ 14.07.2010***
Nr. crt.	***Recomandarea***	***Implementat***	***Parţial implementat***	***Neimplementat***	***Data planificată/ Data implementării***
1	Reanalizarea atribuţiilor Comisiei de planificare strategică în domeniul IT şi redefinirea acestora astfel încât să poată realiza şi monitorizarea implementării proiectelor informatice şi informarea periodică a conducerii asupra realizării acestora.	*X*			31.12.2009
2	Pregătirea profesională anticipată a personalului implicat în elaborarea strategiei, de către managementul responsabil cu aceasta. Reanalizarea strategiei definite la nivelul structurii funcţionale în conformitate cu procedura operaţională aprobată şi actualizarea acesteia astfel încât implementarea sa să contribuie la realizarea unui management modern in domeniul de activitate şi la atingerea obiectivelor strategice ale organizaţiei. Îmbunătăţirea procedurilor operaţionale de lucru privind sistemul de fundamentare a necesarului de resurse pentru elaborarea strategiei.			*X*	31.03.2010
3	Evaluarea performanţelor actuale ale sistemului de organizare şi conducere a activităţilor desfăşurate în cadrul structurii funcţionale, ţinând cont de influenţa factorilor de mediu, interni şi externi, în vederea redefinirii obiectivelor strategice. Implicarea managementului pentru ca obiectivele strategice redefinite să întrunească caracteristicile de a fi realiste, mobilizatoare, stimulative şi să poată fi înţelese de salariaţi, stabilite de metodologie. Totodată, la redefinirea acestora se va urmări asigurarea resurselor necesare implementării lor.	*X*			31.12.2009
4	Dezvoltarea unui sistem de instruire şi pregătire a salariaţilor astfel încât metodologia specifică domeniului de activitate, normativă şi procedurală, să fie aplicată corespunzător pentru dezvoltarea şi implementarea planurilor anuale. În baza planurilor elaborate să se identifice toate atribuţiile necesare pentru atingerea obiectivelor stabilite, iar acestea să fie repartizate corespunzător în cadrul compartimentelor. Totodată, s-a mai recomandat promovarea dezvoltării resurselor umane pentru a obţine competenţele necesare creşterii economice în condiţiile în care au loc reduceri de personal, precum şi evaluarea cuprinzătoare a resurselor		*X*		31.12.2009

	(financiare, instituţionale, programe, personal) necesare implementării planurilor anuale de activitate şi monitorizarea eficientă pentru a se asigura încadrarea în limitele stabilite.				
5	Coroborarea atribuţiilor prezentate prin proceduri cu cele stabilite prin fişele posturilor şi inventarierea stadiului implementării subsistemelor IT la nivelul departamentelor entităţii publice şi stabilirea necesităţilor IT care trebuie incluse în strategia IT.		*X*		31.12.2009
6	Conştientizarea managementului responsabil cu procesul de stabilire şi definire a atribuţiilor prin informări şi consilieri pentru clarificarea modalităţilor practice de definire a unei atribuţii sau unui set de atribuţii pentru asigurarea ariei de competenţă necesară pentru realizarea activităţilor.		*X*		31.12.2009
7	Realizarea unei analize riguroase a sarcinilor şi responsabilităţilor fiecărui angajat, care să stea la baza oricărei iniţiative de organizare a activităţii. Constituirea unei echipe, pe baza deciziei managementului general, care să analizeze şi să redefinească activităţile şi acţiunile realizate în cadrul compartimentelor şi serviciilor, astfel încât să se asigure că obiectivele vor fi realizate în totalitate. La stabilirea obiectivelor se va urmări dacă sunt ataşate toate activităţile necesare obţinerii rezultatelor stabilite, realizate efectiv în cadrul compartimentului, formulate ca acţiuni concrete.			*X*	31.03.2010
8	Analiza actului normativ de organizare şi funcţionare a organizaţiei şi urmărirea atribuţiilor definite departamentului astfel încât să acopere în totalitate activităţile desfăşurate.		*X*		31.12.2009
9	Desfăşurarea procesului de selecţie şi recrutarea în vederea ocupării posturilor de conducere existente la nivelul departamentului IT. În acelaşi timp se va urmări dacă persoanele selectate deţin abilităţile şi aptitudinile manageriale necesare realizării activităţilor specifice celor două servicii şi dacă au pregătirea de bază, de nivel superior, în domeniul IT.			*X*	31.03.2010
10	Elaborarea mecanismelor procedurale şi metodologice privind identificarea riscurilor şi gestionarea acestora, evaluarea riscurilor identificate şi diferenţierea acestora în riscuri inerente şi riscuri acceptabile, precum şi implementarea de instrumente de control pentru riscurile inerente, astfel încât manifestarea acestora să fie limitată şi nivelul acestora să devină unul acceptabil.		*X*		31.03.2010
11	Stabilirea controalelor interne aferente riscurilor identificate şi determinarea gradului de funcţionalitate al acestora şi proiectarea de instrumente sau măsuri de introducere de controale interne, fie individuale, fie în combinaţie cu alte controale, capabile să prevină, detecteze şi să corecteze în mod eficient denaturările semnificative.		*X*		31.12.2009
12	Analiza sarcinilor şi atribuţiilor definite în fişele posturilor şi stabilirea acestora în funcţie de caracteristicile postului, respectiv nivelul postului şi urmărirea definirii aceluiaşi gen de sarcini şi atribuţii numai dacă posturile sunt de acelaşi nivel.		*X*		31.12.2009
13	Identificarea şi definirea corectă în cadrul documentului de organizare şi funcţionare, a atribuţiilor specifice departamentului, a relaţiilor funcţionale pe care compartimentul la are cu alte structuri funcţionale din cadrul organizaţiei.		*X*		31.12.2009
14	Implementarea unei aplicaţii care să monitorizeze alocarea şi utilizarea resurselor în funcţie de gradul de complexitate al operaţiilor efectuate. Urmărirea în permanenţă a echilibrului între necesităţile IT şi resursele alocate acestor scopuri. Protejarea mediile sau locaţiile de stocare împotriva deteriorării sau accesului neautorizat. Realizarea corect şi la intervale de timp stabilite în funcţie de		*X*		31.03.2010

	specificul fiecărei componente, numai de către personal autorizat în acest sens, a procedurilor de mentenanţă a echipamentelor să fie Constituirea în cadrul departamentului IT a unui colectiv specializat în raportarea şi rezolvarea operativă a problemelor de ordin tehnic (Help Desk), care să asigure şi acordarea suportului tehnic de specialitate către utilizatori, fie prin linii telefonice dedicate, fie prin e-mail sau deplasări ale echipelor specializate. Elaborarea şi implementarea unor programe care să automatizeze pe cât posibil verificările efectuate asupra operaţiilor informatice.				
15	Constituirea unor echipe pentru efectuarea de verificări anti-virus la nivelul tuturor staţiilor de lucru din cadrul entităţii publice, configurarea corecta în cazurile în care aceste programe au fost dezactivate, stabilirea de responsabilităţi în cazul în care acestea sunt dezactivate şi produc disfuncţii în cadrul organizaţiei.	*X*			31.12.2009
16	Analiza tuturor aplicaţiilor şi programelor începute şi nefinalizate, identificarea resurselor financiare necesare pentru finalizarea acestora, stabilirea de termene de finalizare şi urmărirea respectării acestora. Noile aplicaţii şi programe vor fi aprobate şi achiziţionate numai dacă sunt compatibile cu cele deja implementate sau aflate în faza de implementare şi numai dacă exista resursele necesare aprobate prin buget.	*X*			31.-03.2010
17	Identificarea riscurilor care guvernează toate subsistemele IT, stabilirea controalelor interne care ar trebui să existe pentru ca acestea să funcţioneze corect, urmărirea controalelor interne care există şi funcţionează, identificarea şi implementarea de instrumente de control pentru controalele interne care nu sunt implementate sau nu funcţionează.		*X*		31.12.2009
18	Implementarea procedurilor operaţionale de lucru cu elemente care să asigure actualizarea în timp util a situaţiilor privind reţelele IT; Tratarea securităţii reţelelor ca pe un proces continuu, astfel încât schimbările în cadrul utilizatorilor, echipamentelor sau aplicaţiilor să se realizeze evitând expunerile la riscuri; Prioritizarea aplicaţiilor informatice, în funcţie de importanţa acestora, în vederea alocării corespunzătoare a măsurilor de securitate, având în vedere că acestea necesită de cele mai multe ori resurse considerabile, care trebuie să fie direct proporţionale cu valoarea datelor sau echipamentelor de protejat; Implementarea unui sistem de management al vulnerabilităţilor, care să identifice precis, cuprinzător şi actualizat la zi, ultimele vulnerabilităţi ale sistemului sau a greşelilor de configurare. Corelarea rapoartelor întocmite în urma identificării şi soluţionării vulnerabilităţilor reţelelor şi aducerea lor la cunoştinţa conducerii entităţii publice.			*X*	31.03.2010
19	Prioritizarea aplicaţiilor informatice, în funcţie de importanţa acestora, în vederea alocării corespunzătoare a măsurilor de securitate şi tratarea securităţii reţelelor ca pe un proces continuu. Implementarea unui sistem de management al vulnerabilităţilor, care să identifice vulnerabilităţile şi greşelile de configurare şi să dispună măsurile operative de soluţionare. Rapoartele întocmite în urma identificării şi soluţionării vulnerabilităţilor reţelelor să fie corelate şi aduse la cunoştinţa conducerii organizaţiei.		*X*		31.12.2009
20	Introducerea de instrumente de control adecvate astfel incit orice acces la echipamentele sau datele si informaţiile organizaţiei sa fie limitat, sau in cazurile in care acesta este permis sa fie supravegheat in totalitate.	*X*			31.12.2009

21	Schimbarea sistematică a parolelor de acces de către utilizatorii sistemului informatic, precum şi stabilirea unei persoane care să aibă în responsabilitate atribuţii şi competenţe de verificare a schimbării periodice a parolelor de acces.		*X*		31.12.2009
22	Organizarea datelor în baze de date, respectiv un fişier format din înregistrări, care conţin câmpuri şi operaţii de căutare, sortare sau recombinare. Pentru aceasta este necesar realizarea următoarelor: definirea, structurarea, ordonarea şi gruparea datelor în colecţii de date omogene; stabilirea legăturilor între date, între elementele unei colecţii de date şi între colecţiile de date, după o ierarhie bine precizată, precum şi memorarea datelor pe un suport informaţional prelucrabil într-un sistem de calcul.		*X*		31.03.2010
23	Inventarierea tuturor staţiilor de lucru pentru a stabili situaţia reală privind utilizarea programelor fără licenţă şi dezinstalarea tuturor programelor nelicenţiate din pachetul Microsoft Office. Totodată, s-a recomandat şi realizarea unei analize complexe în urma căreia managementul entităţii publice să decidă asupra oportunităţii schimbării programelor existente şi achiziţionarea unui număr adecvat de licenţe Microsoft Office.	*X*			31.12.2009
24	Realizarea unui proces de reenginering la nivelul sistemului IT din cadrul entităţii publice, astfel încât salariaţii să poată accesa subsistemele IT de care au nevoie utilizând un singur nume de utilizator şi o singură parolă;			*X*	31.03.2010

Instrucţiuni

1. Introduceţi recomandările de audit după cum sunt prezentate în Raportul de audit intern.
2. Verificaţi coloana corespunzătoare: implementat, parţial implementat, neimplementat
3. Introduceţi data planificată pentru implementare în Raportul de audit intern şi data implementării

Structura auditată: Departamentul Tehnologia Informaţiei
Data: 28.10.2009
Semnătura conducătorului …….

Auditori: Popescu Sorin/ Radu George
Data şi semnătura

Auditori interni,
Popescu Sorin
Radu George

Supervizor,
Dumitru Daniel

Notă:

Această etapă a misiunii de audit presupune asigurarea că recomandările din raportul de audit intern sunt implementate întocmai la termenele stabilite şi în mod eficace, iar conducerea a evaluat riscul de neaplicare a acestor recomandări.

Structura de audit intern va evalua eficacitatea şi oportunitatea acţiunilor stabilite şi întreprinse în vederea implementării recomandărilor, respectarea termenelor şi va determina progresele înregistrate de structura auditată şi modul de îmbunătăţire a activităţilor stabilind valoarea nou creată de auditul intern.

Responsabilul entităţii auditate asigură monitorizarea implementării planului de acţiune şi îl informează periodic pe auditor.

Responsabilul din cadrul structurii de audit intern cu urmărirea recomandărilor trebuie să implementeze şi să actualizeze un proces de urmărire a implementării recomandărilor care să permită supravegherea şi să garanteze că măsurile au fost efectiv implementate de către management

Procedura – P18: URMĂRIREA RECOMANDĂRILOR

Entitatea publică
Serviciul audit intern

PLANUL DE ACŢIUNE ŞI CALENDARUL IMPLEMENTĂRII RECOMANDĂRILOR

Nr. crt.	**Recomandarea**	**Plan de acţiune**	**Calendar implementare**	**Responsabil cu implementarea**
1.	Reanalizarea atribuţiilor Comisiei de planificare strategică în domeniul IT şi redefinirea acestora astfel încât să poată realiza şi monitorizarea implementării proiectelor informatice şi informarea periodică a conducerii asupra realizării acestora.	Identificarea atribuţiilor Comisiei de planificare strategică Revizuirea atribuţiilor şi includerea de atribuţii şi cu privire la monitorizarea implementării proiectelor informatice, precum şi cu privire la raportarea stadiilor de realizare. Cuprinderea acestor atribuţii în cadrul procedurilor de lucru.	31.12.2009	Şeful Depart. IT
2.	Pregătirea profesională anticipată a personalului implicat în elaborarea strategiei, de către managementul responsabil cu aceasta. Reanalizarea strategiei definite la nivelul structurii funcţionale în conformitate cu procedura operaţională aprobată şi actualizarea acesteia astfel încât implementarea sa să contribuie la realizarea unui management modern in domeniul de activitate şi la atingerea obiectivelor strategice ale organizaţiei. Îmbunătăţirea procedurilor operaţionale de lucru privind sistemul de fundamentare a necesarului de resurse pentru elaborarea strategiei.	Stabilirea temei de curs Elaborarea cursului Stabilirea grupului ţintă Organizarea şi desfăşurarea cursului Revizuirea strategiei Actualizarea strategiei Revizuirea procedurilor de lucru privind fundamentarea şi elaborarea strategiei IT	31.03.2010	Şeful Depart. IT
3.	Evaluarea performanţelor actuale ale sistemului de organizare şi conducere a activităţilor desfăşurate în cadrul structurii funcţionale, ţinând cont de influenţa factorilor de mediu, interni şi externi, în vederea redefinirii obiectivelor strategice. Implicarea managementului pentru ca obiectivele strategice redefinite să întrunească caracteristicile de a fi realiste, mobilizatoare, stimulative şi să poată fi înţelese de salariaţi, stabilite de metodologie. Totodată, la redefinirea acestora se va urmări asigurarea resurselor necesare implementării lor.	Realizarea analizei diagnostic la nivelul entităţii Identificarea punctelor forte Identificarea punctelor slabe Identificarea oportunităţilor Identificarea ameninţărilor Identificarea factorilor de influenţă interni şi externi în realizarea strategiei Redefinirea obiectivelor strategice Urmărirea ca obiectivele strategice să fie realiste, mobilizatoare, stimulative şi să fie înţelese de salariaţii care participă la implementarea lor. Identificarea şi aprobarea resurselor necesare realizării obiectivelor strategice. Responsabilizarea managementului cu privire la urmărirea şi coordonarea activităţilor în vederea	31.12.2009	Şeful Depart. IT

		realizării obiectivelor strategice		
4.	Dezvoltarea unui sistem de instruire şi pregătire a salariaţilor astfel încât metodologia specifică domeniului de activitate, normativă şi procedurală, să fie aplicată corespunzător pentru dezvoltarea şi implementarea planurilor anuale. În baza planurilor elaborate să se identifice toate atribuţiile necesare pentru atingerea obiectivelor stabilite, iar acestea să fie repartizate corespunzător în cadrul compartimentelor. Totodată, s-a mai recomandat promovarea dezvoltării resurselor umane pentru a obţine competenţele necesare creşterii economice în condiţiile în care au loc reduceri de personal, precum şi evaluarea cuprinzătoare a resurselor (financiare, instituţionale, programe, personal) necesare implementării planurilor anuale de activitate şi monitorizarea eficientă pentru a se asigura încadrarea în limitele stabilite.	Identificarea temelor de curs necesare pentru ca personalul din cadrul departamentului IT să deprindă cunoştinţele necesare realizării sarcinilor stabilite posturilor. Organizarea şi cuprinderea în cadrul seminarilor a întregului personal din cadrul departamentului IT în funcţie de nevoile identificate Asigurarea că temele de curs cuprind în mod adecvat metodologia domeniului de activitate Analiza comparativă a atribuţiilor stabilite posturilor şi a celor necesare realizării obiectivelor şi urmărirea dacă acestea sunt suficiente sau este necesară completarea lor. Redefinirea atribuţiilor acolo unde este necesar. Urmărirea repartizării în mod omogen a atribuţiilor în cadrul posturilor Pregătirea şi instruirea personalului în vederea dezvoltării competenţelor necesare astfel încât să contribuie la dezvoltarea entităţii. Reevaluarea resurselor şi urmărirea ca acestea să fie suficiente pentru implementarea planurilor de activitate. Monitorizarea resurselor astfel încât să se asigure încadrarea în limitele stabilite	31.12.2009	Şeful Depart. IT
5.	Coroborarea atribuţiilor prezentate prin proceduri cu cele stabilite prin fişele posturilor şi inventarierea stadiului implementării subsistemelor IT la nivelul departamentelor entităţii publice şi stabilirea necesităţilor IT care trebuie incluse în strategia IT.	Compararea atribuţiilor stabilite în fişele posturilor cu activităţile şi responsabilităţile definite în cadrul procedurilor şi urmărirea ca acestea să asigure aria necesară realizării lor. Inventarierea stadiului implementării programelor şi aplicaţilor IT, analiza nerealizărilor conform programelor şi stabilirea de măsuri necesare a fi cuprinse în cadrul strategiei.	31.12.2009	Şeful Depart. IT
6.	Conştientizarea managementului responsabil cu procesul de stabilire şi definire a atribuţiilor prin informări şi consilieri pentru clarificarea modalităţilor practice de definire a unei atribuţii sau unui set de atribuţii pentru asigurarea ariei de competenţă necesară pentru realizarea activităţilor.	Organizarea de grupuri de lucru în vederea conştientizării managementului cu privire la definirea şi stabilirea atribuţiilor	31.12.2009	Şeful Depart.IT
7.	Realizarea unei analize riguroase a sarcinilor şi responsabilităţilor fiecărui angajat, care să stea la baza oricărei iniţiative de organizare a activităţii. Constituirea unei echipe, pe baza deciziei	Evaluarea sarcinilor şi responsabilităţilor stabilite posturilor Urmărirea dacă sarcinile şi responsabilităţile stabilite postului	31.03.2010	Şeful Depart. IT

	managementului general, care să analizeze şi să redefinească activităţile şi acţiunile realizate în cadrul compartimentelor şi serviciilor, astfel încât să se asigure că obiectivele vor fi realizate în totalitate. La stabilirea obiectivelor se va urmări dacă sunt ataşate toate activităţile necesare obţinerii rezultatelor stabilite, realizate efectiv în cadrul compartimentului, formulate ca acţiuni concrete.	individualizează în mod adecvat postul respectiv. Numirea comisiei cu atribuţii de evaluare a activităţilor stabilite fiecărui compartimente Examinarea dacă atribuţiile stabilite comisiei sunt suficiente şi adecvate pentru a evalua dacă posturile existente contribuie în mod adecvat la realizarea obiectivelor		
8.	Analiza actului normativ de organizare şi funcţionare a organizaţiei şi urmărirea atribuţiilor definite departamentului astfel încât să acopere în totalitate activităţile desfăşurate.	Examinarea ROF-ului entităţii şi urmărirea dacă atribuţiile menţionate pentru departamentul IT asigură aria de competenţă necesară realizării activităţilor desfăşurate în cadrul acestuia.	31.12.2009	Şeful Depart. IT
9.	Desfăşurarea procesului de selecţie şi recrutarea în vederea ocupării posturilor de conducere existente la nivelul departamentului IT. În acelaşi timp se va urmări dacă persoanele selectate deţin abilităţile şi aptitudinile manageriale necesare realizării activităţilor specifice celor două servicii şi dacă au pregătirea de bază, de nivel superior, în domeniul IT.	Stabilirea unei proceduri de lucru cu privire la selecţia şi recrutarea personalului în cadrul departamentului IT. Examinarea dacă persoanele selectate în posturile de conducere deţin abilităţi şi aptitudini manageriale şi dacă specialitatea studiilor corespunde necesităţilor postului.	31.03.2010	Şeful Depart. IT
10.	Elaborarea mecanismelor procedurale şi metodologice privind identificarea riscurilor şi gestionarea acestora, evaluarea riscurilor identificate şi diferenţierea acestora în riscuri inerente şi riscuri acceptabile, precum şi implementarea de instrumente de control pentru riscurile inerente, astfel încât manifestarea acestora să fie limitată şi nivelul acestora să devină unul acceptabil.	Responsabilizarea persoanelor cu privire la gestiunea riscurilor Identificarea riscurilor în cadrul departamentului Evaluarea şi analiza riscurilor Tratarea riscurilor Controlul riscurilor	31.03.2010	Şeful Depart. IT
11.	Stabilirea controalelor interne aferente riscurilor identificate şi determinarea gradului de funcţionalitate al acestora şi proiectarea de instrumente sau măsuri de introducere de controale interne, fie individuale, fie în combinaţie cu alte controale, capabile să prevină, detecteze şi să corecteze în mod eficient denaturările semnificative.	Identificarea tuturor riscurilor inerente în cadrul departamentului Stabilirea instrumentelor de control necesare limitării riscurilor Implementarea instrumentelor de control Urmărirea eficienţei şi funcţionalităţii instrumentelor de control şi dacă acestea au limitat riscul şi-l menţin în limite acceptabile.	31.12.2009	Şeful Depart. IT
12.	Analiza sarcinilor şi atribuţiilor definite în fişele posturilor şi stabilirea acestora în funcţie de caracteristicile postului, respectiv nivelul postului şi urmărirea definirii aceluiaşi gen de sarcini şi atribuţii numai dacă posturile sunt de acelaşi nivel.	Reevaluarea sarcinilor stabilite fiecărui post din cadrul departamentului Redefinirea acestora pe posturi în funcţie de caracteristicile şi cerinţele acestora Stabilirea de sarcini fiecărui post în funcţie de nivelul postului şi natura acestuia	31.12.2009	Şeful Depart. IT
13.	Identificarea şi definirea corectă în cadrul documentului de organizare şi funcţionare, a atribuţiilor specifice departamentului, a relaţiilor funcţionale pe care compartimentul la are cu alte structuri funcţionale din cadrul organizaţiei.	Revizuirea atribuţiilor din cadrul ROF-ului şi redefinirea în mod adecvat a acestora Revizuirea relaţiilor funcţionale în cadrul şi în afara departamentului şi redefinirea adecvată a acestora	31.12.2009	Şeful Depart. IT

14.	Implementarea unei aplicaţii care să monitorizeze alocarea şi utilizarea resurselor în funcţie de gradul de complexitate al operaţiilor efectuate. Urmărirea în permanenţă a echilibrului între necesităţile IT şi resursele alocate acestor scopuri. Protejarea mediile sau locaţiile de stocare împotriva deteriorării sau accesului neautorizat. Realizarea corect şi la intervale de timp stabilite în funcţie de specificul fiecărei componente, numai de către personal autorizat în acest sens, a procedurilor de mentenanţă a echipamentelor. Constituirea în cadrul departamentului IT a unui colectiv specializat în raportarea şi rezolvarea operativă a problemelor de ordin tehnic (Help Desk), care să asigure şi acordarea suportului tehnic de specialitate către utilizatori, fie prin linii telefonice dedicate, fie prin e-mail sau deplasări ale echipelor specializate. Elaborarea şi implementarea unor programe care să automatizeze pe cât posibil verificările efectuate asupra operaţiilor informatice.	Conceperea şi implementarea unei aplicaţii care va monitoriza alocarea resurselor financiare pentru fiecare activitate desfăşurată şi care va genera rapoarte cu privire la utilizarea acestora. Analiza comparativă a resurselor consumate pentru realizarea activităţilor, în raport cu cele aprobate Examinarea locaţiilor de stocare a informaţiilor şi urmărirea dacă există condiţii adecvate de stocare. Crearea de aplicaţii care să preîntâmpine accesul neautorizat la programe şi aplicaţii. Realizarea procedurilor de mentenanţă la intervalele de timp planificate Numirea comisiei cu atribuţii în raportarea operativă a problemelor tehnice Stabilirea atribuţiilor comisiei numite. Conceperea şi implementarea unei aplicaţii care să monitorizeze operaţiile efectuate în cadrul programelor şi aplicaţiilor derulate în cadrul entităţii.	31.03.2010	Şeful Depart. IT
15.	Constituirea unor echipe pentru efectuarea de verificări anti-virus la nivelul tuturor staţiilor de lucru din cadrul entităţii publice, configurarea corecta în cazurile în care aceste programe au fost dezactivate, stabilirea de responsabilităţi în cazul în care acestea sunt dezactivate şi produc disfuncţii în cadrul organizaţiei.	Numirea unui responsabil cu examinarea staţiilor de lucru virusate. Examinarea fiecărei staţii de lucru şi devirusarea acestora Configurarea programelor anti-virus pe fiecare staţie de lucru pe bază de licenţă. Stabilirea răspunderilor în sarcina utilizatorilor în cazul în care programele antivirus sunt dezactivate, iar aplicaţiile sau informaţiile conţinute de acestea suferă denaturări.	31.12.2009	Şeful Depart. IT
16.	Analiza tuturor aplicaţiilor şi programelor începute şi nefinalizate, identificarea resurselor financiare necesare pentru finalizarea acestora, stabilirea de termene de finalizare şi urmărirea respectării acestora. Noile aplicaţii şi programe vor fi aprobate şi achiziţionate numai dacă sunt compatibile cu cele deja implementate sau aflate în faza de implementare şi numai dacă exista resursele necesare aprobate prin buget.	Identificarea tuturor aplicaţiilor şi programelor din cadrul entităţii începute şi neimplementate. Identificarea resurselor financiare pentru implementarea lor şi aprobarea acestora. Stabilirea de grafice de implementare şi urmărirea implementării acestora. Examinarea noilor programe şi aplicaţii de achiziţionat. Achiziţionarea acestora numai dacă sunt compatibile cu cele existente şi contribuie la integrarea informaţiilor	31.-03.2010	Şeful Depart. IT
17.	Identificarea riscurilor care guvernează toate subsistemele IT, stabilirea controalelor interne care ar trebui să existe pentru ca acestea să funcţioneze corect, urmărirea controalelor interne care există	Identificarea riscurilor aferente subsistemelor IT Evaluarea instrumentelor de control existente şi urmărirea dacă acestea asigură un nivel acceptat al	31.12.2009	Şeful Depart. IT

	şi funcţionează, identificarea şi implementarea de instrumente de control pentru controalele interne care nu sunt implementate sau nu funcţionează.	riscurilor Stabilirea instrumentelor de control de implementat astfel încât să asigure funcţionalitatea acestora		
18.	Implementarea procedurilor operaţionale de lucru cu elemente care să asigure actualizarea în timp util a situaţiilor privind reţelele IT; Tratarea securităţii reţelelor ca pe un proces continuu, astfel încât schimbările în cadrul utilizatorilor, echipamentelor sau aplicaţiilor să se realizeze evitând expunerile la riscuri;	Revizuirea procedurilor de lucru Elaborarea unei proceduri de lucru cu privire la tratarea securităţii reţelelor. Securizarea tuturor aplicaţiilor şi programelor cu privire la accesul la acestea, inclusiv la informaţiile conţinute.	31.03.2010	Şeful Depart. IT
19	Prioritizarea aplicaţiilor informatice, în funcţie de importanţa acestora, în vederea alocării corespunzătoare a măsurilor de securitate şi tratarea securităţii reţelelor ca pe un proces continuu. Implementarea unui sistem de management al vulnerabilităţilor, care să identifice vulnerabilităţile şi greşelile de configurare şi să dispună măsurile operative de soluţionare. Rapoartele întocmite în urma identificării şi soluţionării vulnerabilităţilor reţelelor să fie corelate şi aduse la cunoştinţa conducerii organizaţiei.	Elaborarea unei proceduri de lucru cu privire la tratarea vulnerabilităţilor. Responsabilizarea unei persoane cu privire la tratarea vulnerabilităţilor. Analiza periodică a vulnerabilităţilor şi elaborarea de rapoarte Informarea conducerii cu privire la vulnerabilităţile identificate şi propunerea de soluţii de remediere	31.12.2009	Şeful Depart. IT
20	Introducerea de instrumente de control adecvate astfel incit orice acces la echipamentele sau datele si informaţiile organizaţiei sa fie limitat, sau in cazurile in care acesta este permis sa fie supravegheat in totalitate.	Examinarea tuturor echipamentelor şi aplicaţiilor Identificarea celor care nu prezintă un sistem adecvat de accesare Stabilirea unui sistem de parole în vederea limitării accesului Stabilirea accesului la informaţii pe nivele de autorizare, în funcţie de nivelul şi cerinţele posturilor.	31.12.2009	Şeful Depart. IT
21	Schimbarea sistematică a parolelor de acces de către utilizatorii sistemului informatic, precum şi stabilirea unei persoane care să aibă în responsabilitate atribuţii şi competenţe de verificare a schimbării periodice a parolelor de acces.	Responsabilizarea unei persoane care să urmărească schimbarea periodică a parolelor. Urmărirea schimbării periodice a parolelor.	31.12.2009	Şeful Depart. IT
22	Organizarea datelor în baze de date, respectiv un fişier format din înregistrări, care conţin câmpuri şi operaţii de căutare, sortare sau recombinare. Pentru aceasta este necesar realizarea următoarelor: definirea, structurarea, ordonarea şi gruparea datelor în colecţii de date omogene; stabilirea legăturilor între date, între elementele unei colecţii de date şi între colecţiile de date, după o ierarhie bine precizată, precum şi memorarea datelor pe un suport informaţional prelucrabil într-un sistem de calcul.	Revizuirea bazelor de date constituite Organizarea informaţiilor în cadrul acestora în mod adecvat, respectiv: - definirea datelor conţinute; - structurarea datelor în funcţie de importanţă; - ordonarea şi gruparea datelor - stabilirea legăturilor între date şi informaţii; - stabilirea nivelurilor de acces la date şi informaţii - organizarea sistemului de securitate, protecţie şi acces la datele şi informaţiile stocate.	31.03.2010	Şeful Depart. IT
23	Inventarierea tuturor staţiilor de lucru pentru a stabili situaţia reală privind utilizarea programelor fără licenţă şi dezinstalarea tuturor programelor nelicenţiate din pachetul Microsoft Office. Totodată, s-a recomandat şi realizarea unei analize complexe în urma căreia	Identificarea staţiilor de lucru Examinarea aplicaţiilor şi programelor utilizate de fiecare staţie de lucru şi stabilirea celor care sunt utilizate fără a exista licenţe. Dezinstalarea tuturor programelor	31.12.2009	Şeful Depart. IT

	managementul entităţii publice să decidă asupra oportunităţii schimbării programelor existente şi achiziţionarea unui număr adecvat de licenţe Microsoft Office.	utilizate fără licenţe. Instalarea de programe şi aplicaţii adecvate pentru care există licenţe. Analiza eficienţei şi eficacităţii aplicaţiilor utilizate şi a oportunităţii schimbării acestora cu unele cu calităţi şi performanţe ridicate.		
24	Realizarea unui proces de reenginering la nivelul sistemului IT din cadrul entităţii publice, astfel încât salariaţii să poată accesa subsistemele IT de care au nevoie utilizând un singur nume de utilizator şi o singură parolă;	Realizarea procesului de reenginering la nivelul departamentului IT şi asigurarea că salariaţii pot accesa subsistemele IT utilizând un singur nume şi o singură parolă de acces.	31.03.2010	Şeful Depart. IT

PROGRAMUL DE ASIGURARE ŞI ÎMBUNĂTĂŢIRE A CALITĂŢII

Şeful structurii de audit intern trebuie să elaboreze un *Program de asigurare şi îmbunătăţire a calităţii activităţii de audit*, adică respectarea normelor metodologice, a Codului privind conduita etica a auditorului intern, a Standardelor şi a bunei practici internaţionale de către toţi auditorii interni.

Prin Programul de asigurare şi îmbunătăţire a calităţii se realizează o evaluare prin adoptarea unui proces permanent de supraveghere a eficacităţii globale a programului de calitate.

Evaluarea constă în supervizarea realizării misiunii de audit intern, prin efectuarea de controale permanente de către şeful structurii de audit intern, prin care acesta examinează eficacitatea normelor de audit intern şi dacă procedurile de asigurare a calităţii misiunii de audit sunt aplicate în mod corespunzător garantând calitatea Raportului de audit intern.

Supervizarea va permite depistarea deficienţelor în anumite etape din derularea misiunii şi va permite iniţierea de activităţi de îmbunătăţire a viitoarelor misiuni de audit intern şi asigurarea perfecţionării profesionale a auditorilor.

Evaluarea se realizează după fiecare misiune de audit intern. Este formalizată prin întocmirea *Fişei de evaluare a misiunii de audit intern*.

EVALUAREA INTERNĂ

Procedura – P19: PROGRAMUL DE ASIGURARE A CALITĂŢII

Entitatea Publică
Serviciul de Audit Intern

FIŞA DE EVALUARE A MISIUNII DE AUDIT INTERN

Misiunea de audit: Tehnologia informaţiei
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 28.09.2009
Avizat: Dumitru Daniel Data: 28.09.2009

Bugetul de timp efectiv: 264 ore	***Bugetul de timp planificat: 260***					
	1	***2***	***3***	***4***	***5***	***Observaţii***
În etapa de pregătire a misiunii, auditorul a identificat riscurile şi controalele prevăzute pentru procesele legate de obiectivele de audit şi a estimat corespunzător riscurile activităţii				*X*		
Programele de audit au fost elaborate în vederea îndeplinirii obiectivelor misiunii în cadrul bugetului de timp alocat				*X*		*A fost necesar să se lucreze peste orele de program*
Obiectivul auditului, scopul, procedurile şi bugetul au fost reanalizate în mod constant pentru a asigura o eficientă folosire a resurselor de audit			*X*			
A existat o bună comunicare între auditor şi auditat şi între					*X*	

Bugetul de timp efectiv: 264 ore	***Bugetul de timp planificat: 260***					
	1	***2***	***3***	***4***	***5***	***Observaţii***
auditor şi conducerea structurii de audit intern;						
A existat o bună comunicare între auditor şi conducerea structurii de audit intern					*X*	
Au fost luate în considerare perspectivele şi nevoile audiaţilor în procesul de audit				*X*		
Au fost atinse obiectivele de audit într-o manieră eficientă şi la timp				*X*		
Auditaţii au avut posibilitatea să revadă constatările şi recomandările când au fost identificate problemele					*X*	
Normele de audit intern, au fost respectate				*X*		
Constatările de audit demonstrează analize profunde şi concluzii, respectiv sunt formulate recomandări practice pentru probleme identificate				*X*		
Comunicările scrise au fost clare, concise, obiective şi corecte				*X*		
Există probe de audit care să susţină concluziile auditorului					*X*	
Procedurile de audit utilizate au avut ca rezultat dovezi suficiente, competente, relevante şi folositoare				*X*		
Documentele au fost completate în mod corespunzător şi în conformitate cu normele de audit intern				*X*		
Bugetul de timp a fost respectat					*X*	
Nivel de productivitate personală al auditorului intern.				*X*		

EVALUAREA EXTERNĂ

Evaluarea misiunii de audit intern mai poate fi realizată şi de conducerea structurii auditate căreia i se înaintează un chestionar de evaluare prin care i se solicită să prezinte o apreciere asupra desfăşurării misiunii de audit şi a modului de implicare al auditorilor interni pe parcursul misiunii.

Evaluarea misiunii de audit intern de către structura auditată este formalizată prin *Fişa de evaluare a misiunii de audit intern* întocmită de către structura auditată.

Entitatea publică
Serviciul Audit Intern

FIŞA DE EVALUARE A MISIUNII DE AUDIT INTERN DE CĂTRE STRUCTURA AUDITATĂ

Misiunea de audit: Tehnologia informaţiei
Perioada auditată: 01.01.2008 – 30.06.2009
Întocmit: Popescu Sorin/Radu George Data: 28.09.2009
Avizat: Dumitru Daniel Data: 28.09.2009

Nr. crt.	Obiectiv auditat	Note					Obs.
		1	2	3	4	5	
1.	Obiectivele de audit au fost comunicate clar la începutul misiunii				X		
2.	Au fost furnizate suficiente informaţii privind misiunea de efectuat					X	
3.	Misiunea a contribuit la obţinerea de rezultate sau la îmbunătăţirea unora deja existente					X	
4.	Misiunea a beneficiat de direcţii clare şi precise privind modul de desfăşurare				X		
5.	Obiectivele de audit stabilite au fost în concordanta cu activităţile desfăşurate				X		
6.	Constatările au fost prezentate într-o maniera logică, structurată, dinamică şi interesantă					X	
7.	S-a răspuns în toate cazurile la întrebările legate de misiunea de audit, iar răspunsurile au condus la obţinerea de concluzii relevante				X		
8.	Misiunea a fost desfăşurată adecvat, intervenţia la fata locului a privit doar obiectivele stabilite şi comunicate				X		
9.	A existat un feed-back pe tot parcursul misiunii, iar acesta a fost util în găsirea de soluţii la probleme					X	
10.	Cum evaluaţi în general misiunea de audit				X		
11.	Consideraţi ca obiectivele de audit stabilite au privit activităţile cu riscuri majore				X		
12.	In desfăşurarea misiunii de audit au fost prezentate constatările şi recomandările când au fost identificate probleme					X	
13.	A existat o buna comunicare intre auditor şi auditat					X	
14.	Auditorii au avut un comportament adecvat şi profesional					X	
15.	Ce v-a plăcut cel mai mult pe timpul misiunii de audit – descrieţi cel puţin 3 aspecte care v-au plăcut cel mai mult *claritatea recomandărilor* *conduita auditorilor interni* *calitatea discuţiilor*						

16.	Ce v-a plăcut cel mai puţin pe timpul misiunii de audit – descrieţi cel puţin 3 aspecte care v-au plăcut cel mai puţin *Întâlnirile pe parcursul misiunii au fost limitate, nu întotdeauna din vina auditatului.*
17.	Ce obiective de audit consideraţi că nu au fost atinse în totalitate din cele comunicate *Nu sunt comentarii.*
18.	Ce obiective de audit consideraţi că ar fi necesar a fi cuprinse în programul viitor de audit *Calitatea procedurilor privind achiziţiile publice elaborate în urma recomandărilor.*
19.	Alte comentarii

Tabelele de mai sus vor fi completate ţinând cont de următorul sistem de punctaj:
1 pentru nesatisfăcător;
2 pentru slab;
3 pentru satisfăcător;
4 pentru bine;
5 pentru foarte bine.

Notă: În practică se va urmări ca pentru orice notare sub 3 să se solicite explicaţii scrise.

Evaluarea externă a funcţionalităţii activităţii de audit intern se realizează şi de U.C.A.A.P.I. şi organul ierarhic superior pentru structurile din subordine prin verificarea respectării normelor metodologice generale şi specifice, a Standardelor de audit intern, a bunei practici recunoscute în domeniu şi a Codului etic al profesiei.

Activitatea de evaluare externă a activităţii de audit intern, în România, conform cadrului normativ general, se realizează o dată la 5 ani, ocazie cu care, în funcţie de necesităţi, se iniţiază măsuri corective în colaborare cu conducătorul entităţii evaluate în cauză.

Documentele de evaluare internă şi externă se arhivează în Dosarul permanent, Secţiunea - *Supervizarea*.

În speranţa că prezentul ghid practic va constitui pentru cei interesaţi un suport pentru realizarea misiunilor de audit intern la un nivel corespunzător bunei practici recunoscută în domeniu, aşteptăm aprecierile şi eventual sugestiile dumneavoastră, de care vom încerca să ţinem cont cu ocazia elaborării viitoarelor lucrări.