MINISTERUL FINANȚELOR PUBLICE
UNITATEA CENTRALA DE ARMONIZARE PENTRU AUDITUL PUBLIC INTERN

GHID PRACTIC
MISIUNEA DE AUDIT INTERN
PRIVIND
ACTIVITATEA IT

AVIZAT
GHITA MARCEL
Sef serviciu pentru Strategie si Metodologie Generala

ELABORAT
CONSTANTIN VASILE NICOLAE
Auditor superior

Ghidul practic privind realizarea unei misiuni de audit intern pentru activitatea Serviciului Juridic, constituie un model pentru desfasurarea misiunilor in baza Legii nr. 672/2002 privind auditul public intern si a Normelor generale pentru exercitarea auditului public intern aprobate prin OMFP nr. 38/2003, cu modificarile si completarile ulterioare.

Asteptam sugestiile dumneavoastra pe adresa UCAAPI sau pe e-mail: marcel.ghita@mfinante.gv.ro sau cornelia.nicolau@mfinante.gv.ro

BUCURESTI
2006

CUVANT INAINTE

Ghidul de audit intern privind activitatea IT reprezinta un model practic de desfasurare a unei misiuni, prin parcurgerea in detaliu, a fiecarui pas, intr-o maniera didactica. Ghidul poate fi utilizat de entitatile din sectorul public si in acelasi timp va reprezenta suportul pentru realizarea propriului ghid practic specific entitatii.

Elaborarea ghidului are la baza prevederile art. 8 lit. c) din *Legea nr. 672/2002 privind auditul public intern*, referitoare la dezvoltarea si implementarea unor proceduri si metodologii uniforme, bazate pe standardele internationale.

In conformitate cu prevederile punctului 4, Partea I din *Normele generale de exercitare a auditului public intern, aprobate prin OMF nr. 38/2003* (Manualul de audit intern), misiunea de audit intern are drept scop evaluarea sistemelor de management si control intern ale entitatii, urmarind transparenta si conformitatea cu cadrul normativ.

Realizarea ghidului practic presupune parcurgerea procedurilor si documentelor specifice structurate pe cele patru etape prezentate prin normele generale.

- *In etapa de pregatire a misiunii de audit intern* au fost elaborate documentele prevazute de normele generale si s-au adus clarificari, in special, cu privire la modul concret de dezvoltare a procedurii de *Analiza riscurilor*, succesiunea documentelor, structura acestora si modul de completare, nivelul de apreciere si impartire al riscurilor in mari, medii si mici, clasarea si ierarhizarea acestora in vederea finalizarii procedurii pe baza careia se va concentra munca pe teren si a *Programului interventiei a fata locului*.

- *In etapa de interventie la fata locului* s-au realizat testarea pe teren a operatiilor auditabile, pe baza *Programului interventiei a fata locului*, prin utilizarea diferitelor tehnici de esantionare, liste de verificare, teste, foi de lucru, interviuri si note de relatii, elemente care s-au constituit in probe de audit si au stat la baza intocmirii FIAP-urilor si FCRI- urilor, care vor fi incluse in raport.

- *In etapa de elaborare a Raportului de audit intern* s-a urmarit structurarea acestuia pe *Tematica in detaliu a misiunii de audit* obtinuta in procedura de *Analiza riscurilor* si transferarea FIAP-urilor si FCRI- urilor intr-o maniera standardizata pentru a putea fi utilizat de factorii de management.

- *In etapa de urmarire a recomandarilor* in afara documentelor stabilite de normele generale sunt propuse unele modele de documente pentru evaluarea interna si externa a activitatii de audit intern.

ENTITATEA PUBLICĂ
Compartimentul Audit Intern
Nr. 25 din 08.01.2006

ORDIN DE SERVICIU

In conformitate cu prevederile Legii nr. 672/2002 privind auditul public intern, a O.M.F.P. nr. 38/2003 de aprobare a normelor metodologice generale privind exercitarea activităţii de audit intern, a Ordinului managerului general nr. 1024/2003 prin care s-au aprobat Normele proprii de exercitare a auditului intern în cadrul entităţii publice şi a Planului de audit intern pentru anul 2006, se va efectua misiunea de audit intern la Direcţia Tehnologia Informaţiei în perioada 25.01.2006 – 17.04.2006.

Scopul misiunii de audit este de a da asigurări asupra *activităţii IT de la nivelul entităţii publice* şi a conformităţii cu cadrul legislativ şi normativ aplicabil, fiind structurate pe următoarele domenii auditabile:

- *Plan strategic*;
- *Organizarea şi funcţionarea Departamentului IT;*
- *Implementarea sistemului IT;*
- *Securitatea IT.*

Menţionăm că se va efectua un audit de conformitate al modului de organizare a activităţii de tehnologia informaţiei din entitatea publică.

Echipa de auditori interni este formată din următorii:

1. Popescu Sorin;
2. Radu George.

Coordonator Compartimentul de Audit Intern,
Dumitru Daniel

Procedura - P02: Iniţierea auditului

ENTITATEA PUBLICĂ
Compartimentul Audit Intern

DECLARAŢIA DE INDEPENDENŢĂ

Nume şi prenume: Popescu Sorin
Misiunea de audit: Tehnologia Informatiei Data: 10.01.2006

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
Dacă în timpul misiunii de audit, apare orice incompatibilitate personală, externă sau organizaţională care ar putea să vă afecteze abilitatea dvs. de a lucra şi a face rapoartele de audit imparţiale, notificaţi coordonatorul Compartimentului Audit Public Intern de urgenţă?	X	-

Auditor,
Popescu Sorin

Coordonatorul Compartimentului Audit Intern,
Dumitru Daniel

1 Incompatibilităţi personale: Nu.
2. Pot fi eliminate incompatibilităţile: Nu este cazul.
Dacă da, explicaţi cum anume: Nu este cazul.
Data: 10.01.2006
Semnătura: Dumitru Daniel

Procedura - P02: Inițierea auditului

ENTITATEA PUBLICĂ
Compartimentul Audit Intern

DECLARAȚIA DE INDEPENDENȚĂ

Nume şi prenume: Radu George
Misiunea de audit: Tehnologia Informatiei Data: 10.01.2006

Incompatibilități în legătură cu entitatea/structura auditată		
	Da	Nu
Ați avut/aveți vreo relație oficială, financiară sau personală cu cineva care ar putea să vă limiteze măsura în care puteți să vă interesați, să descoperiți sau să constatați slăbiciuni de audit în orice fel?	-	X
Aveți idei preconcepute față de persoane, grupuri, organizații sau obiective care ar putea să vă influențeze în misiunea de audit?	-	X
Ați avut/aveți funcții sau ați fost/sunteți implicat(ă) în ultimii 3 ani într-un alt mod în activitatea entității/structurii ce va fi auditată?	-	X
Aveți responsabilități în derularea programelor şi proiectelor finanțate integral sau parțial de Uniunea Europeană?	-	X
Ați fost implicat în elaborarea şi implementarea sistemelor de control ale entității/structurii ce urmează a fi auditată?	-	X
Sunteți soț/soție, rudă sau afin până la gradul al patrulea inclusiv cu conducătorul entității/structurii ce va fi auditată sau cu membrii organului de conducere colectivă?	-	X
Aveți vreo legătură politică, socială care ar rezulta dintr-o fostă angajare sau primirea de redevențe de la vreun grup anume, sau organizație sau nivel guvernamental?	-	X
Ați aprobat înainte facturi, ordine de plată şi alte instrumente de plată pentru entitatea/structura ce va fi auditată?	-	X
Ați ținut anterior contabilitatea la entitatea/structura ce va fi auditată?	-	X
Aveți vreun interes direct sau unul de fond financiar indirect la entitatea/structura ce va fi auditată?	-	X
Dacă în timpul misiunii de audit, apare orice incompatibilitate personală, externă sau organizațională care ar putea să vă afecteze abilitatea dvs. de a lucra şi a face rapoartele de audit imparțiale, notificați coordonatorul Compartimentului Audit Public Intern de urgență?	X	-

Auditor, Coordonatorul Compartimentului Audit Intern,
Radu George Dumitru Daniel

1. Incompatibilități personale: Nu.
2. Pot fi eliminate incompatibilitățile: Nu este cazul.
   Dacă da, explicați cum anume: Nu este cazul.

Data: 10.01.2006 Semnătura: Dumitru Daniel

ENTITATEA PUBLICĂ
Compartimentul Audit Intern
Nr. 29 din 10.01.2006

NOTIFICAREA PRIVIND DECLANŞAREA MISIUNII DE AUDIT INTERN

Către: Direcţia Tehnologia Informaţiei
De la: Coordonatorul Compartimentului Audit Intern

Referitor la misiunea de audit intern „***Modul de organizare a activităţii de tehnologia informaţiei din entitatea publică***"

Stimate domnule Pătrulescu Ştefan,

În conformitate cu Planul de audit intern pe anul 2006, urmează ca în perioada 25.01.2006 – 17.04.2006 să efectuăm o misiune de audit intern cu tema ***Tehnologia informaţiei.***

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

- prezentarea auditorilor;
- prezentarea principalelor obiective ale misiunii de audit intern;
- programul intervenţiei la faţa locului;
- scopul misiunii de audit intern;
- alte aspecte.

Pentru o mai bună înţelegere a activităţii dumneavoastră, vă rugăm sa ne puneţi la dispoziţie următoarea documentaţie necesară privind activitatea de tehnologie a informaţiei: legile şi reglementările ce se aplica activităţilor dumneavoastră, organigrama direcţiei dumneavoastră, Regulamentul de organizare şi funcţionare, fişele posturilor, procedurile scrise care descriu sarcinile ce trebuie realizate pe linia organizării activităţii, un exemplar al rapoartelor de activitate, notelor, misiunilor de audit anterioare care se referă la aceasta temă.

Dacă aveţi unele întrebări privind desfăşurarea misiunii, vă rugăm să-l contactaţi pe domnul Popescu Sorin - auditor, coordonatorul misiunii sau pe şeful structurii de audit intern.

Cu stimă,

Data: 10.01.2006

Coordonatorul Compartimentului Audit Intern
Dumitru Daniel

Procedura – P04: Colectarea şi prelucrarea informaţiilor

ENTITATEA PUBLICĂ
Compartimentul Audit Intern

COLECTAREA INFORMAŢIILOR

Misiunea de audit**:** ***Tehnologia Informaţiei***
Perioada auditată: **01.01- 31.12.2005**
Întocmit: **Popescu Sorin / Radu George** **Data: 10.01.2006**
Avizat: **Dumitru Daniel** **Data: 10.01.2006**

COLECTAREA INFORMAŢIILOR			
DIRECŢIA TEHNOLOGIA INFORMAŢIEI	**DA**	**NU**	**Observaţii**
Identificarea legilor şi regulamentelor aplicabile structurii auditate	X	-	
Obţinerea organigramei	X	-	
Obţinerea Regulamentului de organizare şi funcţionare	X	-	
Obţinerea fişelor posturilor	X	-	
Obţinerea procedurilor scrise	-	X	Există doar parţial
Identificarea personalului responsabil	X	-	
Obţinerea exemplarului de Raport de audit intern anterior	-	X	Anterior nu au fost realizate misiuni de audit intern asupra tehnologiei informaţiei la nivelul entităţii publice

Procedura – P05 : Analiza riscurilor

ENTITATEA PUBLICĂ
Compartimentul Audit Intern

LISTA CENTRALIZATOARE A OBIECTELOR AUDITABILE

Misiunea de audit: Tehnologia informației
Perioada auditată: 01.01.2005- 31.12.2005
Întocmit: Popescu Sorin/Radu George **Data:** 20.01.2006
Avizat: Dumitru Daniel **Data:** 20.01.2006

Nr. crt.	DOMENIUL	OBIECTE AUDITABILE	OBS.
I.	**Plan strategic**	1. Politicile entității publice în domeniul IT	
		2. Modalitatea de elaborare a planului strategic şi a planurilor anuale	
		3. Subsistemele informatice pentru funcțiile principale	
		4. Integrarea subsistemelor informatice	
		5. Stabilirea responsabililor cu elaborarea si actualizarea planului	
		6. Aprobarea planului	
II.	**Organizarea şi funcționarea departamentului IT**	7. Organizarea departamentului IT	
		8. Stabilirea responsabilităților prin fişele posturilor	
		9. Calificarea şi pregătirea salariaților	
		10. Pregătirea profesională continuă	
		11. Sistemul de evaluare a personalului	
		12. Sistemul de gestionare a riscurilor – conducerea Registrului riscurilor	
III.	**Implementarea sistemului IT**	13. Gradul de realizare a subsistemelor informatice stabilite prin plan	
		14. Existența controalelor generale la nivelul subsistemelor IT	
		15. Funcționalitatea subsistemelor în rețea	
		16. Situația licențelor pentru programele de calculator	
		17. Asigurarea integrării subsistemelor componente	
		18. Elaborarea manualelor de utilizare şi a manualelor de operare	
		19. Instruirea utilizatorilor subsistemelor IT	

Nr. crt.	DOMENIUL	OBIECTE AUDITABILE	OBS.
IV.	**Securitatea IT**	20. Politica de securitate IT	
		21. Monitorizarea implementării politicii de securitate IT	
		22. Evaluarea controalelor fizice în domeniul IT	
		23. Siguranța accesului la rețea și a comunicării datelor în rețea	
		24. Programe antivirus	
		25. Recuperarea datelor în caz de dezastru	
		26. Sistemul de arhivare	

Nota:

Lista centralizatoare a obiectelor auditabile ***reprezintă primul document care se elaborează în cadrul*** *procedurii Analiza riscurilor* ***și cuprinde, pentru acest studiu de caz, 26 de obiecte auditabile, structurate pe 4 obiective, care vor fi analizate pe parcursul derulării misiunii de audit intern.***

Procedura - P05 : Analiza riscurilor

ENTITATEA PUBLICĂ
Compartimentul Audit Intern

IDENTIFICAREA RISCURILOR

Misiunea de audit: Tehnologia informației
Perioada auditată: 01.01.2005- 31.12.2005
Întocmit: Popescu Sorin/Radu George **Data:** 20.01.2006
Avizat: Dumitru Daniel **Data:** 20.01.2006

Nr. crt	DOMENIUL	OBIECTE AUDITABILE	RISCURI SEMNIFICATIVE	OBS.
I.	Plan strategic	1. Politicile entității publice în domeniul IT	1. Inexistența unei atitudini favorabile în privința informatizării activității entității publice	
		2. Modalitatea de elaborare a planului strategic şi a planurilor anuale	2. Fundamentarea insuficientă a planului	
			3. Necorelarea planurilor anuale	
			4. Lipsa prioritizării activităților	
		3. Subsistemele informatice pentru funcțiile principale	5. Neacoperirea domeniilor de activitate ale entității publice cu subsisteme informatice	
			6. Necorelarea termenelor previzionate de realizare a subsistemelor	
			7. Nedefinirea responsabilităților	
			8. Insuficienta previzionare a resurselor	
		4. Integrarea subsistemelor informatice	9. Incompatibilitatea subsistemelor informatice	
		5. Stabilirea responsabililor cu elaborarea si actualizarea planului	10. Nedesemnarea responsabilului cu elaborarea planului	
			11. Nestabilirea persoanei responsabile cu actualizarea planului	
		6. Aprobarea planului	12. Planul nu este aprobat	
			13. Planul nu este aprobat de persoanele competente	
			14. Coordonarea neadecvată a planurilor	
II.	Organizarea şi funcționarea departamentului IT	7. Organizarea departamentului IT	15. Departamentului IT nu este subordonat unui nivel managerial corespunzător	
			16. Inexistența şi/sau neaprobarea organigramei	
			17. Neformalizarea procedurilor specifice activităților desfăşurate	
			18. Existența unui număr mare de posturi de conducere deținute cu delegație	
			19. Număr mare de posturi de execuție neocupate	
			20. Personal de execuție neadecvat	

Nr. crt	DOMENIUL	OBIECTE AUDITABILE	RISCURI SEMNIFICATIVE	OBS.
			21. Dotare cu hard şi soft inadecvat pentru desfăşurarea activităţilor specifice	
			22. Inexistenţa unui sistem de control managerial la nivelul departamentului	
			23. Neefectuarea monitorizării modului de realizare a obiectivelor generale şi specifice ale departamentului	
		8. Stabilirea responsabilităţilor prin fişele posturilor	24. Neactualizarea fişelor posturilor	
			25. Nerespectarea principiului segregării sarcinilor de serviciu	
			26. Necuprinderea atribuţiilor stabilite prin ROF în fişele posturilor	
		9. Calificarea şi pregătirea salariaţilor	27. Calificarea necorespunzătoare/insuficientă a personalului	
		10. Pregătirea profesională continuă	28. Inexistenţa planurilor de pregătire profesională continuă	
			29. Neaprobarea planurilor de pregătire profesională ontinuă	
			30. Nerealizarea activităţilor previzionate prin planurile de pregătire profesională continuă	
		11. Sistemul de evaluare a personalului	31. Inexistenţa unui sistem de evaluare anuală a salariaţilor	
			32. Nerealizarea evaluării pe parcursul anului a salariaţilor departamentului	
			33. Evaluarea formală a personalului	
		12. Sistemul de gestionare a riscurilor – conducerea Registrului riscurilor	34. Inexistenţa unei politici unitare privind gestionarea riscurilor	
			35. Inexistenţa unui responsabil privind gestionarea riscurilor	
			36. Nedesemnarea unei persoane responsabilă cu elaborarea şi monitorizarea Registrului riscurilor	
			37. Neactualizarea sistematică a Registrului riscurilor	
III.	Implementarea sistemului IT	13. Gradul de realizare a subsistemelor informatice stabilite prin plan	38. Lipsă de coordonare a aplicaţiilor ce rulează în sistemul informatic	
			39. Nealocarea corespunzătoare a resurselor necesare realizării subsistemelor informatice	
			40. Evoluţii tehnologice cu implicaţii asupra îndeplinirii planului	
			41. Modificarea cadrului legal şi procedural ce reglementează activităţile pentru care se realizează subsistemele informatice	
		14. Complementaritatea subsistemelor informatice	42. Implicaţiile evoluţiilor tehnologice în domeniul IT	
			43. Modificarea cadrului legal şi procedural ce reglementează activităţile pentru care se realizează subsistemele informatice	
		15. Funcţionalitatea subsistemelor în reţea	44. Inexistenţa unei politici de transmitere a datelor în reţea	

Nr. crt	DOMENIUL	OBIECTE AUDITABILE	RISCURI SEMNIFICATIVE	OBS.
			45. Implicațiile evoluțiilor tehnologice în domeniul IT	
		16. Situația licențelor pentru programele de calculator	46. Limitări bugetare în privința achiziționării licențelor	
			47. Disfuncționalități în procesul de achiziționare al licențelor	
		17. Asigurarea integrării subsistemelor componente	48. Modificarea cadrului legal şi procedural ce reglementează activitățile pentru care se realizează subsistemele informatice	
			49. Evoluții tehnologice cu implicații asupra integrării subsistemelor	
			50. Neconcordanțe în integrarea subsistemelor	
		18. Elaborarea manualelor de utilizare şi a manualelor de operare	51. Inexistența/Insuficiența manualelor de utilizare şi a manualelor de operare	
			52. Lipsa unor componente şi existența unor elemente neclarificate în conținutul manualelor	
		19. Instruirea utilizatorilor subsistemelor IT	53. Inexistența unui program de instruire al utilizatorilor	
			54. Neefectuarea instruirii sistematice a utilizatorilor subsistemelor IT	
IV.	Securitatea IT	20. Politica de securitate IT	55. Inexistența politicii de securitate	
			56. Neaplicarea politicii de securitatea în mod consecvent	
		21. Monitorizarea implementării politicii de securitate IT	57. Inexistența unui responsabil desemnat cu monitorizarea implementării politicii de securitate IT	
			58. Neântocmirea şi netransmiterea sistematică a rapoartelor de monitorizare	
			59. Inexistența unui sistem de clasificare şi protejare adecvată a informațiilor confidențiale existente în format electronic	
		22. Evaluarea controalelor fizice în domeniul IT	60. Lipsa procedurilor privind implementarea controalelor fizice în domeniul IT	
			61. Nedesemnarea responsabilității pentru monitorizarea controalelor fizice	
			62. Lipsa unor proceduri pentru realizarea controalelor fizice	
			63. Neefectuarea controalelor fizice conform procedurilor	
		23. Siguranța accesului la rețea şi a comunicării datelor în rețea	64. Lipsa procedurilor privind siguranța accesului utilizatorilor în rețea	
			65. Inexistența responsabilului desemnat cu monitorizarea implementării procedurilor privind siguranța accesului utilizatorilor în rețea	
			66. Neefectuarea monitorizării sistematice	
			67. Neimplementarea măsurilor privind siguranța accesului utilizatorilor în rețea conform procedurilor	

Nr. crt	DOMENIUL	OBIECTE AUDITABILE	RISCURI SEMNIFICATIVE	OBS.
		24. Programe antivirus	68. Lipsa procedurilor privind implementarea programelor antivirus	
			69. Inexistența responsabilului desemnat cu monitorizarea implementării procedurilor privind implementarea programelor antivirus	
			70. Neefectuarea monitorizării sistematice	
			71. Neluarea măsurilor necesare privind implementarea programelor antivirus conform procedurilor	
		25. Recuperarea datelor în caz de dezastru	72. Lipsa procedurilor privind recuperarea datelor în caz de dezastru	
			73. Inexistența responsabilului desemnat cu monitorizarea implementării procedurilor privind recuperarea datelor în caz de dezastru	
			74. Neefectuarea monitorizării sistematice	
			75. Neluarea măsurilor necesare privind recuperarea datelor în caz de dezastru conform procedurilor	
		26. Sistemul de arhivare	76. Lipsa procedurilor privind arhivarea datelor	
			77. Nedesemnarea responsabilității pentru arhivarea datelor	
			78. Neefectuarea evaluării periodice a activității de arhivare	

Nota:

Identificarea riscurilor ***este al doilea document care se elaborează în cadrul procedurii*** *Analiza riscurilor* ***şi presupune asocierea riscurilor semnificative la operațiilor stabilite în*** *Lista centralizatoare a obiectelor auditabile.* ***De regulă, se asociază unul sau mai multe riscuri posibile, determinate de auditorii interni pe baza informațiilor colectate dar si din riscurile practice reieşite din propria experiență. În situația în care la operațiile auditabile se ataşează mai multe riscuri analiza acestora se va putea realiza pentru fiecare risc în parte sau pe total operație/obiect auditabil.***

În acest studiu de caz, au fost identificate 26 de operații auditabile, prezentate în *Lista centralizatoare a obiectelor auditabile,* ***cărora le-au fost ataşate 78 riscuri, aşa cum rezultă din documentul*** *Identificarea riscurilor.*

Procedura – P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Compartimentul Audit Intern

CHESTIONAR DE CONTROL INTERN

Misiunea de audit: Tehnologia informației
Perioada auditată: 01.01.2005 – 01.05.2006
Întocmit: Popescu Sorin / Radu George **Data:** 25.01.2006
Avizat: Dumitru Daniel **Data:** 25.01.2006

ACTIVITATEA DE AUDIT	DA	NU	OBS.
Obiectivul I. PLAN STRATEGIC			
1.1 Procedurile privind planul strategic			
- Activitățile întreprinse concură la realizarea planului strategic?	X		
1.2 Definirea responsabilitatilor în mod oficial			
- În politicile entității publice sunt definite clar obiectivele şi care sunt măsurile necesare ce trebuiesc implementate?	X		
- Există structuri manageriale care să administreze şi să monitorizeze atingerea acestor obiective?	X		
- Este desemnat un grup de lucru responsabil pentru actualizarea planului?	X		
1.3 Acoperirea prin plan a tuturor domeniilor entității publice			
– Entitatea publică a elaborat un plan strategic ?	X		
– Există strategii elaborate de fiecare departament şi susțin aceste strategii planul?		X	Departamentele înființate după elaborarea planului strategic nu sunt luate în calcul prin planul strategic
– Au fost corelate prin plan termenele de realizare a subsistemelor IT?	X		
1.4 Existența unui sistem IT prevăzut pentru fiecare activitate principală			
- Planul strategic IT acoperă toate procesele care se desfăşoară în cadrul entității publice?		X	Planul trebuie actualizat potrivit schimbărilor legislative apărute
1.4 Aprobarea planului de managementul general			
– A fost planul aprobat de managementul general?	X		
– Este personalul de conducere al departamentelor implicat în aprobarea planului?	X		
1.5 Verificarea în mod periodic a stadiul de implementare a planului			
- Există procedură de verificare a stadiului de realizare al planului?	X		
1.6 Actualizarea planului			
- Este planul actualizat periodic?	X		S-a constatat necesitatea actualizării planului şi în timpul anului în curs
1.7 Alocarea resurselor necesare pentru realizarea obiectivelor stabilite prin plan			
- Sunt identificate resursele necesare pentru fiecare element al planului strategic ?	X		

ACTIVITATEA DE AUDIT	DA	NU	OBS.
- Există resursele necesare?	X		
1.8 Documentarea şi fundamentarea planului strategic			
- Este planul documentat şi fundamentat?	X		
Obiectivul II. MANAGEMENT ŞI ORGANIZARE IT			
2.1 Organizarea departamentului IT			
- Există o organigramă oficială aprobată de management?	X		
- Sunt toate posturile de conducere ocupate?		X	
- Sunt toate posturile de execuţie ocupate?		X	
- Se iau măsuri de ocupare a posturilor vacante?	X		
2.2 Definirea responsabilităţilor salariaţilor în fişele posturilor			
- Există fişe ale posturilor pentru întregul personal care să definească în mod clar sfera obligaţiilor?	X		
- Cuprind fişele posturilor atribuţiile şi responsabilităţile ce le revin salariaţilor în activitatea de zi cu zi?	X		
2.3 Există o separare a sarcinilor de serviciu?			
- Există o separare a sarcinilor pentru funcţiile de:			
▪ Proiectare a sistemelor?	X		
▪ Testare a sistemelor?	X		
▪ Implementare a sistemelor?	X		
• Sisteme de operare curente?	X		
2.4 Asigurarea pregătirii profesionale continue a salariaţilor			
- Există planuri de pregătire profesională continuă?		X	
- Salariaţii participa la cursuri de perfecţionare?	X		
- Pregătirea profesionala a salariaţilor se realizează conform atribuţiilor şi responsabilităţilor stabilite prin fişa postului?	X		
2.5 Managementul riscului			
- Există un proces fo rmalizat de management al riscului?		X	
- Au fost riscurile identificate şi evaluate?		X	
- S-au adoptat măsuri adecvate de gestionare a riscurilor majore?		X	
- Este Registrul riscurilor ţinut la zi?	X		
Obiectivul III. IMPLEMENTAREA SISTEMULUI IT			
3.1 Gradul de realizare al subsistemelor IT stabilite prin plan			
- Există un sistem procedurat de realizare a subsistemelor IT?	X		
- Subsistemele IT au fost realizate la termenele stabilite?		X	
3.2 Asigurarea integrării subsistemelor IT			
- Specificaţiile privind cerinţele sistemului IT ţin cont de subsistemele existente şi de necesitatea de a le integra?	X		
- Există un administrator de sistem care să asigure dezvoltarea, întreţinerea şi integrarea sistemelor?	X		
- Se efectuează testarea implementării tuturor subsistemelor IT noi?	X		
3.3 Existenţa controalelor generale de sistem la nivelul subsistemelor IT			
- Există un control adecvat din punct de vedere temporal al înregistrărilor?	X		
- Sunt tranzacţiile autorizate în mod explicit prin mijloace manuale sau electronice?		X	
- Sunt funcţiunile de introducere de date şi de autorizare restricţionate şi separate?		X	
- Introducerea parametrilor şi a altor date permanente ce urmează a fi procesate este controlată în mod strict?		X	
- În etapa de introducere, este validat caracterul complet şi corect al datelor?		X	
- Există proceduri clare pentru elemente de date respinse la introducere?		X	

ACTIVITATEA DE AUDIT	DA	NU	OBS.
- Există orare clare pentru introducerea datelor şi sunt acestea respectate?		X	
- Aveţi un sistem pentru detectarea posibilelor înregistrări duble?	X		
- Există o planificare a procesării şi este aceasta înțeleasă de utilizatori şi personalul operativ?		X	
- Sunt toate datele, inclusiv cele transferate din alte sisteme, supuse validării în timpul prelucrării?		X	
- Programele furnizează confirmări cu privire la finalizarea cu succes a procesării sau există proceduri de recuperare şi de reintroducere în cazul opririlor anormale?		X	Programele nu furnizează în toate cazurile confirmări cu privire la finalizarea cu succes a procesării
- Se confirmă prelucrarea integrală a procesărilor?		X	
- Există proceduri pentru gestionarea înregistrărilor respinse de programele de aplicații?		X	
- Există personal responsabil de gestionarea rezultatelor, de verificarea şi de asigurarea caracterului complet şi acceptabil al acestora?	X		
- Când înregistrările sunt trecute dintr-un subsistem IT în altul, sunt cele introduse în al doilea armonizate cu cele produse de primul?		X	
- Atunci când înregistrările sunt respinse la transferarea între sisteme, pot ele fi identificate şi cercetate?	X		
- Sunt utilizatorii responsabili de introducerea, modificarea sau ştergerea înregistrărilor în cadrul sistemului?	X		
- În cazul existenței unor rapoarte privind pista de audit sunt acestea complete iar rapoartele indică dacă şi când sunt oprite mecanismele de urmărire?		X	Nu există rapoarte privind pista de audit
- Sunt fişierele salvate în back up la intervale regulate în timpul prelucrării pentru a permite recuperarea operațiunilor?	X		
- Sunt efectuate verificări periodice ale integrității bazelor de date şi se reţin copii de siguranță ale bazelor de date de la o verificare la alta?	X		
- Instrucțiunile operatorilor şi utilizatorilor specifică în mod clar procedurile de urmat în cazul unei deficiențe a aplicației în timpul prelucrării?	X		
3.4 Funcționalitatea subsistemelor IT în rețea			
- Sunt păstrate statistici cu privire la funcționare şi performanță?	X		
- Sunt statisticile analizate în mod regulat pentru a identifica problemele de funcționare?	X		
- Există procese prin care să se asigure remedierea deficiențelor de funcționare?	X		
3.5 Situația licențelor pentru aplicații			
- Există licențe pentru toate copiile programelor nelaborate în cadrul entității publice?		X	
- Există un proces pentru evaluarea regulată a necesarului de licențe?		X	
3.6 Instruirea utilizatorilor este asigurată?			
- Există manuale de utilizare?	X		
- Instruirea utilizatorilor se realizează conform unor programe bine stabilite?		X	
- Este utilizată o gamă largă de metode de instruire, inclusiv practică?		X	
Obiectivul IV. SECURITATEA IT			
4.1 Există o politică de securitate IT?			
Există documente de politică privind securitatea informației?	X		
Este politica de securitate IT aprobată de conducerea superioară?	X		

ACTIVITATEA DE AUDIT	DA	NU	OBS.
Există persoane responsabile cu monitorizarea respectării politicii?	X		
Politica defineşte securitatea informaţiei şi principiile de securitate care trebuie urmate de către personal?	X		
Securitatea informaţiei impune: - Realizarea unei analize de risc în mod regulat - Desemnarea unui responsabil cu instalarea computerelor şi/sau sistemelor - Ca personalul să fie conştient cu privire la siguranţa informaţiei - Respectarea licenţelor pentru programe, şi a obligaţiilor legale, reglementare şi contractuale - Raportarea încălcării politicii de securitate şi a deficienţelor securităţii - Protejarea informaţiei în termenii cerinţelor acestora de confidenţialitate, integritate şi disponibilitate?	X		
Politica de securitate interzice: - utilizarea informaţiilor şi sistemelor organizaţiei fără autorizaţie şi pentru scopuri care nu au legătură cu munca - afirmaţiile cu conotaţii obscene, discriminatorii sau abuzive, care pot fi ilegale (ex prin utilizarea e-mail sau Internet) - descărcarea unor materiale ilegale (ex cu conţinut obscen sau discriminatoriu) - scoaterea informaţiei sau echipamentelor din sediu fără autorizare - utilizarea neautorizată a informaţiei, infrastucturii sau echipamentelor - copierea neautorizată a informaţiei/programelor - compromiterea parolelor (ex prin notarea lor pe documente lăsate pe birou sau divulgarea lor către alte persoane) - utilizarea informaţiilor prin care pot fi identificate persoane în scopuri de afaceri şi fără autorizare expresă - discutarea informaţiilor legate de afaceri în locuri publice - falsificarea probelor în cazul unui incident	X		
Politica de securitate a informaţiei specifică faptul că utilizatorii sunt obligaţi: - să închidă mijloacele sau documentaţia importantă când nu sunt utilizate (adică se respectă politica 'mesei de lucru curate') - să iasă din sistem atunci când un terminal urmează să fie lăsat nesupravegheat (ex în timpul unor întâlniri, a pauzei de masă, sau pe timpul nopţii)?	X		
Politica de securitate a informaţiei este: - comunicată întregului personal şi părţilor externe cu acces la informaţiile şi sistemele întreprinderii - revizuită periodic conform unui proces de revizuire definit - complectată prin asimilarea modificărilor apărute?	X		
Politica de securitate a informaţiei specifică faptul că acţiuni disciplinare pot fi luate împotriva persoanelor care încalcă prevederile sale?	X		
4.2 Este stabilită răspunderea pentru monitorizarea implementării politicii?			
Există o persoană din conducerea superioară cu responsabilitate generală pentru securitatea informaţiei?	X		
Există un grup de lucru de nivel înalt, comitet sau organism echivalent însărcinat cu coordonarea activităţii de securitate a informaţiei în întreaga organizaţie?			
Grupul se întâlneşte în mod regulat (ex de trei ori sau de mai multe ori pe an) şi elaborează rapoarte cuprinzând acţiunile stabilite în cadrul întâlnirii?	X		
• Din grupul de lucru la nivel înalt fac parte:		X	

ACTIVITATEA DE AUDIT	DA	NU	OBS.
- persoane din conducere superioară (adică un director al consiliului sau al unui organism echivalent) - unul sau mai mulți „responsabili" de activități (adică persoane însărcinate cu diferite arii funcționale) - şeful securității informației sau echivalent - reprezentanți ai altor funcții interesate (ex. audit intern, asigurări, personal, securitate fizică) - seful IT, sau echivalent?			
• Grupul de lucru de nivel înalt este responsabil pentru: - luarea în considerare a intereselor privind securitatea informației pentru toate părțile organizației - asigurarea tratării intereselor privind securitatea informației într-o manieră coerentă şi consecventă - aprobarea politicilor şi standardelor / procedurilor de securitate a informației - monitorizarea performanțelor securității informației şi a expunerii organizației la amenințări la adresa securității informației - aprobarea şi stabilirea priorităților activității de îmbunătățire a securității informației - asigurarea cuprinderii securității informației în procesul de planificare a informației la nivel de organizație - coordonarea implementării instrumentelor de control aferente securității informației în noile sisteme şi servicii - accentuarea importanței securității informației în cadrul organizației?	X		
4.3 Există instrumente de contro fizice aplicate mediului IT?			
• Este proiectarea instalației susținută de standarde/proceduri documentate, care necesită: - ca modul de concepere să țină cont de cerințele activității utilizatorilor şi să fie consecvent cu alte sisteme utilizate de organizație - ca sistemul să fie conceput în aşa fel încât să suporte situații previzibile în utilizarea sistemului IT de către organizație?	X		
• Sunt mediile de lucru curente separate de activitatea de testare a dezvoltării şi recepției prin depozitarea utilităților sistemului departe de mediul curent atunci când nu sunt în uz, şi prin utilizarea unor camere pentru calculatoare, procesoare, domenii şi partiții separate?	X		
• Este accesul fizic restricționat la sistemele de calculatoare restricționat personalului autorizat prin: - Instalarea de încuietori acționate cu carduri sau echivalent - Încuierea uşilor/ferestrelor atunci când mediul este eliberat - Instalarea de alarme împotriva efracției - Asigurarea purtării de către toate persoanele a unor mijloace vizibile de identificare - Angajarea de personal de pază ?	X		
• În cadrul sistemului, este: - restricționat accesul fizic la telefoane /fax şi echipamentele utilizate pentru tipărire - mijloacele şi documentația de importanță critică sunt în siguranță atunci când nu sunt în uz (ex. ca parte a politicii 'mesei de lucru curată') - sistemele de detectare a accesului neautorizat instalat pe uşile exterioare şi pe ferestrele accesibile sunt verificate periodic - calculatoarele portabile şi componentele lor (ex. PC-uri, chip-uri de memorie) sunt protejate împotriva furtului (ex. prin marcarea	X		

ACTIVITATEA DE AUDIT	DA	NU	OBS.
permanentă a echipamentelor vulnerabile sau fixarea calculatoarelor pe mese sau pe standurile de echipamente). - vizitatorii sistemului: - au acces numai pentru scopuri clare şi autorizate - sunt monitorizaţi prin înregistrarea orei sosirii şi a plecării - sunt supravegheaţi permanent - sunt instruiţi cu privire la cerinţele de siguranţă ale zonei, detaliindu-se procedurile de urgenţă şi li se atrage atenţia că orice timp de înregistrare (ex. filmare sau fotografiere) este interzisă.			
- Sunt echipamentele şi facilităţile critice protejate prin situarea lor în afara zonelor de acces public şi prin păstrarea confidenţialităţii detaliilor cu privire la acestea?	X		
- Este accesul fizic în camerele care adăpostesc echipamente şi facilităţi critice protejate prin: - definirea şi întărirea perimetrului de securitate fizică - păstrarea camerelor sub supraveghere continuă - poziţionarea echipamentelor (ex. PC-uri) astfel încât informaţiile critice să nu poată fi observate	X		
- Autorizaţiile pentru acces fizic la instalaţii sunt: - emise în conformitate cu standardele /procedurile documentate - revizuite periodic pentru a se asigura accesul la acestea numai a persoanelor potrivite - revocate imediat ce nu mai sunt necesare?	X		
4.4 Comunicaţiile de date în format electronic sunt sigure?			
- Există o strategie pentru utilizarea continuu eficientă, eficace şi sigură a facilităţilor reţelei?	X		
- Este responsabilitatea pentru administrarea reţelei definită clar?	X		
- Sunt utilizatorii reţelei instruiţi cu privire la utilizarea reţelei şi securitatea acesteia?		X	
- Administratorii de reţea primesc instruire adecvată şi potrivită cu privire la siguranţa şi controlul reţelei?	X		
- Sunt informaţiile privind standardele tehnice şi configurarea facilităţilor reţelei documentate în mod clar?	X		
- Este activitatea în reţea monitorizată pentru a se asigura că securitatea transferului de date nu a fost afectată?	X		
- Sunt prevederile de service pentru reţea complet documentate, susţinute, monitorizate şi acceptate de toate părţile?	X		
- Există proceduri pentru aprobarea şi instalarea conexiunilor la reţea?	X		
- Pot doar utilizatorii autorizaţi să efectueze conexiuni la reţea şi există proceduri pentru verificarea conexiunilor neautorizate?	X		
- Este utilizarea reţelei monitorizată pentru a verifica conexiunile neautorizate la reţea şi echipamentele care funcţionează (sau sunt utilizate) în mod incorect?	X		
- Este codificarea utilizată pentru a preveni accesul neautorizat la datele transmise prin reţea?	X		
- Sunt reţelele proiectate şi construite pentru a mări la maximum eficienţa traficului de date?	X		
- Există aranjamente pentru întreţinerea şi asigurarea componentelor fizice, infrastructurii de comunicaţii, programelor de administrare a reţelei şi a pierderii cu consecinţe importante?	X		
- Sunt programele de administrare a reţelei şi fişierele de date de pe fiecare server de date şi echipament al reţelei salvate pentru siguranţă în mod regulat şi copii ale acestora păstrate în locuri sigure?	X		
- Există metode de recuperare şi de continuare a activităţii în	X		

ACTIVITATEA DE AUDIT	DA	NU	OBS.
eventualitatea defectării a liniilor şi nodurilor de reţea?			
- Este accesul fizic la domeniile critice ale reţelei (ex. centrele de operare a reţelei, camerele echipamentelor, camerele de echipamente, firewalls) restricţionat numai la personalul autorizat. Terţii, cum ar fi furnizorii sau inginerii de service ar trebui supravegheaţi atunci când au acces la echipamentele de comunicaţii.	X		
- Sunt zonele critice, cum ar fi centrele de operare a reţelei şi camerele care adăpostesc echipamente importante ale reţelei (inclusiv cele aflate la distanţă), protejate împotriva: - Riscurilor naturale, cum ar fi incendiul şi inundaţiile - Penelor de curent (ex. prin utilizarea unor surse de curent permanente şi a acumulatorilor) - Accesului neautorizat (ex. prin instalarea de încuietori la uşi şi a jaluzelelor la ferestre).	X		
- Sunt cablurile de comunicaţii protejate prin intermediul: ascunderii sistemului, tevilor, puncte de inspecţie/închidere încuiate, alimentare şi rutare alternative, evitarea rutelor prin spaţii accesibile publicului?	X		
- Există proceduri implementate pentru monitorizarea şi cercetarea încercărilor de acces neautorizat?	X		
- Performanţa sistemelor este monitorizată comparativ cu obiectivele agreate prin revizuirea utilizării curente în orele normale şi de vârf utilizând programe de monitorizare automată prin revizuirea jurnalelor de activitate ale sistemului, în mod regulat prin investigarea obstacolelor/ supraîncărcării.	X		
- Există activităţi de planificare a capacităţii efectuate pentru a permite asigurarea unei capacităţi suplimentare înainte de apariţia obstacolelor / supraîncărcării	X		
- Este disponibilitatea sistemului (adică timp de răspuns şi de funcţionare) măsurată din punctul de vedere al utilizatorilor activităţii, spre exemplu prin monitorizarea performanţei staţiilor de lucru.	X		
- Este monitorizarea efectuată periodic, inclusiv: ▪ scanarea sistemelor gazdă pentru punctele vulnerabile cunoscute, cum ar fi prin utilizarea instrumentelor automate (de exemplu programe: Nessus, Pingware) ▪ dacă utilităţile /comenzile puternice au fost dezactivate pe sistemele gazdă corelate (ex. prin utilizarea unui 'sniffer') ▪ - verificarea existenţei unor configurări de reţele wireless neautorizate.	X		
- Sunt utilizate mecanismele de detectare a accesului neautorizat, inclusiv: ▪ -detectarea caracteristicilor atacurilor cunoscute (ex. refuzul serviciului sau supraîncărcarea sistemelor buffer) ▪ un proces pentru efectuarea regulată a actualizării programelor de detectarea a intruziunilor, pentru incorporarea noilor caracteristici sau a caracteristicilor actualizate. ▪ furnizarea de alerte atunci când este detectată o activitate suspectă, susţinută de procese documentate pentru răspuns la intruziunile suspectate ▪ - protejarea mecanismelor de detectare a intruziunilor împotriva atacurilor, cum ar fi izolarea pe un sistem separat.	X		
- Sunt rapoartele de utilizare de la furnizorii de servicii (ex. facturi) verificate pentru a descoperi orice utilizare neobişnuită a sistemelor.	X		
- Sunt rezultatele activităţilor de monitorizare revizuite de conducerea IT şi prezentate conducerii utilizatorului căruia îi sunt furnizate	X		

ACTIVITATEA DE AUDIT	DA	NU	OBS.
serviciile.			
- Există jurnale de înregistrare a activităților pentru identificarea modificărilor neautorizate?			
- Sunt înregistrate toate evenimentele cheie în cadrul rețelei?	X		
- Conducerea IT autorizează înregistrarea activităților şi revizuirea procesului care urmează a fi aplicat (ex. frecvența revizuirilor şi răspunderea pentru efectuarea acestora).	X		
- Sunt înregistrările active tot timpul şi protejate de suprascriere intenționată sau accidentală? Mecanismele trebuie să fie stabilite astfel încât atunci când înregistrările privind evenimentele devin sisteme depline acestea nu sunt oprite din lipsă de spațiu pe disc şi înregistrarea va continua cu minimă oprire sau chiar fără.	X		
- Înregistrările evenimentelor conțin detalii ale: timpilor de pornire /oprire pentru sisteme şi procese cheie, înregistrarea cu succes a utilizatorilor autorizați în sistem şi încercările eşuate de înregistrare, situații de eroare şi de excepție, acces sau schimbări ale fişierelor şi programelor, acces la capacitățile privilegiate.	X		
- Există informații suficiente înregistrate pentru a identifica: Nume de utilizator individuale, programe speciale şi informații accesate data/ora accesării, căile de acces (inclusiv calculatoare/porturi de la care a fost obținut accesul), modele de acces pentru a permite urmărirea tranzacțiilor sau activitatea unui anumit utilizator schimbarea parametrilor de înregistrare în sistem	X		
- Sunt înregistrările păstrate destul timp pentru a respecta cerințele legale/ale organismelor de reglementare şi pentru a fi revizuite periodic. Revizuirea înregistrărilor va fi: susținută de proceduri /standarde documentate, fundamentată pe o evaluare avizată a impactului unor evenimente individuale asupra activității efectuată cu instrumente automate.	X		
4.5 Există un program antivirus?			
- Există standarde /proceduri documentate pentru protecție împotriva viruşilor care să specifice: - modul de configurare a programului antivirus - mecanismele de actualizare a programului antivirus - proces pentru gestionarea atacurilor cu virus	X		
- Este programul de protecție împotriva viruşilor configurat pentru a: ▪ scana memoria calculatoarelor, fişierele executabile (inclusiv fişierele macro de pe programul desktop), fişierele protejate (ex. fişierele comprimate şi cele protejate de parole) şi mediile de înmagazinare amovibile ▪ scana traficul de date (intrare/ieşire) inclusiv e-mail şi descărcarea de fişiere de pe Internet) ▪ fi activ permanent ▪ emite o alertă atunci când este suspectat un virus ▪ dezinfecta, şterge sau pune în carantină viruşii identificați ▪ asigura că nu pot fi dezactivate caracteristicile de protecție împotriva viruşilor şi nu poate fi redusă funcționalitatea principală.	X		
- Se efectuează verificări regulate pentru a asigura că: ▪ Programul de protecție împotriva viruşilor nu a fost dezafectat ▪ Configurarea programului de protecție împotriva viruşilor este corectă ▪ Au fost aplicate efectiv toate actualizările.		X	

ACTIVITATEA DE AUDIT	DA	NU	OBS.
- Sunt utilizatorii: - avertizaţi cu privire la pericolul reprezentat de viruşi - atenţionaţi rapid cu privire la noi riscuri de virusare (ex. prin e-mail) - îndrumaţi să raporteze atacuri suspectate sau reale ale unor viruşi către un singur punct de contact şi asistenţă - permanent susţinuţi de experţi tehnici şi specialişti	X		
4.6 Planul de recuperare a datelor în caz de dezastru			
- A fost efectuată o cercetare şi o evaluare cu privire la impactul riscurilor asupra activităţii?	X		
- A fost pregătit şi aprobat de conducere un plan de recuperare în caz de dezastru ?	X		
- Au fost pregătite planuri pentru situaţii neprevăzute, cum ar fi defecţiuni de importanţă redusă?	X		
- Au fost planurile documentate şi transmise personalului cheie ?	X		
- A fost responsabilitatea privind recuperarea în caz de dezastru delegată unei echipe şi rolurile membrilor acesteia înregistrate?	X		
- Este planul de recuperare în caz de dezastru verificat periodic, reevaluat şi actualizat în lumina noilor schimbărilor intervenite în evaluarea riscurilor?	X		
- Au fost stabilite facilităţi de recuperare în caz de dezastru şi sunt acestea verificate periodic pentru a se asigura eficienţa, caracterul operaţional şi curent al acestora?	X		
- Sunt procedurile de recuperare luate în considerare în specificaţiile tehnice ale unei noi aplicaţii pentru calculator şi pentru a proteja sistemele în dezvoltare?	X		
- Sunt măsurile de salvare a informaţiilor esenţiale şi a programelor luate destul de frecvent pentru a îndeplini cerinţele activităţii?	X		
- Măsurile de realizare a copiilor de siguranţă permit programelor şi informaţiilor să fie restaurate in perioada de timp critică pentru aplicaţie (adică în punctul după care vor fi suferite pierderi inacceptabile).	X		
- Sunt copiile de siguranţă protejate împotriva pierderii, deteriorării şi accesului neautorizat prin: stocarea lor în seifuri ignifuge, aflate în locaţie, pentru a permite restaurarea rapidă a informaţiilor ; susţinerea lor prin copii păstrate în alte locaţii pentru a permite restaurarea sistemului prin utilizarea unor facilităţi alternative în caz de dezastru; restricţionarea accesului numai la personalul autorizat?	X		
4.7 Este arhivarea efectuată într-un mod sigur?			
- Există politici /standarde pentru arhivarea datelor din sistemul de procesare în timp real?	X		
- Sunt datele arhivate păstrate într-un loc de stocare sigur?	X		
- Sunt mediile de arhivare revizuite periodic pentru a stabili dacă acestea pot fi încă citite.	X		
- Există evidenţe cu privire la datele care sunt păstrate în arhive?	X		

ENTITATEA PUBLICĂ
Serviciul Audit Intern

STABILIREA FACTORILOR DE RISC, PONDERILE ACESTORA ŞI APRECIEREA NIVELURILOR RISCURILOR

Misiunea de audit**:** ***Tehnologia informației***
Perioada auditată: **01.01.2005- 31.12.2005**
Întocmit: **Popescu Sorin/Radu George** **Data: 20.01.2006**
Avizat: **Ionescu Mircea** **Data: 20.01.2006**

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

Notă:

Prin acest document se stabilesc, în funcție de importanța şi greutatea factorilor de risc, ponderile şi nivelurile de apreciere ale riscurilor.

Cei trei factori de risc sunt stabiliți prin normele generale şi sunt acoperitori pentru entitate, însă dacă se doreşte evidențierea şi 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 - P05 : Analiza riscurilor

ENTITATEA PUBLICĂ
Compartimentul Audit Intern

STABILIREA NIVELULUI RISCULUI ŞI A PUNCTAJULUI TOTAL AL RISCULUI

Misiunea de audit: Tehnologia informației
Perioada auditată: 01.01.2005 – 01.01.2006
Întocmit: Popescu Sorin / Radu George **Data:** 20.01.2006
Avizat: Dumitru Daniel **Data:** 20.01.2006

Nr. crt.	DOMENIUL	OBIECTE AUDITABILE	RISCURI SEMNIFICATIVE	Criterii de analiza a riscurilor						Punctaj total
				Aprecierea controlului intern (F1)		Aprecierea cantitativă (F2)		Aprecierea calitativă (F3)		
				P_1 50%	N_1	P_2 30%	N_2	P_3 20%	N_3	
I.	Plan strategic	1. Politicile entității publice în domeniul IT	Inexistența unei atitudini favorabile în privința informatizării activității entității publice	0,5	2	0,3	3	0,2	2	2,3
		2. Modalitatea de elaborare a planului strategic şi a planurilor anuale	Fundamentarea insuficientă a planului	0,5	2	0,3	2	0,2	3	2,2
			Necorelarea planurilor anuale	0,5	2	0,3	2	0,2	2	2,0
			Lipsa prioritizării activităților	0.5	2	0.3	2	0.2	2	2,0
		3. Subsistemele informatice pentru funcțiile principale	Neacoperirea domeniilor de activitate ale entității publice cu subsisteme informatice	0,5	3	0,3	3	0,2	2	2,8
			Necorelarea termenelor previzionate de realizare a subsistemelor	0,5	2	0,3	2	0,2	3	2,2
			Nedefinirea responsabilităților	0,5	2	0,3	3	0,2	1	2,1
			Insuficienta previzionare a resurselor	0,5	2	0,3	2	0,2	2	2,0
		4. Integrarea subsistemelor informatice	Incompatibilitatea subsistemelor informatice	0,5	1	0,3	2	0,2	2	1,5
		5. Stabilirea responsabililor cu elaborarea si actualizarea planului	Nedesemnarea responsabilului cu elaborarea planului	0,5	2	0,3	3	0,2	3	2,5
			Nestabilirea persoanei responsabile cu actualizarea planului	0,5	2	0,3	2	0,2	2	2,0

Nr. crt.	DOMENIUL	OBIECTE AUDITABILE	RISCURI SEMNIFICATIVE	Criterii de analiza a riscurilor						Punctaj total
				Aprecierea controlului intern (F1)		Aprecierea cantitativă (F2)		Aprecierea calitativă (F3)		
				P_1 50%	N_1	P_2 30%	N_2	P_3 20%	N_3	
		6. Aprobarea planului	Planul nu este aprobat	0,5	3	0,3	2	0,2	3	2,7
			Planul nu este aprobat de persoanele competente	0,5	3	0,3	3	0,2	2	2,8
			Coordonarea neadecvată a planurilor	0,5	1	0,3	3	0,2	2	1,8
II.	Organizarea şi funcționarea departamentului IT	7. Organizarea departamentului IT	Departamentului IT nu este subordonat unui nivel managerial corespunzător	0,5	2	0,3	2	0,2	2	2,0
			Inexistența și/sau neaprobarea organigramei	0,5	3	0,3	3	0,2	2	2,8
			Neformalizarea procedurilor specifice activităților desfășurate	0,5	2	0,3	2	0,2	3	2,2
			Existența unui număr mare de posturi de conducere deținute cu delegație	0,5	2	0,3	3	0,2	1	2,1
			Număr mare de posturi de execuție neocupate	0,5	3	0,3	1	0,2	2	2,3
			Personal de execuție neadecvat	0,5	2	0,3	2	0,2	3	2.2
			Dotare cu hard şi soft inadecvat pentru desfășurarea activităților specifice	0,5	2	0,3	2	0,2	2	2,0
			Inexistența unui sistem de control managerial la nivelul departamentului	0,5	2	0,3	2	0,2	2	2,0
			Neefectuarea monitorizării modului de realizare a obiectivelor generale şi specifice ale departamentului	0,5	1	0,3	3	0,2	2	1,8
		8. Stabilirea responsabilităților prin fişele posturilor	Neactualizarea fişelor posturilor	0,5	1	0,3	1	0,2	2	1,2
			Nerespectarea principiului segregării sarcinilor de serviciu	0,5	1	0,3	3	0,2	2	1,5
			Necuprinderea atribuțiilor stabilite prin ROF în fişele posturilor	0,5	1	0,3	2	0,2	1	1,3
		9. Calificarea şi pregătirea salariaților	Calificarea necorespunzătoare/insuficientă a personalului	0,5	1	0,3	2	0,2	1	1,3

Nr. crt.	DOMENIUL	OBIECTE AUDITABILE	RISCURI SEMNIFICATIVE	Criterii de analiza a riscurilor						Punctaj total
				Aprecierea controlului intern (F1)		Aprecierea cantitativă (F2)		Aprecierea calitativă (F3)		
				P_1 50%	N_1	P_2 30%	N_2	P_3 20%	N_3	
		10. Pregătirea profesională continuă	Inexistența planurilor de pregătire profesională continuă	0,5	2	0,3	2	0,2	1	1,8
			Neaprobarea planurilor de pregătire profesională continuă	0,5	2	0,3	2	0,2	2	2,0
			Nerealizarea activităților previzionate prin planurile de pregătire profesională continuă	0,5	3	0,3	2	0,2	1	2,3
		11. Sistemul de evaluare a personalului	Inexistența unui sistem de evaluare anuală a salariaților	0,5	1	0,3	2	0,2	2	1,5
			Nerealizarea evaluării pe parcursul anului a salariaților departamentului	0,5	1	0,3	1	0,2	2	1,2
			Evaluarea formală a personalului	0,5	1	0,3	2	0,2	1	1,3
		12. Sistemul de gestionare a riscurilor – conducerea Registrului riscurilor	Inexistența unei politici unitare privind gestionarea riscurilor	0,5	2	0,3	2	0,2	2	2,0
			Inexistența unui responsabil privind gestionarea riscurilor	0,5	2	0,3	3	0,2	2	2,3
			Nedesemnarea unei persoane responsabilă cu elaborarea şi monitorizarea Registrului riscurilor	0,5	2	0,3	2	0,2	2	2,0
			Neactualizarea sistematică a Registrului riscurilor	0,5	3	0,3	2	0,2	1	2,3
III.	Implementarea sistemului IT	13. Gradul de realizare a subsistemelor informatice stabilite prin plan	Lipsă de coordonare a aplicațiilor ce rulează în sistemul informatic	0,5	2	0,3	2	0,2	2	2,0
			Nealocarea corespunzătoare a resurselor necesare realizării subsistemelor informatice	0,5	3	0,3	3	0,2	1	2,6
			Evoluții tehnologice cu implicații asupra îndeplinirii planului	0,5	2	0,3	2	0,2	1	1,8

Nr. crt.	DOMENIUL	OBIECTE AUDITABILE	RISCURI SEMNIFICATIVE	Criterii de analiza a riscurilor						Punctaj total
				Aprecierea controlului intern (F1)		Aprecierea cantitativă (F2)		Aprecierea calitativă (F3)		
				P_1 50%	N_1	P_2 30%	N_2	P_3 20%	N_3	
			Modificarea cadrului legal şi procedural ce reglementează activităţile pentru care se realizează subsistemele informatice	0,5	3	0,3	1	0,2	1	2,0
		14. Existența controalelor generale la nivelul subsistemelor IT	Implicațiile evoluțiilor tehnologice în domeniul IT	0,5	2	0,3	2	0,2	2	2,0
			Modificarea cadrului legal şi procedural ce reglementează activităţile pentru care se realizează subsistemele informatice	0,5	2	0,3	1	0.2	3	1,9
		15. Funcționalitatea subsistemelor în rețea	Inexistența unei politici de transmitere a datelor în rețea	0,5	1	0,3	2	0,2	1	1,3
			Implicațiile evoluțiilor tehnologice în domeniul IT	0,5	1	0,3	2	0,2	2	1,5
		16. Situația licențelor pentru programele de calculator	Limitări bugetare în privința achiziționării licențelor	0,5	3	0,3	3	0,2	1	2,6
			Disfuncționalități în procesul de achiziționare al licențelor	0,5	3	0,3	2	0,2	1	2,3
		17. Asigurarea integrării subsistemelor componente	Modificarea cadrului legal şi procedural ce reglementează activităţile pentru care se realizează subsistemele informatice	0,5	1	0,3	2	0,2	1	1,3
			Evoluții tehnologice cu implicații asupra integrării subsistemelor	0,5	1	0,3	3	0,2	1	1,6
			Neconcordanțe în integrarea subsistemelor	0,5	1	0,3	2	0,2	3	1,7
		18. Elaborarea manualelor de utilizare şi a manualelor de operare	Inexistența/Insuficiența manualelor de utilizare şi a manualelor de operare	0,5	2	0,3	1	0,2	1	1,5
			Lipsa unor componente şi existența unor elemente neclarificate în conținutul manualelor	0,5	1	0,3	2	0,2	2	1,5
		19. Instruirea utilizatorilor subsistemelor IT	Inexistența unui program de instruire al utilizatorilor	0,5	2	0,3	3	0,2	3	2,5

Nr. crt.	DOMENIUL	OBIECTE AUDITABILE	RISCURI SEMNIFICATIVE	Criterii de analiza a riscurilor						Punctaj total
				Aprecierea controlului intern (F1)		Aprecierea cantitativă (F2)		Aprecierea calitativă (F3)		
				P_1 50%	N_1	P_2 30%	N_2	P_3 20%	N_3	
			Neefectuarea instruirii sistematice a utilizatorilor subsistemelor IT	0,5	2	0,3	2	0,2	1	1,8
IV.	Securitatea IT	20. Politica de securitate IT	Inexistența politicii de securitate	0,5	2	0,3	3	0,2	2	2,3
			Neaplicarea politicii de securitatea în mod consecvent	0,5	2	0,3	2	0,2	3	2,2
		21. Monitorizarea implementării politicii de securitate IT	Inexistența unui responsabil desemnat cu monitorizarea implementării politicii de securitate IT	0,5	3	0,3	3	0,2	2	2,5
			Neântocmirea şi netransmiterea sistematică a rapoartelor de monitorizare	0,5	2	0,3	2	0,2	2	2,0
			Inexistența unui sistem de clasificare şi protejare adecvată a informațiilor confidențiale existente în format electronic	0,5	2	0,3	1	0,2	3	1,9
		22. Evaluarea controalelor fizice în domeniul IT	Lipsa procedurilor privind implementarea controalelor fizice în domeniul IT	0,5	2	0,3	2	0,2	2	2,0
			Nedesemnarea responsabilității pentru monitorizarea controalelor fizice	0,5	3	0,3	2	0,2	2	2,5
			Lipsa unor proceduri pentru realizarea controalelor fizice	0,5	2	0,3	3	0,2	3	2,5
			Neefectuarea controalelor fizice conform procedurilor	0,5	3	0,3	3	0,2	1	2,6
		23. Siguranța accesului la rețea şi a comunicării datelor în rețea	Lipsa procedurilor privind siguranța accesului utilizatorilor în rețea	0,5	2	0,3	2	0,2	1	1,8
			Inexistența responsabilului desemnat cu monitorizarea implementării procedurilor privind siguranța accesului utilizatorilor în rețea	0,5	2	0,3	2	0,2	2	2,0
			Neefectuarea monitorizării sistematice	0,5	3	0,3	1	0,2	3	2,4

Nr. crt.	DOMENIUL	OBIECTE AUDITABILE	RISCURI SEMNIFICATIVE	Criterii de analiza a riscurilor						Punctaj total
				Aprecierea controlului intern (F1)		Aprecierea cantitativă (F2)		Aprecierea calitativă (F3)		
				P_1 50%	N_1	P_2 30%	N_2	P_3 20%	N_3	
			Neimplementarea măsurilor privind siguranța accesului utilizatorilor în rețea conform procedurilor	0,5	2	0,3	3	0,2	2	2,3
		24. Programe antivirus	Lipsa procedurilor privind implementarea programelor antivirus	0,5	3	0,3	2	0,2	3	2,7
			Inexistența responsabilului desemnat cu monitorizarea implementării procedurilor privind implementarea programelor antivirus	0,5	2	0,3	2	0,2	2	2,0
			Neefectuarea monitorizării sistematice	0,5	2	0,3	2	0,2	1	1,8
			Neluarea măsurilor necesare privind implementarea programelor antivirus conform procedurilor	0,5	2	0,3	3	0,2	3	2,5
		25. Recuperarea datelor în caz de dezastru	Lipsa procedurilor privind recuperarea datelor în caz de dezastru	0,5	2	0,3	2	0,2	2	2,0
			Inexistența responsabilului desemnat cu monitorizarea implementării procedurilor privind recuperarea datelor în caz de dezastru	0,5	2	0,3	3	0,2	1	2,1
			Neefectuarea monitorizării sistematice	0,5	3	0,3	1	0,2	2	2,2
			Neluarea măsurilor necesare privind recuperarea datelor în caz de dezastru conform procedurilor	0,5	3	0,3	2	0,2	1	2,3
		26. Sistemul de arhivare	Lipsa procedurilor privind arhivarea datelor	0,5	1	0,3	2	0,2	2	1,5
			Nedesemnarea responsabilității pentru arhivarea datelor	0,5	1	0,3	2	0,2	3	1,7
			Neefectuarea evaluării periodice a activității de arhivare	0,5	1	0,3	1	0,2	3	1,4

NOTA:

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

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

Unde:

T = punctaj total;

P_i = ponderea riscului pentru fiecare criteriu;

N_i = nivelul riscurilor pentru fiecare criteriu utilizat;

Evaluarea riscurilor asociate operaţiilor auditabile pe baza informaţiilor în posesia cărora a intrat auditorul intern, până în acest moment, din documentele primite de la entitate şi din rapoarte anterioare, dar şi din expertiza personală în domeniu şi este o evaluare cu un oarecare grad de subiectivitate.

Din aceste motive se recomandă ca auditorii interni să aibă în vedere posibilitatea îmbunătăţirii acestei lucrări pe durata misiunii de audit şi în special în etapa ***Intervenţiei la faţa locului****, funcţie de informaţiile, documentele şi probele de audit pe care le realizează.Procedura* ***Analiza riscurilor*** *se consideră a fi un "****document viu****" care poate fi actualizată permanent pe parcursul desfăşurării misiunii de audit intern.*

Procedura - P05 : Analiza riscurilor

ENTITATEA PUBLICĂ
Compartimentul Audit Intern

CLASAREA OPERAȚIILOR ÎN FUNCȚIE DE ANALIZA RISCULUI

Misiunea de audit: Tehnologia informației
Perioada auditată: 01.01.2005 – 31.12.2005
Întocmit: Popescu Sorin / Radu George **Data:** 20.01.2006
Avizat: Dumitru Daniel **Data:** 20.01.2006

Nr. crt.	DOMENIUL	OBIECTE AUDITABILE	RISCURI SEMNIFICATIVE	PUNCTAJ TOTAL	CLASARE	OBS.
I.	Plan strategic	1. Politicile entității publice în domeniul IT	1. Inexistența unei atitudini favorabile în privința informatizării activității entității publice	2,3	Mare	
		2. Modalitatea de elaborare a planului strategic şi a planurilor anuale	2. Fundamentarea insuficientă a planului	2,2	Mediu	
			3. Necorelarea planurilor anuale	2,0	Mediu	
			4. Lipsa prioritizării activităților	2,0	Mediu	
		3. Subsistemele informatice pentru funcțiile principale	5. Neacoperirea domeniilor de activitate ale entității publice cu subsisteme informatice	2,8	Mare	
			6. Necorelarea termenelor previzionate de realizare a subsistemelor	2,2	Mediu	
			7. Nedefinirea responsabilităților	2,1	Mediu	
			8. Insuficienta previzionare a resurselor	2,0	Mediu	
		4. Integrarea subsistemelor informatice	9. Incompatibilitatea subsistemelor informatice	1,5	Mic	Nu
		5. Stabilirea responsabililor cu elaborarea si actualizarea planului	10. Nedesemnarea responsabilului cu elaborarea planului	2,5	Mare	
			11. Nestabilirea persoanei responsabile cu actualizarea planului	2,0	Mediu	
		6. Aprobarea planului	12. Planul nu este aprobat	2,7	Mare	
			13. Planul nu este aprobat de persoanele competente	2,8	Mare	
			14. Coordonarea neadecvată a planurilor	1,8	Mediu	
II.	**Gestionarea şi organizarea**	7. Organizarea departamentului IT	15. Departamentului IT nu este subordonat unui nivel managerial corespunzător	2,0	Mediu	

Nr. crt.	DOMENIUL	OBIECTE AUDITABILE	RISCURI SEMNIFICATIVE	PUNCTAJ TOTAL	CLASARE	OBS.
	depart. IT		16. Inexistența şi/sau neaprobarea organigramei	2,8	Mare	
			17. Neformalizarea procedurilor specifice activităților desfăşurate	2,2	Mediu	
			18. Existența unui număr mare de posturi de conducere deținute cu delegație	2,1	Mediu	
			19. Număr mare de posturi de execuție neocupate	2,3	Mare	
			20. Personal de execuție neadecvat	2.2	Mediu	
			21. Dotare cu hard şi soft inadecvat pentru desfăşurarea activităților specifice	2,0	Mediu	
			22. Inexistența unui sistem de control managerial la nivelul departamentului	2,0	Mediu	
			23. Neefectuarea monitorizării modului de realizare a obiectivelor generale şi specifice ale departamentului	1,8	Mediu	
		8. Stabilirea responsabilităților prin fişele posturilor	24. Neactualizarea fişelor posturilor	1,2	Mic	Nu
			25. Nerespectarea principiului segregării sarcinilor de serviciu	1,5	Mic	Nu
			26. Necuprinderea atribuțiilor stabilite prin ROF în fişele posturilor	1,3	Mic	Nu
		9. Calificarea şi pregătirea salariaților	27. Calificarea necorespunzătoare/insuficientă a personalului	1,3	Mic	Nu
		10. Pregătirea profesională continuă	28. Inexistența planurilor de pregătire profesională continuă	1,8	Mediu	
			29. Neaprobarea planurilor de pregătire profesională continuă	2,0	Mediu	
			30. Nerealizarea activităților previzionate prin planurile de pregătire profesională continuă	2,3	Mare	
		11. Sistemul de evaluare a personalului	31. Inexistența unui sistem de evaluare anuală a salariaților	1,5	Mic	Nu
			32. Nerealizarea evaluării pe parcursul anului a salariaților departamentului	1,2	Mic	Nu
			33. Evaluarea formală a personalului	1,3	Mic	Nu
		12. Sistemul de gestionare a riscurilor – conducerea Registrului riscurilor	34. Inexistența unei politici unitare privind gestionarea riscurilor	2,0	Mediu	
			35. Inexistența unui responsabil privind gestionarea riscurilor	2,3	Mare	

Nr. crt.	DOMENIUL	OBIECTE AUDITABILE	RISCURI SEMNIFICATIVE	PUNCTAJ TOTAL	CLASARE	OBS.
			36. Nedesemnarea unei persoane responsabilă cu elaborarea şi monitorizarea Registrului riscurilor	2,0	Mediu	
			37. Neactualizarea sistematică a Registrului riscurilor	2,3	Mare	
III.	**Implementarea sistemului IT**	13. Gradul de realizare a subsistemelor informatice stabilite prin plan	38. Lipsă de coordonare a aplicațiilor ce rulează în sistemul informatic	2,0	Mediu	
			39. Nealocarea corespunzătoare a resurselor necesare realizării subsistemelor informatice	2,6	Mare	
			40. Evoluții tehnologice cu implicații asupra îndeplinirii planului	1,8	Mediu	
			41. Modificarea cadrului legal şi procedural ce reglementează activitățile pentru care se realizează subsistemele informatice	2,0	Mediu	
		14. Existența controalelor generale la nivelul subsistemelor IT	42. Implicațiile evoluțiilor tehnologice în domeniul IT	2,0	Mediu	
			43. Modificarea cadrului legal şi procedural ce reglementează activitățile pentru care se realizează subsistemele informatice	1,9	Mediu	
		15. Funcționalitatea subsistemelor în rețea	44. Inexistența unei politici de transmitere a datelor în rețea	1,3	Mic	Nu
			45. Implicațiile evoluțiilor tehnologice în domeniul IT	1,5	Mic	Nu
		16. Situația licențelor pentru programele de calculator	46. Limitări bugetare în privința achiziționării licențelor	2,6	Mare	
			47. Disfuncționalități în procesul de achiziționare al licențelor	2,3	Mare	
		17. Asigurarea integrării subsistemelor componente	48. Modificarea cadrului legal şi procedural ce reglementează activitățile pentru care se realizează subsistemele informatice	1,3	Mic	Nu
			49. Evoluții tehnologice cu implicații asupra integrării subsistemelor	1,6	Mic	Nu
			50. Neconcordanțe în integrarea subsistemelor	1,7	Mic	Nu
		18. Elaborarea manualelor de utilizare şi a manualelor de operare	51. Inexistența/Insuficiența manualelor de utilizare şi a manualelor de operare	1,5	Mic	Nu
			52. Lipsa unor componente şi existența unor elemente neclarificate în conținutul manualelor	1,5	Mic	Nu
		19. Instruirea utilizatorilor	53. Inexistența unui program de instruire al utilizatorilor	2,5	Mare	

Nr. crt.	DOMENIUL	OBIECTE AUDITABILE	RISCURI SEMNIFICATIVE	PUNCTAJ TOTAL	CLASARE	OBS.
		subsistemelor IT	54. Neefectuarea instruirii sistematice a utilizatorilor subsistemelor IT	1,8	Mediu	
IV.	**Securitatea IT**	20. Politica de securitate IT	55. Inexistența politicii de securitate	2,3	Mare	
			56. Neaplicarea politicii de securitatea în mod consecvent	2,2	Mediu	
		21. Monitorizarea implementării politicii de securitate IT	57. Inexistența unui responsabil desemnat cu monitorizarea implementării politicii de securitate IT	2,5	Mare	
			58. Neântocmirea şi netransmiterea sistematică a rapoartelor de monitorizare	2,0	Mediu	
			59. Inexistența unui sistem de clasificare şi protejare adecvată a informațiilor confidențiale existente în format electronic	1,9	Mediu	
		22. Evaluarea controalelor fizice în domeniul IT	60. Lipsa procedurilor privind implementarea controalelor fizice în domeniul IT	2,0	Mediu	
			61. Nedesemnarea responsabilității pentru monitorizarea controalelor fizice	2,5	Mare	
			62. Lipsa unor proceduri pentru realizarea controalelor fizice	2,5	Mare	
			63. Neefectuarea controalelor fizice conform procedurilor	2,6	Mare	
		23. Siguranța accesului la rețea şi a comunicării datelor în rețea	64. Lipsa procedurilor privind siguranța accesului utilizatorilor în rețea	1,8	Mediu	
			65. Inexistența responsabilului desemnat cu monitorizarea implementării procedurilor privind siguranța accesului utilizatorilor în rețea	2,0	Mediu	
			66. Neefectuarea monitorizării sistematice	2,4	Mare	
			67. Neimplementarea măsurilor privind siguranța accesului utilizatorilor în rețea conform procedurilor	2,3	Mare	
		24. Programe antivirus	68. Lipsa procedurilor privind implementarea programelor antivirus	2,7	Mare	
			69. Inexistența responsabilului desemnat cu monitorizarea implementării procedurilor privind implementarea programelor antivirus	2,0	Mediu	
			70. Neefectuarea monitorizării sistematice	1,8	Mediu	
			71. Neluarea măsurilor necesare privind implementarea programelor antivirus conform procedurilor	2,5	Mare	

Nr. crt.	DOMENIUL	OBIECTE AUDITABILE	RISCURI SEMNIFICATIVE	PUNCTAJ TOTAL	CLASARE	OBS.
		25. Recuperarea datelor în caz de dezastru	72. Lipsa procedurilor privind recuperarea datelor în caz de dezastru	2,0	Mediu	
			73. Inexistența responsabilului desemnat cu monitorizarea implementării procedurilor privind recuperarea datelor în caz de dezastru	2,1	Mediu	
			74. Neefectuarea monitorizării sistematice	2,2	Mediu	
			75. Neluarea măsurilor necesare privind recuperarea datelor în caz de dezastru conform procedurilor	2,3	Mare	
		26. Sistemul de arhivare	76. Lipsa procedurilor privind arhivarea datelor	1,5	Mic	Nu
			77. Nedesemnarea responsabilității pentru arhivarea datelor	1,7	Mic	Nu
			78. Neefectuarea evaluării periodice a activității de arhivare	1,4	Mic	Nu

Nota:

Pentru continuarea analizei, auditorii interni au împărţit cele 78 de riscuri structurate pe cele 26 de obiecte auditabile, 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 - 2,2
- *Riscuri mari* 2,3 - 3,0

Pentru moment, riscurile mici vor fi ignorate, 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 - P05 : Analiza riscurilor

ENTITATEA PUBLICĂ
Compartimentul Audit Intern

TABELUL PUNCTE TARI ŞI PUNCTE SLABE

Misiunea de audit: Tehnologia informației
Perioada auditată: 01.01.2005 – 31.12.2005
Întocmit: Popescu Sorin / Radu George **Data:** 20.01.2006
Avizat: Dumitru Daniel **Data:** 20.01.2006

Nr. crt.	Domeniul	Obiecte auditabile	Riscuri semnificative	T/S	Consecințele funcționării/ nefuncționării controlului intern	Grad de încredere al auditorului în controlul intern	OBS.
I.	Plan strategic	1. Politicile entității publice în domeniul IT	Inexistența unei atitudini favorabile în privința informatizării activității entității publice	S		Scăzut	
		2. Modalitatea de elaborare a planului strategic şi a planurilor anuale	Fundamentarea insuficientă a planului	S		Mediu	
			Necorelarea planurilor anuale	S		Scăzut	
			Lipsa prioritizării activităților	S		Mediu	
		3. Subsistemele informatice pentru funcțiile principale	Neacoperirea domeniilor de activitate ale entității publice cu subsisteme informatice	S		Scăzut	
			Necorelarea termenelor previzionate de realizare a subsistemelor	S		Mediu	
			Nedefinirea responsabilităților	S		Scăzut	
			Insuficienta previzionare a resurselor	S		Scăzut	
		5. Stabilirea responsabililor cu elaborarea si actualizarea planului	Nedesemnarea responsabilului cu elaborarea planului	S		Mediu	

Nr. crt.	Domeniul	Obiecte auditabile	Riscuri semnificative	T/S	Consecinţele funcţionării/ nefuncţionării controlului intern	Grad de încredere al auditorului în controlul intern	OBS.
			Nestabilirea persoanei responsabile cu actualizarea planului	T	Există sistem de control intern eficient	Ridicat	NU
		6. Aprobarea planului	Planul nu este aprobat	S		Scăzut	
			Planul nu este aprobat de persoanele competente	S		Mediu	
			Coordonarea neadecvată a planurilor	S		Scăzut	
II.	**Gestionarea şi organizarea depart. IT**	7. Organizarea departamentului IT	Departamentului IT nu este subordonat unui nivel managerial corespunzător	S		Mediu	
			Inexistenţa şi/sau neaprobarea organigramei	T	Există sistem de control intern eficient	Ridicat	NU
			Neformalizarea procedurilor specifice activităţilor desfăşurate	S		Scăzut	
			Existenţa unui număr mare de posturi de conducere deţinute cu delegaţie	S		Scăzut	
			Număr mare de posturi de execuţie neocupate	S		Mediu	
			Personal de execuţie neadecvat	S		Scăzut	
			Dotare cu hard şi soft inadecvat pentru desfăşurarea activităţilor specifice	T	Există sistem de control intern eficient	Ridicat	NU
			Inexistenţa unui sistem de control managerial la nivelul departamentului	S		Mediu	
			Neefectuarea monitorizării modului de realizare a obiectivelor generale şi specifice ale departamentului	S		Scăzut	
		10. Pregătirea profesională continuă	Inexistenţa planurilor de pregătire profesională continuă	S		Mediu	
			Neaprobarea planurilor de pregătire profesională continuă	S		Scăzut	
			Nerealizarea activităţilor previzionate prin planurile de pregătire profesională continuă	S		Mediu	

Nr. crt.	Domeniul	Obiecte auditabile	Riscuri semnificative	T/S	Consecințele funcționării/ nefuncționării controlului intern	Grad de încredere al auditorului în controlul intern	OBS.
		12. Sistemul de gestionare a riscurilor – conducerea Registrului riscurilor	Inexistența unei politici unitare privind gestionarea riscurilor	S		Scăzut	
			Inexistența unui responsabil privind gestionarea riscurilor	S		Scăzut	
			Nedesemnarea unei persoane responsabilă cu elaborarea şi monitorizarea Registrului riscurilor	S		Scăzut	
			Neactualizarea sistematică a Registrului riscurilor	S		Mediu	
III.	**Implementarea sistemului IT**	13. Gradul de realizare a subsistemelor informatice stabilite prin plan	Lipsă de coordonare a aplicațiilor ce rulează în sistemul informatic	S		Scăzut	
			Nealocarea corespunzătoare a resurselor necesare realizării subsistemelor informatice	S		Scăzut	
			Evoluții tehnologice cu implicații asupra îndeplinirii planului	S		Mediu	
			Modificarea cadrului legal şi procedural ce reglementează activitățile pentru care se realizează subsistemele informatice	S		Scăzut	
		14. Existența controalelor generale la nivelul subsistemelor IT	Implicațiile evoluțiilor tehnologice în domeniul IT	S		Scăzut	
			Modificarea cadrului legal şi procedural ce reglementează activitățile pentru care se realizează subsistemele informatice	S		Scăzut	
		16. Situația licențelor pentru programele de calculator	Limitări bugetare în privința achiziționării licențelor	S		Scăzut	
			Disfuncționalități în procesul de achiziționare al licențelor	S		Mediu	
		19. Instruirea utilizatorilor subsistemelor IT	Inexistența unui program de instruire al utilizatorilor	T	Există sistem de control intern eficient	Ridicat	NU
			Neefectuarea instruirii sistematice a utilizatorilor subsistemelor IT	S		Mediu	
IV.	**Securitatea IT**	20. Politica de	Inexistența politicii de securitate	S		Scăzut	

Nr. crt.	Domeniul	Obiecte auditabile	Riscuri semnificative	T/S	Consecințele funcționării/ nefuncționării controlului intern	Grad de încredere al auditorului în controlul intern	OBS.
		securitate IT	Neaplicarea politicii de securitatea în mod consecvent	S		Scăzut	
		21. Monitorizarea implementării politicii de securitate IT	Inexistența unui responsabil desemnat cu monitorizarea implementării politicii de securitate IT	S		Mediu	
			Neântocmirea şi netransmiterea sistematică a rapoartelor de monitorizare	S		Scăzut	
			Inexistența unui sistem de clasificare şi protejare adecvată a informațiilor confidențiale existente în format electronic	T	Există sistem de control intern eficient	Ridicat	NU
		22. Evaluarea controalelor fizice în domeniul IT	Lipsa procedurilor privind implementarea controalelor fizice în domeniul IT	S		Scăzut	
			Nedesemnarea responsabilității pentru monitorizarea controalelor fizice	T	Există sistem de control intern eficient	Ridicat	NU
			Lipsa unor proceduri pentru realizarea controalelor fizice	S		Mediu	
			Neefectuarea controalelor fizice conform procedurilor	S		Scăzut	
		23. Siguranța accesului la rețea şi a comunicării datelor în rețea	Lipsa procedurilor privind siguranța accesului utilizatorilor în rețea	S		Scăzut	
			Inexistența responsabilului desemnat cu monitorizarea implementării procedurilor privind siguranța accesului utilizatorilor în rețea	S		Scăzut	
			Neefectuarea monitorizării sistematice	T	Există sistem de control intern eficient	Ridicat	NU
			Neimplementarea măsurilor privind siguranța accesului utilizatorilor în rețea conform procedurilor	S		Mediu	
		24. Programe antivirus	Lipsa procedurilor privind implementarea programelor antivirus	S		Scăzut	

Nr. crt.	Domeniul	Obiecte auditabile	Riscuri semnificative	T/S	Consecințele funcționării/ nefuncționării controlului intern	Grad de încredere al auditorului în controlul intern	OBS.
			Inexistența responsabilului desemnat cu monitorizarea implementării procedurilor privind implementarea programelor antivirus	S		Scăzut	
			Neefectuarea monitorizării sistematice	S		Scăzut	
			Neluarea măsurilor necesare privind implementarea programelor antivirus conform procedurilor	S		Mediu	
		25. Recuperarea datelor în caz de dezastru	Lipsa procedurilor privind recuperarea datelor în caz de dezastru	S		Scăzut	
			Inexistența responsabilului desemnat cu monitorizarea implementării procedurilor privind recuperarea datelor în caz de dezastru	S		Scăzut	
			Neefectuarea monitorizării sistematice	S		Scăzut	
			Neluarea măsurilor necesare privind recuperarea datelor în caz de dezastru conform procedurilor	S		Scăzut	

Nota:

*În faza de ierarhizare se elaborează documentul **Tabelul puncte tari şi puncte slabe, prin transferarea o**perațiilor auditabile cu riscuri semnificative (mari şi medii) din documentul **Clasarea operațiilor în funcție de analiza riscului** care cuprinde un număr de 18 obiecte auditabile şi 60 de riscuri asociate acestora.*

*Ierarhizarea obiectelor auditabile constă în evaluarea funcționalității sistemelor de control intern, care limitează efectele riscurilor şi care dau posibilitatea auditorilor interni să aprecieze acele obiecte auditabile ca fiind "**puncte tari**", celelalte riscuri pentru care nu există activități de control sau acestea sunt nefuncționale vor fi în continuare considerate "**puncte slabe**". Astfel, în urma analizei au rezultat 7 riscuri asociate obiectelor auditabile care au fost evaluate ca fiind "**puncte tari**" şi vor fi eliminate, pentru moment, 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 operațiile considerate ca fiind **puncte slabe** , ocazie cu care vor fi renumerotate.*

Procedura - P05 : Analiza riscurilor

ENTITATEA PUBLICĂ
Compartimentul Audit Intern

TEMATICA IN DETALIU A OPERAȚIILOR AUDITABILE

Misiunea de audit: Tehnologia informației
Perioada auditată: 01.01.2005- 31.12.2005
Întocmit: Popescu Sorin/Radu George **Data:** 20.01.2006
Avizat: Dumitru Daniel **Data:** 20.01.2006

Nr. crt.	DOMENIUL	OBIECTE AUDITABILE	Nr. paragraf din Raportul de audit intern
I.	Plan strategic	1. Politicile entității publice în domeniul IT	
		2. Modalitatea de elaborare a planului strategic şi a planurilor anuale	
		3. Subsistemele informatice pentru funcțiile principale	
		4. Stabilirea responsabililor cu elaborarea si actualizarea planului	
		5. Aprobarea planului	
II.	Organizarea şi funcționarea departamentului IT	6. Organizarea departamentului IT	
		7. Pregătirea profesională continuă	
		8. Sistemul de gestionare a riscurilor – conducerea Registrului riscurilor	
III.	Implementarea sistemului IT	9. Gradul de realizare a subsistemelor informatice stabilite prin plan	
		10. Existența controalelor generale la nivelul subsistemelor IT	
		11. Situația licențelor pentru programele de calculator	
		12. Instruirea utilizatorilor subsistemelor IT	
IV.	Securitatea IT	13. Politica de securitate IT	
		14. Monitorizarea implementării politicii de securitate IT	
		15. Evaluarea controalelor fizice în domeniul IT	
		16. Siguranța accesului la rețea şi a comunicării datelor în rețea	
		17. Programe antivirus	
		18. Recuperarea datelor în caz de dezastru	

Nota:

Procedura *Analiza riscurilor* ***a început cu elaborarea documentului*** *Lista centralizatoare a obiectelor auditabile,* ***care a cuprins 26 de operații/obiecte auditabile, şi s-a finalizat cu*** *Tematica în detaliu a misiunii de audit,* ***în care au fost selectate numai 18 de obiecte auditabile.***

În continuare, cele 18 de operații/obiecte auditabile, 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 intervenției la fața locului****, care se vor materializa în F.I.A.P.-uri şi F.C.R.I.-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.*

Menționăm,totuşi, că procedura *Analiza riscurilor* ***trebuie să rămână un „****document viu****” care în funcție de constatările rezultate în*** *Etapa de intervenție la fața locului* ***să fie actualizată ori de câte ori se impune.***

Procedura – P06: Elaborarea programului de audit intern

ENTITATEA PUBLICĂ
Serviciul Audit Intern

PROGRAMUL DE AUDIT INTERN

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005- 31.12.2005
Întocmit: Popescu Sorin/Radu George **Data:** 27.03.2006
Avizat: Dumitru Daniel **Data:** 27.03.2006

ETAPELE MISIUNII	DOMENIUL	ACTIVITĂȚI	DURATA (H)	PERSOANELE IMPLICATE	LOCUL DESF.
Tema generală:	***Tehnologia Informatiei***		**376**		
1. PREGĂTIREA MISIUNII DE AUDIT			**152**		
		1. Intocmirea şi procesarea Ordinului de serviciu	2	Popescu Sorin	SAI
		2. Intocmirea si validarea Declarației de independență	2	Popescu Sorin	SAI
		3. Pregătirea şi transmiterea Notificării privind declanşarea misiunii de audit intern către părțile interesate	2	Radu George	SAI
		4. Colectarea şi prelucrarea informațiilor	30	Popescu Sorin	SAI AUDITAT
		5. Elaborarea Chestionarului de control intern	16	Popescu Sorin/ Radu George	SAI
		6. Întocmirea Listelor de verificare	40	Popescu Sorin/ Radu George	SAI
		7. Analiza riscurilor	32	Popescu Sorin	SAI
		8. Întocmirea Programului de audit intern	8	Popescu Sorin	SAI
		9.Intocmirea Programului preliminar al intervenției la fața locului	4	Radu George	SAI
		10. Organizarea Şedinței de deschidere cu Direcția IT.	4	Radu George	SAI

ETAPELE MISIUNII	DOMENIUL	ACTIVITĂȚI	DURATA (H)	PERSOANELE IMPLICATE	LOCUL DESF.
		11. Redactarea Minutei şedinţei de deschidere.	4	Radu George	SAI AUDITAT
		12. Organizarea Şedinţei de inchidere cu Direcţia IT.	4	Radu George	SAI AUDITAT
		13. Redactarea Minutei şedinţei de inchidere.	4	Radu George	AUDITAT
II.INTERVENȚIA LA FAȚA LOCULUI			**140**		
	OBIECTIVUL 1. **Plan strategic**		**38**		
		1.1. Efectuarea testărilor, detaliate *Programul intervenţiei la faţa locului*	16	Popescu Sorin	AUDITAT
		1.2. Discutarea constatărilor cu conducatorul departamentului IT	2	Popescu Sorin	SAI
		1.3. Elaborarea F.I.A.P. – urilor	8	Popescu Sorin	SAI
		1.4. Colectarea dovezilor	4	Radu George	AUDITAT
		1.5. Revizuirea documentelor de lucru din punct de vedere al conţinutului şi al formei şi întocmirea Notei centralizatoare a documentelor de lucru	8	Radu George	AUDITAT
	OBIECTIVUL 2. **Organizarea şi funcţionarea departamentului IT**		**32**		
		2.1. Efectuarea testărilor, detaliate *Programul intervenţiei la faţa locului*	16	Popescu Sorin	AUDITAT
		2.2. Discutarea constatărilor cu conducatorul departamentului IT	2	Popescu Sorin	SAI
		2.3. Elaborarea F.I.A.P. - urilor	4	Popescu Sorin	SAI
		2.4. Colectarea dovezilor	2	Radu George	AUDITAT
		2.5. Revizuirea documentelor de lucru din punct de vedere al conţinutului şi al formei şi întocmirea Notei centralizatoare a documentelor de lucru	8	Radu George	AUDITAT
	OBIECTIVUL 3. **Implementarea sistemului IT**		**28**		
		3.1. Efectuarea testărilor, detaliate *Programul intervenţiei la faţa locului*	16	Popescu Sorin	AUDITAT
		3.2. Discutarea constatărilor cu conducatorul departamentului IT	2	Popescu Sorin	SAI
		3.3. Elaborarea F.I.A.P. - urilor	4	Popescu Sorin	SAI
		3.4. Colectarea dovezilor	4	Radu George	AUDITAT

ETAPELE MISIUNII	DOMENIUL	ACTIVITĂȚI	DURATA (H)	PERSOANELE IMPLICATE	LOCUL DESF.
		3.5. Revizuirea documentelor de lucru din punct de vedere al conținutului şi al formei şi întocmirea Notei centralizatoare a documentelor de lucru	2	Radu George	AUDITAT
	OBIECTIVUL 4. **Securitatea IT**		**42**		
		4.1. Efectuarea testărilor, detaliate *Programul intervenției la fața locului*	8	Popescu Sorin	AUDITAT
		4.2. Discutarea constatărilor cu şeful de serviciu	2	Popescu Sorin	SAI
		4.3. Elaborarea F.I.A.P. - urilor	8	Popescu Sorin	SAI
		4.4. Colectarea dovezilor	16	Radu George	AUDITAT
		4.5. Revizuirea documentelor de lucru din punct de vedere al conținutului şi al formei şi întocmirea Notei centralizatoare a documentelor de lucru	8	Radu George	AUDITAT
III. RAPORTUL DE AUDIT INTERN			**80**		
		14. Redactarea si revizuirea proiectului de Raport de audit intern	40	Popescu Sorin	SAI
		15. Transmiterea proiectului de Raport de audit intern la auditat şi solicitarea răspunsului asupra conținutului în 15 zile	4	Radu George	SAI
		16. Organizarea Reuniunii de conciliere, dacă este cazul	8	Radu George	AUDITAT
		17. Includerea în Raportul de audit intern a aspectelor sesizate de structura auditata si reținute de auditori, finalizarea si intocmirea sintezei raportului	16	Popescu Sorin	SAI
		18. Obținerea avizarii Raportului de audit intern aprobat de conducerea instituției	8	Radu George	SAI
		19. Transmiterea recomandărilor aprobate către auditat	4	Radu George	AUDITAT
IV. URMĂRIREA RECOMANDĂRILOR			**4**		
		20. Intocmirea fisei de urmarire a recomandarilor	4	Popescu Sorin	SAI

Auditorii,
Popescu Sorin
Radu George

Supervizorul,
Dumitru Daniel

Procedura - P06: Elaborarea programului de audit intern

ENTITATEA PUBLICĂ
Serviciul Audit Intern

PROGRAMUL INTERVENȚIEI LA FAȚA LOCULUI

Misiunea de audit: Tehnologia Informatiei
Perioada auditată: 01.01.2005- 31.12.2005
Întocmit: Popescu Sorin/Radu George Data: 27.03.2006
Avizat: Dumitru Daniel Data: 27.03.2006

	Obiectivul I. Plan strategic						
Nr. crt.	OBIECTE AUDITABILE	TIPUL TESTĂRII	Locul	Durata (h)	Nr. test	Nr. lista verificare	Auditori
1.	Politicile entității publice în domeniul IT	- Analiza politicii entității publice în domeniul IT	DIT	8		LV 1	Popescu Sorin
2.	Modalitatea de elaborare a planului strategic şi a planurilor anuale	- Verificarea elaborării şi aprobarea planului strategic şi a planurilor anuale; - Analiza corelării planurilor strategice cu planurile anuale	DIT	4		LV 1	Radu George
3.	Subsistemele IT pentru funcțiile principale	- Examinarea faptului dacă subsistemele IT acoperă în totalitate nevoile pentru funcțiile principale - Analizarea acoperirii cu subsisteme IT a nevoilor funcțiilor principale nou-create - Analizarea corelării între termenele de realizare a subsistemelor IT	DIT	8	T 1.7	LV 1	Radu George
4.	Stabilirea responsabililor cu elaborarea si actualizarea planului	- Examinarea definirii clare a responsabilităților	DIT	6		LV 1	Radu George

5.	Aprobarea planului	- Examinarea conformitatii planului cu politicile entitatii publice in domeniul IT	DIT	8		LV 1	Radu George
Obiectivul II. Organizarea şi funcţionarea departamentului IT							
6.	Organizarea departamentului IT	-Analizarea organigramei depart. IT - Analizarea managementului resurselor umane la nivelul Departamentului IT	DIT	16	T 2.5	LV 2	Popescu Sorin
7.	Pregatirea profesionala continua	- Analizarea planurilor de pregatire profesionala continua - Verificarea existenței unui sistem de verificare a cunoștințelor dobândite după efectuarea cursurilor - Analizarea realizării pregătirii profesionale a salariaților conform atribuțiilor şi responsabilităților stabilite prin fişa postului	DIT	10		LV 2	Popescu Sorin
8.	Sistemul de gestionare a riscurilor – conducerea Registrului riscurilor	- Analizarea sistemului de evaluare a riscurilor - Verificarea existența şi actualizarea Registrului riscurilor	DIT	10		LV 2	Popescu Sorin
Obiectivul III. Implementarea sistemului IT							
9.	Gradul de realizare a subsistemelor informatice stabilite prin plan	- Verificarea realizării la termenele stabilite a subsistemelor IT; - Analizați activitatea de monitorizare a implementării subsistemelor IT	DIT	4		LV 3	Popescu Sorin
10.	Existența controalelor generale la nivelul subsistemelor IT	- Evaluarea controlului datelor introduse în aplicații; - Evaluarea controlului pe parcursul procesării datelor; - Evaluarea controlului datelor rezultate în urma procesării; - Analizați validarea datelor transferate din alte aplicații; - Evaluarea controalelor care verifică înregistrările duble;	DIT	8	T 3.6.	LV 3	Popescu Sorin

		- Verificarea autorizării electronice şi/sau manuale a tranzacţiilor; - Analizarea efectuarea tranzacţiilor numai de la computere definite în prealabil;					
11.	Situaţia licenţelor pentru programele de calculator	- Verificarea situaţia licenţelor deţinute atât pentru sistemul de operare Windows - Verificarea situaţia licenţelor deţinute atât pentru pachetul de programe Microsoft Office - Verificarea existenţa controalelor de sistem ce alertează administratorul în cazul utilizării de soft-uri pentru care nu s-au achiziţionat licenţe	DIT	8	T 3.8.	LV 3	Popescu Sorin
12.	Instruirea utilizatorilor subsistemelor IT	- Verificarea existenţei şi respectării programelor de instruirea a utilizatorilor subsistemelor IT	DIT	4		LV 3	Popescu Sorin
Obiectivul IV. Securitatea IT							
13.	Politica de securitate IT	- Verificarea existenţa politicii de securitate IT - Verificarea actualizarea politicii de securitate IT	DIT	6		LV 4	Radu George
14.	Monitorizarea implementării politicii de securitate IT	- Analizarea întocmirea şi transmiterea sistematică a rapoartelor de monitorizare	DIT	6		LV 4	Radu George
15.	Evaluarea controalelor fizice în domeniul IT	- Verificaţi dotarea camerelor în care se află servere-le cu echipamente adecvate.	DIT	8	T 4.7.	LV 4	Radu George
16.	Siguranţa accesului la reţea şi a comunicării datelor în reţea	- Verificarea alocării numelui de utilizator şi parolei aferente pentru accesul la reţea - Monitorizarea conectării la reţea conform listei de logg-are	DIT	8	T 4.8.	LV 4	Radu George

17.	Programe antivirus	- Verificarea implementării programelor anti-virus conform procedurilor - Monitorizarea sistematică a funcționalității programelor anti-virus - Verificarea sistemului de actualizare a programelor anti-virus	DIT	16	T 4.9.	LV 4	Radu George
18.	Recuperarea datelor în caz de dezastru	- Verificarea elaborării planului de recuperare a datelor în caz de dezastru - Verificarea desemnării responsabililor cu monitorizarea implementării procedurilor privind recuperarea datelor în caz de dezastru - Verificarea efectuării monitorizării sistematice	DIT	16		LV 4	Radu George

Auditorii,
Popescu Sorin
Radu George

Supervizorul,
Dumitru Daniel

ENTITATEA PUBLICA
Serviciul Audit Intern

MINUTA ŞEDINŢEI DE DESCHIDERE

Misiunea de audit: Tehnologia informatiei
Perioada auditată: 01.01.-31.12.2005
Întocmit: Popescu sorin/Radu George Data:
Avizat: Dumitru Daniel Data:

A. Lista participanţilor:

Numele	Funcţia	Direcţia/ Serviciul	Nr. telefon	E-mail	Semnătura
Dumitru Daniel	Coordonator	CAPI			
Popescu Sorin	Auditor	SAPI			
Radu George	Auditor	SAPI			
Patrulescu George	Conducator	DIT			
Voiculescu Alin	Sef	STDAM			
Boerescu Ilie	Sef	SCD			
Teodorescu Rodica	Sef	SEE			
Eleodor Darius	Sef	SAPP			
Iordache Camelia	Sef	SRC			
Paun Elena	Sef	SSD			
Badea Stefan	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 intern;
- Prezentarea funcţiei de audit intern de către auditori, în special a obiectivelor generale ale auditului intern, 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 auditaţilor 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 Directiei IT Juridic; resursele umane insuficiente şi neatractivitatea nivelului salariului pentru atragerea unor specialişti; fluctuatia mare a personalului implicat in activitatea IT.
- Stabilirea persoanelor pe care auditorii le pot contacta în vederea colectării informaţiilor, efectuării de teste asupra muncii lor şi pentru a lua interviuri. De asemenea, a fost stabilit programul întâlnirilor şi timpul necesar pentru realizarea acestor proceduri.

- Stabilirea condițiilor minime pe care auditatul trebuie să le asigure în vederea realizării misiunii de audit (spațiu de lucru, calculatoare, posibilitate de editare etc.)
- Convenirea unor aspecte procedurale, respectiv eventualitatea unor şedințe intermediare în cursul auditului, informarea sistematică asupra constatărilor.
- Stabilirea Reuniunii de închidere, inclusiv a participanților.
- Stabilirea modalității de redactare a Raportului de audit intern (când, cum şi cui va fi distribuit). Recomandările formulate, ca urmare a eventualelor disfuncționalități constatate, vor fi discutate şi analizate cu structura auditată, inclusiv calendarul implementării şi persoanele răspunzătoare cu implementarea recomandărilor.

LISTA DE VERIFICARE NR. 1

Obiectivul I. PLAN STRATEGIC

Nr. crt.	ACTIVITATEA DE AUDIT	DA	NU	OBS.
1.1.	*Examinarea procedurilor privind planul strategic*	-	-	
	1.1.1. Verificarea gradului de acoperire cu activități care concura la realizarea planului strategic:	-	-	
	- Activități identificate			
	- Proceduri aferente activităților			
	- Aprobarea procedurilor de către persoanele competente;	-	-	
	- Stabilirea modelelor de formulare specifice;	-	-	
	- Precizarea modalităților de complectare a modelelor;	-	-	
	- Oferirea unor exemple în acest sens;	-	-	
	- Actualizarea sistematică a procedurilor;	-	-	
	1.1.2. Înglobarea activităților de control intern în punctele cheie ale procesului;	-	-	
	1.1.3. Respectarea principiul dublei semnături;	-	-	
	1.1.4. Stabilirea responsabilităților persoanelor implicate în activitatea implementării sistemului IT;	-	-	
	1.1.5. Modalitatea arhivării documentelor.	-	-	
1.2.	*Compararea atribuțiilor privind planul strategic cuprinse în proceduri cu cele din fişele posturilor şi evaluarea completitudinii preluării acestora*	-	-	
1.3.	*Examinarea cunoaşterii procedurilor privind planul strategic de către responsabilii cu realizarea acestei activități*	-	-	
1.4.	*Aprecierea calității procedurilor de către personalul de execuție responsabil cu planul strategic*	-	-	
	a. consideră procedurile corespunzătoare?	-	-	
	b. constatată disfuncționalități în timpul aplicării practice?	-	-	
	c. există propuneri de perfecționare a procedurilor	-	-	
1.5.	*Politica entității publice în domeniul IT*			
	a. Analizați politica entității publice în domeniul IT şi stabiliți dacă asigură atingerea obiectivelor entității publice	**X**		**Interviu nr. 1.5.** **Notă de relații nr. 1.5.**
	b. Verificați dacă politica entității publice în domeniul IT se reflectă în planul strategic şi în planurile anuale			
	c. Examinați dacă managerii, cu responsabilități în monitorizarea implementării politicii IT, au fost consultați la elaborarea planului strategic			

Nr. crt.	ACTIVITATEA DE AUDIT	DA	NU	OBS.
	d. Analizați activitatea de actualizare a planului strategic			
1.6.	*Elaborarea planului strategic şi a planurilor anuale*			
	a. Analizați sistemul de fundamentare a planului strategic	**X**		**Interviu nr. 1.6.** **Notă de relații nr. 1.6.**
	b. Analizați corelarea planului strategic cu planurile anuale			
	c. Evaluați existența unui sistem de prioritizare al activităților cuprinse în plan			
	d. Verificați elaborarea şi aprobarea planului strategic şi a planurilor anuale			
1.7.	*Subsistemele IT pentru funcțiile principale*			
	a. Analizați sistemul de elaborare a subsistemelor IT pentru funcțiile principale.	**-**	**-**	**Interviu nr. 1.7.** **Test nr. 1.7.** **Foaie de lucru nr. 1.7.** **Listă de control nr. 1.7.** **FIAP nr. 1.7.**
	b. Existența programului pentru instruirea utilizatorilor subsistemului IT	**X**		
	c. Examinați dacă subsistemele IT acoperă în totalitate nevoile pentru funcțiile principale ale entității publice		**X**	
	d. Analizați dacă nevoile de subsisteme IT pentru funcțiile principale nou-create au fost acoperite.		**X**	
	e. Verificați dacă departamentele înființate ca urmare a funcțiilor principale nou-create au fost solicitate să-şi exprime cerințele specifice privind realizarea unor subsisteme IT proprii activității lor		**X**	
	f. Analizați existența corelării între termenele de realizare a subsistemelor.	**X**		
	g. Analizați procedurile pe baza cărora se realizează subsistemele IT şi stabiliți dacă acestea sunt suficiente pentru implementarea acestor subsisteme în condiții optime.	**X**		
	h. Stabiliți dacă există studii de fezabilitate pentru subsistemele IT planificate.	**-**	**-**	
1.8.	*Stabilirea responsabililor cu elaborarea şi actualizarea planului*	**X**		
	a. Verificați documentele oficiale prin care au fost desemnate persoanele responsabile cu elaborarea şi actualizarea planului.	**X**		**Interviu nr. 1.8.**
	b. Examinați dacă responsabilitățile sunt clar definite	**X**		
	c. Verificați dacă persoanele nominalizate au fost încunoştințate şi acțiunile întreprinse pentru îndeplinirea acestor sarcini de serviciu.	**X**		

Nr. crt.	ACTIVITATEA DE AUDIT	DA	NU	OBS.
	d. Analizați dacă fişa postului pentru persoanele responsabile au fost actualizate, cuprinzând noile sarcini primite.	**X**		
	e. Analizați procedurile utilizate pentru elaborarea şi actualizarea planului	**-**	**-**	
	f. Identificați deciziile luate în vederea elaborării şi actualizării planului şi analizați dacă aceste sunt în conformitate cu procedurile existente la nivelul entității publice	**-**	**-**	
	g. Examinați instrumentele utilizate pentru estimarea resurselor şi termenelor necesare pentru realizarea planului utilizate în faza de elaborare a planului	**-**	**-**	
	h. Verificați dacă prin elaborarea planului au fost stabilite praguri bugetare pentru activitățile ce trebuiesc realizate şi procedurile ce vor fi aplicate în cazul în care aceste praguri bugetare sunt depăşite	**-**	**-**	
1.9.	*Aprobarea planului*			
	a. Verificați dacă planul este aprobat de persoanele competente	**X**		**Interviu nr. 1.9.**
	b. Analizați dacă planul aprobat este în conformitate cu politicile entității publice în domeniul IT			
	c. Analizați împreună cu factorii responsabili de realizarea subsistemelor IT pentru funcțiile principale din cadrul entității publice dacă există departamente importante pentru care nu s-au realizat subsisteme IT			

Data: 01.04.2005

Auditor intern,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern

INTERVIU nr. 1.5.
privind politica entităţii publice în domeniul IT
adresat
domnului Pătrulescu George, conducător Departament IT

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005 - 31.12.2005

Nr. crt.	***Întrebări***	Da	Nu	Obs.
1.	Există o politică a entităţii publice în domeniul IT?	X		
2.	Este aceasta aprobată de managementul entităţii publice?	X		
3.	Politica defineşte principalele domenii de interes în domeniul IT?	X		
4.	Politia IT este susţinută prin planul strategic?	X		
5.	Este politica IT actualizată periodic?	X		
6.	Politica IT asigură îndeplinirea obiectivelor generale ale entităţii publice?	X		
7.	Politica IT stabileşte stadiul actual, modalităţile de realizare şi stadiul viitor de dezvoltare al sistemului IT?	X		
8.	Este politicii IT adusă la cunoştiinţa salariaţilor implicaţi în implemnatrea acesteia?	X		
9.	Salariaţii cu responsabilităţi în acest sens au luat măsurile necesare pentru implementarea politicii IT?	X		
10.	Utilizatorii sistemului IT cunosc şi aplică prevederile politicii IT aplicabile departamentului în care îşi desfăşoară activitatea?	X		
11.	Aveţi cunoştiinţă de existenţa unor cazuri de încălcare a politicii IT? Dacă da prezentaţi măsurile luate la nivelul entităţii publice.	X		

Data: 03.04.2005

Intervievat,	Auditor,	Supervizor,
Pătrulescu George	Radu George	Dumitru Daniel

NOTA:
Pe baza răspunsurilor la interviu şi a documentelor transmise s-a hotărât ca pentru acest obiectiv să nu se elaboreze FIAP.
Informaţiile primite prin documentele transmise în cadrul interviului vor fi utilizate la elaborarea Raportului de audit intern.

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

NOTĂ DE RELAȚII nr. 1. 5.
privind elaborarea politicii entității publice
adresat
domnului Pătrulescu George, conducător Departament IT

Întrebarea nr. 1: *A fost elaborată politica entității publice în domeniul IT?*
Răspuns nr. 1: În calitate de conducător la departamentului IT am participat la elaborarea politicii IT . Menționez că politica IT a fost formalizată şi aprobată de către managementul entității publice.

Întrebarea nr. 2: Politica IT defineşte principalele domenii de interes în domeniul IT şi este susținută prin planul strategic?
Răspuns nr. 2: Politica IT a fost formulată pe baza sistemului IT existent şi prevede cerințele ce trebuiesc îndeplinite de acesta pe termen mediu şi lung, fiind enunțate principiile generale pentru atingerea acestora. Politica IT şi planul strategic au fost corelate, prin plan prezentându-se modul de îndeplinire a dezideratelor formulate prin politica IT.

Întrebarea nr. 3: Politica IT a fost adusă la cunoştința salariaților?
Răspuns nr. 3: Annual salariații entității publice complectează şi semnează o declarație pe propria răspundere prin care îşi asumă cunoaşterea şi respectarea politicilor IT în activitatea desfăşurată. De asemenea, menționez că politica IT este publicată pe site-ul organizației, fiind o informație de interes public.

Întrebarea nr. 4: Aveți cunoştință de existența unor cazuri de încălcare a politicii IT? Dacă da, puteți să ne prezentați măsurile luate la nivelul entității publice?
Răspuns nr. 4: *Până în prezent nu au fost constatate cazuri de încălcare a prevederilor politicii IT.*

Întrebarea nr. 5: Politica IT este actualizată periodic*?*
Răspuns nr. 5: Până în prezent politica IT nu a fost actualizată. Aceasta a fost elaborată cu 2 ani în urmă, şi este încă de actualitate.

Întrebarea nr. 6: Cum se va realiza actualizarea politicii IT*?*
Răspuns nr. 6: Politica IT a fost elaborată la cererea managementului entității publice şi va fi actualizată, probabil, tot la cererea managementului.

Întrebarea nr. 7: Există o procedură de actualizare a politicii IT?
Răspuns nr. 7: Nu.

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

Intervievat,	Auditor,	Supervizor,
Pătrulescu George	Radu George	Dumitru Daniel

Nota:
Nu se va elabora FIAP, dar aspectele constatate vor fi menționate în raportul de audit intern

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

INTERVIU
privind planul strategic nr. 1.6.
adresat
domnului Pătrulescu George, conducător Departament IT

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005 - 31.12.2005

Nr. crt.	***Întrebări***	Da	Nu	Observații
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 al activităților cuprinse în plan?	X		Da, prin planul strategic aprobat se urmăreşte atingerea obiectivelor strategice stabilite prin politicile entității publice în domeniul IT.
4.	Este sistem de prioritizare al activităților cuprinse în plan actualizat periodic?	X		
5.	Planul strategic şi planurile anuale sunt elaborate conform procedurilor formalizate?	X		Entitatea publică a elaborat şi aprobat un set de proceduri menite să formalizeze activitatea de elaborare a planului strategic şi a planurilor anuale

Data: 03.04.2005

Intervievat,	Auditor,	Supervizor,
Pătrulescu George	Radu George	Dumitru Daniel

NOTA:
Pe baza răspunsurilor la interviu şi a documentelor transmise s-a hotărât ca pentru acest obiectiv să nu se elaboreze FIAP.
Informațiile primite prin documentele transmise în cadrul interviului vor fi utilizate la elaborarea Raportului de audit intern.

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

NOTĂ DE RELAȚII nr. 1.6.
privind elaborarea planului strategic şi a planurilor anuale
adresată,
domnului Pătrulescu George, conducător Departament IT

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 inițial 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 entității 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 funcțiilor principale ale entității publice, pornindu-se de la sistemul IT existent şi urmărindu-se realizarea măsurilor necesare în vederea atingerii parametrilor stabiliți prin politica IT.

Întrebarea nr. 4: Există un sistem de prioritizare al activităților cuprinse în plan?
Răspuns nr. 4: *Da. Implementarea subsistemelor IT se va realiza conform planificării pornind de la importanța acestora pentru entitatea publică şi ținându-se cont de resursele de care dispune organizația.*

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

Intervievat,	Auditor,	Supervizor,
Pătrulescu George	Radu George	Dumitru Daniel

Nota:
Nu se va elabora FIAP, dar aspectele constatate vor fi menționate în raportul de audit intern .

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

INTERVIU nr. 1.7.
privind subsistemele IT pentru funcţiile principale
adresat
domnului Pătrulescu George, conducător Departament IT

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005 - 31.12.2005

Nr. crt.	*Întrebări*	Da	Nu	Obs.
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		Da, 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 reanalizată periodic (trimestrial, anual) o analiză a nevoilor de susbsisteme 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 previzonate resursele necesare pentru elaborarea subsistemelor IT?	X		Departamentul IT asigură resursele umane necesare pentru elaborarea subsistemelor IT.

Data: 03.04.2005

Intervievat,	Auditor,	Supervizor,
Pătrulescu George	Radu George	Dumitru Daniel

NOTA:
Pe baza răspunsurilor la interviu şi a documentelor transmise s-a hotărât ca pentru acest obiectiv să se elaboreze FIAP.

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST NR. 1.7.

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005- 31.12.2005

Obiectul testului:
Subsistemele IT pentru funcțiile principale.

Obiectivele testului

- Subsistemele IT pentru funcții principale apărute la recomandarea Comisiei Europene şi sau ca urmare a schimbărilor legislative apărute în România.
- Nerespectarea termenelor de implementare al subsistemelor IT.

Descrierea testului

Populația statistică a fost constituită din cele trei de funcții principale nou-create la nivelul entității publice]n baza recomandărilor Comisiei Europene, identificate ca urmare a analizei modificărilor operate în organigramă la data elaborării planului strategic.

Eşantionul pentru realizarea testării situației subsistemelor IT pentru funcțiile principale a fost constituit din totalul populației statistice, respectiv 100%.

Testarea a constat în examinarea următoarelor elemente stabilite prin *Lista de verificare nr. 1, poz. 1.7*, şi anume:

- Examinați dacă subsistemele IT acoperă în totalitate nevoile pentru funcțiile principale ale entității publice
- Analizați dacă nevoile de subsisteme IT pentru funcțiile principale nou-create au fost acoperite
- Verificați dacă departamentele înființate ca urmare a funcțiilor principale nou-create au fost solicitate să-şi exprime cerințele specifice privind realizarea unor subsisteme IT proprii activității lor
- Analizați procedurile pe baza cărora se realizează subsistemele IT şi stabiliți dacă acestea sunt suficiente pentru implementarea acestor subsisteme în condiții optime

Testarea s-a concretizat în elaborarea *Listei de control nr. 1 privind analiza subsistemelor IT pentru funcțiile principale nou-create*.

Constatări

Din analiza Listei de control rezultate s-a constatat că în cadrul entității publice există structuri nou-înființate, ca urmare a schimbărilor legislative apărute pentru care nu

s-au realizat aplicații 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 înființată – *Autoritatea de Management a Fondurilor de Coeziune* – care a notificat departamentul IT, dar implementarea nu s-a realizat în termen.

Concluzii

În acest caz se va elabora FIAP.

Auditor,
Radu George

Supervizor,
Dumitru Daniel

FOAIE DE LUCRU nr. 1.7.

Obiectivul nr. 1: PLAN STRATEGIC

Obiectul nr. 1.7. : Subsistemele IT pentru funcțiile principale

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

- populația totală este de 8 funcții principale nou-create;
- eşantionul va fi de 37,5%, respectiv 8 x 37,5% = 3 funcții principale;
- eşantionul se va constitui din:
  - *Autoritatea de Management a Fondurilor Structurale*
  - *Autoritatea de Management a Fondurilor de Coeziune*
  - *Autoritatea competentă pentru acreditarea agențiilor de plată*

  conform celor prezentate în Lista de control anexată la Testul nr. 1.1.:
- eşantionul constituit va fi verificat integral;
- în urma verificării se va întocmi un test.

Data: 08.04.2005

Auditor,
Radu George

Supervizor,
Dumitru Daniel

Lista control nr. 1. 7.

privind Analiza subsistemelor IT pentru funcţiile principale nou-create

Nr. crt.	Elemente Testate / Eşantion	*Examinaţi dacă subsistemele IT acoperă în totalitate nevoile pentru funcţiile principale ale entităţii publice*	*Analizaţi dacă nevoile de subsisteme IT pentru funcţiile principale nou-create au fost acoperite*	*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*	*Analizaţi procedurile pe baza cărora se realizează subsistemele IT şi stabiliţi dacă acestea sunt suficiente pentru implementarea acestor subsisteme în condiţii optime*
1.	*Autoritatea de Management a Fondurilor Structurale*	FIAP	FIAP	FIAP	X
2.	*Autoritatea de Management a Fondurilor de Coeziune*	FIAP	FIAP	FIAP	X
3.	*Autoritatea competentă pentru acreditarea agenţiilor de plată*	FIAP	FIAP	X	X

Data: 01.04.2005

Auditor,
Radu George

Supervizor,
Dumitru Daniel

Procedura - P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI NR. 1.7.

Misiunea de audit: *Audit IT.*
Perioada auditată: 01.01.2005 – 01.01.2006

PROBLEMA

Existența unor departamente care nu dispun de subsisteme IT specifice activităților care se desfăşoară în cadrul entității publice.

CONSTATARE

- Din analiză s-a constatat că în cadrul entității publice există structuri nou-înființate ca urmare a recomandărilor Comisiei Europene şi a schimbărilor legislative, care nu au notificat departamentul IT în privința nevoilor lor de aplicații informatice specifice. În acelaşi timp, s-au constatat şi departamente nou înființate care au fost solicitate să-şi exprime nevoile pentru realizarea subsistemelor IT specifice activității lor, dar care nu s-au realizat conform planificării.

CAUZE

- Inexistența la nivelul entității publice a unor proceduri complete de elaborare a strategiei IT care să permită actualizarea sistematica, functie de schimbările legislative;
- Insuficiența personalului de specialitate.

CONSECINȚE

- Domenii importante de activitate ale entității publice pentru care nu s-a realizat implementarea subsistemelor IT necesare pentru desfăşurarea activității au randamente scăzute, ceea ce afectează ansamblul entității publice;
- Sarcinile pentru posturile vacante au fost redistribuite între salariații existenți în cadrul Direcției IT.

RECOMANDĂRI

- Elaborarea unei proceduri scrise şi formalizate pentru actualizarea strategia IT la nivelul entității publice pentru departamentele nou-create;
- Stabilirea responsabilității pentru actualizarea strategiei IT;
- Preocupare pentru angajarea personalului de specialitate şi ocuparea posturilor vacante;
- Coroborarea atribuțiilor prezentate prin proceduri cu cele stabilite prin fişele posturilor;
- Inventarierea stadiului implementării subsistemelor IT la nivelul departamentelor entității publice şi stabilirea necesităților IT care trebuiesc incluse în strategia IT.

Întocmit, Radu George	Supervizat, Dumitru Daniel	Pentru conformitate, Eleodor Darius

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

INTERVIU nr. 1.8.
Privind stabilirea responsabililor cu elaborarea şi actualizarea planului
adresat
domnului Pătrulescu George, conducător Departament IT

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005 - 31.12.2005

Nr. crt.	***Întrebări***	Da	Nu	Observaţii
1.	Există documente oficiale prin care au fost desemnate persoanele responsabile cu elaborarea şi actualizarea planului?	X		
2.	Sunt responsabilitățile clar definite în documentele oficiale?	X		
3.	Există nominalizate în mod oficial persoanele responsabile?	X		
4.	Persoanele responsabile au fost încunoştinţate?	X		
5.	Fişele posturilor au fost actualizate pentru a reflecta noile responsabilităţi primite?	X		
6.	Persoanele nominalizate şi-au îndeplinit sarcinile privind elaborarea şi actualizarea planului strategic şi a planurilor anuale?	X		

Data: 03.04.2005

Intervievat,	Auditor,	Supervizor,
Pătrulescu George	Radu George	Dumitru Daniel

NOTA:
Pe baza răspunsurilor la interviu şi a documentelor transmise s-a hotărât ca pentru acest obiectiv să nu se elaboreze FIAP.
Informaţiile primite prin documentele transmise în cadrul interviului vor fi utilizate la elaborarea Raportului de audit intern.

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

INTERVIU nr. 1.9.
Privind aprobarea planului strategic
adresat
domnului Pătrulescu George, conducător Departament IT

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005 - 31.12.2005

Nr. crt.	*Întrebări*	Da	Nu	Observaţii
1.	Planul strategic este aprobat de persoanele competente?	X		
2.	Planul aprobat este fundamentat în mod corespunzător?	X		Planul strategic a fost fundamentat conform procedurilor entităţii publice.
3.	Planul strategic este în conformitate cu politicile entităţii publice în domeniul IT?	X		Da, prin planul strategic aprobat se urmăreşte atingerea obiectivelor strategice stabilite prin politicile entităţii publice în domeniul IT.
4.	Procedurile pe baza cărora se realizează subsistemele IT sunt suficiente pentru implementarea acestor subsisteme în condiţii optime?		X	Entitatea publică a elaborat şi aprobat un set de proceduri menite să formalizeze implementarea acestor subsisteme în condiţii optime. Totuşi, cadrul procedural trebuie îmbunătăţit continuu pe măsură ce organizaţia soluţionează şi trebuie să reglementeze probleme noi, neplanificate, cu care se confruntă în asigurarea funcţionării în bune condiţii a subsistemelor IT.
5.	Există studii de fezabilitate pentru subsistemele IT planificate?	X		

Data: 03.04.2005

Intervievat,	Auditor,	Supervizor,
Pătrulescu George	Radu George	Dumitru Daniel

NOTA:
Pe baza răspunsurilor la interviu şi a documentelor transmise s-a hotărât ca pentru acest obiectiv să nu se elaboreze FIAP.
Informaţiile primite prin documentele transmise în cadrul interviului vor fi utilizate la elaborarea Raportului de audit intern.

LISTA DE VERIFICARE NR. 2

Obiectivul II. ORGANIZAREA ŞI FUNCȚIONAREA DEPARTAMENTULUI IT

Nr. crt.	ACTIVITATEA DE AUDIT	DA	NU	OBS.
2.1.	*Examinarea procedurilor privind organizarea şi funcționarea departamentului IT:*	-	-	
	Verificarea gradului de acoperire prin procedură a activităților privind organizarea şi funcționarea departamentului IT:	-	-	
	a. Elaborarea şi aprobarea procedurilor de către persoanele competente;	-	-	
	b. Aplicarea procedurilor în activitatea desfăşurată;	-	-	
	c. Evaluarea şi actualizarea sistematică a procedurilor;	-	-	
	d. Conformitatea procedurilor cu cadrul legal în vigoare;	-	-	
	e. Stabilirea responsabilităților persoanelor componente pe linia existenței unui cadru procedural adecvat la nivelul departamentului IT;	-	-	
2.2.	*Compararea atribuțiilor cuprinse în fişele posturilor cu cele din proceduri şi evaluarea completitudinii preluării acestora*	-	-	
2.3.	*Examinarea cunoaşterii procedurilor de către responsabilii cu realizarea activității*	-	-	
2.4.	*Aprecierea calității procedurilor de către responsabilii acestora:*			
	a. Consideră procedurile corespunzătoare?	-	-	
	b. Constatată disfuncționalități în timpul aplicării practice?	-	-	
	c. Există propuneri de perfecționare a procedurilor	-	-	
	d. Modul de soluționare a propunerilor de perfecționare a procedurilor	-	-	
2.5.	*Organizarea departamentului IT*	**X**		
	a. Verificarea existenței organigramei departamentului IT	**-**	**-**	

Nr. crt.	ACTIVITATEA DE AUDIT	DA	NU	OBS.
	b. Verificarea aprobării organigramei de către persoanele competente	-	-	
	c. Analizarea organigramei departamentului IT:	X		
	- Număr total de posturi de conducere;	X		
	- Număr posturi de conducere ocupate cu delegație;		X	
	- Număr total de posturi de execuție;	X		
	- Număr posturi de execuție neocupate		X	
	d. Evaluați demersurile realizate de departamentul IT pentru ocuparea posturilor de conducere		X	
	e. Analizați consecințele funcționării departamentului IT prin delegarea persoanelor de conducere		X	
	f. Evaluați preocuparea conducerii pentru ocuparea posturilor de execuție	X		**Test nr. 2.5.**
	g. Existența unui plan de implementare a măsurilor necesare menite să asigure buna desfăşurare a activității în cazul existenței unui număr mare de posturi vacante		X	**Listă control nr. 2.5.**
	h. Analizați dotarea departamentului cu echipamente hard şi soft adecvate pentru desfăşurarea activităților specifice, astfel:	-	-	**FIAP nr. 2.5.**
	- Număr suficient de calculatoare dotate corespunzător	-	-	
	- Număr suficient de servere	-	-	
	- Număr suficient de echipamente auxiliare (imprimante, xerox-uri, scanere, conexiuni la intranet/Internet)	-	-	
	- Programe IT adecvate	-	-	
	i. Verificați existența unui responsabil cu efectuarea monitorizării modului de realizare a obiectivelor generale şi specifice ale departamentului	-	-	
2.6.	*Stabilirea responsabilităților prin fişele posturilor*	-	-	
	a. Verificați actualizarea fişelor posturilor	-	-	
	b. Verificați cuprinderea atribuțiilor stabilite prin ROF în fişele posturilor	-	-	
2.7.	*Analizați calificarea şi pregătirea salariaților*	-	-	
2.8.	*Analizați pregătirea profesională continuă a salariaților*	X		
	a. Existența planurilor de pregătire profesională continuă		X	
	b. Verificați efectuarea sistematică a analizei îndeplinirii planului		X	
	c. Existența altor forme de pregătire profesională	-	-	

Nr. crt.	ACTIVITATEA DE AUDIT	DA	NU	OBS.
	d. Existența unui sistem de verificare a cunoştinţelor dobândite după efectuarea cursurilor		**X**	**Interviu nr. 2.8.** **FIAP nr. 2.8**.
	e. Analizați dacă pregătirea profesională a salariaților este realizată conform atribuțiilor şi responsabilităților stabilite prin fişa postului.	**X**		
	f. Verificați dacă pregătirea profesională a salariaților asigură atingerea obiectivelor organizației		**X**	
	g. Verificați existența unui sistem de indicatori de performanță pentru evaluarea gradului de pregătire profesională		**X**	
2.9.	*Examinați sistemul de evaluare a personalului*	-	-	
	a. Verificați existența unui sistem de evaluare anuală a salariaților	-	-	
	b. Analizați realizarea evaluării pe parcursul anului a salariaților	-	-	
	c. Verificați evaluarea formală a personalului	-	-	
2.10.	*Examinarea sistemului de gestionare a riscurilor generale*			
	a. Verificați existența unei politici unitare privind gestionarea riscurilor		X	**Interviu nr. 2.10.** **FIAP nr. 2.10.**
	b. Verificați existența unui sistem de evaluare a riscurilor			
	c. Identificați desemnarea unui responsabil privind gestionarea riscurilor la nivelul departamentului IT			
	d. Verificați existența Registrului riscurilor la nivelul Direcției IT			
	e. Analizați actualizarea sistematică a Registrului riscurilor			
	f. Verificați dacă riscurile majore prezentate în Registrul riscurilor elaborat la nivelul Direcției IT se regăsesc în Registrul riscurilor elaborat la nivelul întregii entități publice			

Data: 01.04.2005

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

TEST NR. 2.5.

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005- 31.12.2005

Obiectul testului

Organizarea şi funcționarea departamentului IT.

Obiectivele testului

- Corelația dintre numărul de posturi de conducere ocupate şi cele deținute cu delegație.

Descrierea testului

Departamentul IT din cadrul entității publice are 7 servicii funcționale. Eşantionul va fi constituit din întreaga populație, deci 100%, deoarece există un număr rezonabil de servicii.

Testarea a constat în examinarea la nivelul departamentului IT a următoarelor elemente stabilite prin *Lista de verificare nr. 2, poz. 2.5*, şi anume:

- Analiza organigramei departamentului IT:
  - Număr total de posturi de conducere
  - Număr posturi de conducere ocupate cu delegație
  - Număr total de posturi de execuție
  - Număr posturi de execuție neocupate.
- Evaluați 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.
- Analizați consecințele funcționării departamentului IT prin delegarea personalului de conducere
  - Număr de sesizări ale departamentelor beneficiare ale serviciilor IT;
  - Număr de subsisteme IT neimplementate la termenele planificate.

- Analizați preocuparea conducerii pentru ocuparea posturilor de execuție;
    - Număr de examene organizate pentru ocuparea posturilor
    - Număr de solicitări către compartimentul de Resurse Umane pentru organizarea examenelor.
- Existența unui plan de implementare a măsurilor necesare menite să asigure buna desfăşurare a activității în cazul existenței unui număr mare de posturi vacante.

Testarea s-a concretizat în elaborarea *Listei de control nr. 2.1. privind organizarea şi funcționarea departamentului IT*.

Constatări

Din analiza modului de acoperire a necesarului de resurse umane la nivelul departamentului IT s-a constatat că, datorită numărului mare de posturi vacante existent şi utilizarea sistemului de delegare a personalului special pentru exercitarea funcțiilor de conducere, salariații trebuie să-şi îndeplinească sarcinile de serviciu ce le revin ca urmare a delegării, dar şi sarcinile curente de serviciu, fapt ce afectează calitatea îndeplinirii acestor atribuții

De asemenea, s-a constatat că nu este organizat şi nu a fost ținut la zi Registrul riscurilor cuprinzând riscurile potențiale şi istoricul acestora, cu efectele şi consecințele lor, precum şi activitățile de control intern care au fost prevăzute pentru limitarea riscurilor.

Concluzii

În acest caz se va elabora FIAP.

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

Lista control nr. 2.5.

privind Organizarea şi funcţionarea departamentului IT

Nr. crt	Elemente testate / Eşantion	Analizarea organigramei departamentului IT				Evaluaţi demersurile realizate de departamentul IT pentru ocuparea posturilor		Analizaţi consecinţele funcţionării departamentului IT cu persoane de conducere cu delegaţie		Existenţa preoupării pentru ocuparea posturilor de execuţie		Existenţa unui plan de implementare a măsurilor necesare menite 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 de tehnored. şi dezvoltare aplicaţii multimedia*	3	1	12	4	FIAP		X	X	FIAP	X	FIAP
2.	*Serviciul comunicaţii date*	1	0	9	5	FIAP	FIAP	X	X	X	X	FIAP
3.	*Serviciul exploatarea echip.*	1	0	10	3	FIAP	FIAP	X	X	X	X	FIAP
4.	*Serviciul analiza, proiectare şi programare*	3	2	14	3	FIAP	FIAP	X	FIAP	FIAP	X	FIAP
5.	*Serviciul retele calculatoare*	1	0	9	2	FIAP	FIAP	X	X	X	X	FIAP

Nr. crt	Elemente testate / Eşantion	Analizarea organigramei departamentului IT				Evaluaţi demersurile realizate de departamentul IT pentru ocuparea posturilor		Analizaţi consecinţele funcţionării departamentului IT cu persoane de conducere cu delegaţie		Existenţa preoupării pentru ocuparea posturilor de execuţie		Existenţa unui plan de implementare a măsurilor necesare menite 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.	
6.	*Serviciul sinteză dezvoltare*	1	0	11	6	FIAP	FIAP	X	X	X	X	FIAP
7.	*Serviciul asistenţă tehnică*	1	0	10	4	FIAP	FIAP	FIAP	X	X	X	FIAP

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

Procedura - P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI NR. 2.5.

Misiunea de audit: *Audit IT*
Perioada auditată:

PROBLEMA

Existența unui număr mare de posturi de execuție vacante şi a unui număr mare de posturi de conducere deținute cu delegație.

CONSTATARE

Din analiza stadiului implementării subsistemelor IT specifice s-a constatat că datorită numărului mare de posturi vacante existente şi utilizării sistemului de delegare a personalului specializat pentru exercitarea funcțiilor de conducere, aceştia trebuie să-şi îndeplinească sarcinile de serviciu ce le revin ca urmare a delegării, dar şi sarcinile curente de serviciu, ceea ce afectează îndeplinirea atribuțiilor de serviciu şi calitatea acestora.

CAUZE

- Lipsa unei strategii la nivelul entității publice pentru ocuparea posturilor vacante şi mai ales a celor de conducere;
- Inexistența unor proceduri pentru suplinirea posturilor vacante şi pentru delegarea funcțiilor de conducere.

CONSECINȚE

- Activitatea din cadrul unor departamente nu se desfăşoară la parametrii stabiliți. Din analiza acestei situații în cadrul entității publice se constată frecvent întârzieri în implementarea diferitelor aplicații, nerealizarea testărilor finale la termenele planificate, netransmiterea rapoartelor periodice de monitorizare.

- Din practică se demonstrează că persoanele cu delegație nu au întotdeauna acelaşi nivel de implicare pentru soluționarea problemelor care apar comparativ cu titularii posturilor.

RECOMANDĂRI

- Elaborarea procedurilor scrise şi formalizate pentru suplinirea posturilor vacante şi delegarea funcțiilor de conducere precum şi stabilirea responsabililor pentru elaborarea şi actualizarea acestor proceduri;
- Realizarea unui program de pregătire profesională a persoanelor delegate pe funcții de conducere la nivelul entității publice.

Întocmit,	Supervizat,	Pentru conformitate,
Popescu Sorin	Dumitru Daniel	Pătrulescu George

ENTITATEA PUBLICĂ
Serviciul Audit Intern

INTERVIU nr. 2.8.
privind Pregătirea profesională continuă a salariaților
adresat
domnului Pătrulescu George, conducător Departament IT

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005 - 31.12.2005

Nr. crt.	Întrebări	Da	Nu	Obs.
1.	Ați semnat fişa postului pentru acest an?	X		
2.	Pregătirea profesională continuă este o activitate cuprinsă în fişa postului dumneavoastră?	X		
3.	Aveți aprobat un plan de pregătire profesională continuă?		X	
4.	Verificați efectuarea sistematică a analizei îndeplinirii planului?		X	
5.	Există alte forme de pregătire profesională a salariaților?	X		
6.	Există un sistem de verificare a cunoştințelor dobândite ca urmare a cursurilor efectuate?		X	
7.	Pregătirea profesională a salariaților este în concordanță cu atribuțiile şi responsabilitățile stabilite prin fişa postului?		X	
8.	Pregătirea profesională a salariaților asigură atingerea obiectivelor organizației?	X		
9.	Aveți manuale de utilizare?		X	
10.	Există indicatori de performanță pe baza cărora să se poată evalua gradul de pregătire profesională al salariaților coroborat cu nivelul de realizare a obiectivelor strategice ale entității?		X	

Data: 03.04.2005

Intervievat,	Auditor,	Supervizor,
Pătrulescu George	Popescu Sorin	Dumitru Daniel

NOTA:
Pe baza răspunsurilor la interviu şi a documentelor transmise s-a hotărât ca pentru acest obiectiv să se elaboreze FIAP.
De asemenea, informațiile primite în cadrul interviului vor fi utilizate şi la elaborarea Raportului de audit intern.

Procedura - P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI NR. 2.8.

Misiunea de audit: *Audit IT*
Perioada auditată:

PROBLEMA
Inexistența unui sistem de pregătire profesională continuă a salariaților departamentului IT.

CONSTATARE

Din analiză s-a constatat că aproximativ 20% dintre angajații care au acces la sistemul IT implementat au fost angajați în cadrul entității publice în ultimele 3 luni şi nu au primit o pregătire profesională adecvată privind modul de utilizare a acestuia. Din totalul personalului angajat s-a constatat că doar utilizatorii inițiali au primit instruire în acest sens.

De asemenea, instrucțiunile de utilizare pentru sistemul IT nu sunt prezentate într-un format adecvat, respectiv nu există manuale de utilizare, în documentația pusă la dispoziția departamentului. Astfel, majoritatea angajaților nu au instrucțiuni clare cu privire la modul de operare a sistemului, ceea ce duce la comiterea de erori.

CAUZE

- Inexistența planului de pregătire profesională continuă;
- Nedesemnarea unui responsabil cu planul de pregătire profesională continuă;
- Neasigurarea instruirii adecvate a utilizatorilor;
- Inexistența procedurilor scrise şi formalizate cu pregătirea profesională continuă.

CONSECINȚE

- Deşi până în prezent nu au apărut erori cu grave implicații financiare, totuşi există pericolul apariției unor probleme/disfuncționalități datorate pregătirii profesionale a salariaților.

RECOMANDĂRI

- Elaborarea unui sistem de pregătire profesională continuă a salariaților;
- Elaborarea procedurilor scrise şi formalizate pentru pregătirea profesională continuă;
- Stabilirea unor responsabilități cu elaborarea procedurilor şi actualizarea acestora;
- Coroborarea atribuțiilor şi responsabilităților stabilite prin proceduri cu fişele posturilor;
- Analiza planului de pregătire profesională continuă şi al gradului de realizare al acestuia în vederea elaborării planului pentru anul viitor;
- Stabilirea responsabilităților cu monitorizarea acestora, o atenție deosebită fiind pentru utilizatorii noi care trebuie să primească instruire specială pentru toate subsistemele IT pe care le vor utiliza, conform unui program bine stabilit.

Întocmit,	Supervizat,	Pentru conformitate,
Popescu Sorin	Dumitru Daniel	Pătrulescu George

ENTITATEA PUBLICĂ
Serviciul Audit Intern

INTERVIU nr. 2.10.
privind sistemul de gestionare a riscurilor
adresat
domnului Pătrulescu George, conducător Direcţia IT

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005 - 31.12.2005

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: 03.04.2005

Intervievat,	Auditor,	Supervizor,
Pătrulescu George	Popescu Sorin	Dumitru Daniel

NOTA:
Pe baza răspunsurilor la interviu şi a documentelor transmise s-a hotărât ca pentru acest obiectiv să se elaboreze FIAP.
Informaţiile primite în cadrul interviului vor fi utilizate şi la elaborarea Raportului de audit intern.

Procedura - P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI NR. 2.10.

Misiunea de audit: *Audit IT*
Perioada auditată:

PROBLEMA

Inexistența unui sistem de identificare, evaluare şi management al riscurilor la nivelul entității publice.

CONSTATARE

Din analiză s-a constatat că nu există preocupări pentru gestionarea riscurilor din cadrul entității şi nu a fost ținut Registrul riscurilor cuprinzând riscurile potențiale şi istoricul acestora, cu efectele şi consecințele lor, precum şi activitățile de control intern asociate pentru limitarea riscurilor.

CAUZE

- Inexistența procedurilor scrise şi formalizate pentru realizarea Registrului riscurilor;
- Neacordarea atenției cuvenite managementului riscurilor de către personalul entității publice.

CONSECINȚE

- Producerea unor evenimente nedorite pentru care entitatea publică nu este pregătită să acționeze;
- Există pericolul de a nu identifica riscuri majore şi de a nu fi asociate controale interne adecvate pentru reducerea efectului riscurilor la un nivel acceptabil pentru entitatea publică.

RECOMANDĂRI

- Stabilirea unei strategii de gestionare a riscurilor la nivelul entității publice;
- Stabilirea responsabililor pentru elaborarea şi actualizarea sistematică a procedurilor privind întocmirea Registrului riscurilor;
- Coroborarea atribuțiilor şi responsabilităților din proceduri cu cele din fişa postului referitor la gestionarea riscurilor;
- Organizarea şi ținerea la zi a Registrului riscurilor cuprinzând măsurile de control intern care sunt luate pentru limitarea acestora;

- Monitorizarea sistematică, la cererea managerului responsabil cu probleme administrative, a modului de respectare în activitatea zilnică a procedurilor scrise şi formalizate menite să asigure gestionare a riscului;
- Instruirea personalului pentru complectarea Registrului Riscurilor de către responsabilul cu ținerea acestuia;
- Informarea echipei de auditori în privința stadiului elaborării, însuşirii şi monitorizării riscurilor.

Întocmit, Popescu Sorin	Supervizat, Dumitru Daniel	Pentru conformitate, Pătrulescu George

LISTA DE VERIFICARE NR. 3

Obiectivul III. IMPLEMENTAREA SISTEMULUI IT

Nr. crt.	ACTIVITATEA DE AUDIT	DA	NU	OBS.
3.1.	*Examinarea procedurilor privind implementarea sistemului IT*	-	-	
	3.1.1. Verificarea gradului de acoperire a activităților privind implementarea sistemului IT:	-	-	
	- Aprobarea procedurilor de către persoanele competente;	-	-	
	- Stabilirea modelelor de formulare specifice;	-	-	
	- Precizarea modalităților de complectare a modelelor;	-	-	
	- Oferirea unor exemple în acest sens;	-	-	
	- Actualizarea sistematică a procedurilor;	-	-	
	- Conformitatea procedurilor cu politica IT;	-	-	
	3.1.2. Înglobarea activităților de control intern în punctele cheie ale procesului;	-	-	
	3.1.3. Respectarea principiul dublei semnături;	-	-	
	3.1.4. Stabilirea responsabilităților persoanelor implicate în activitatea implementării sistemului IT;	-	-	
	3.1.5. Asigurarea transpunerii prelucrărilor într-un sistem informatizat, respectiv realizarea codificării modelelor de formulare şi informațiile activităților, algoritmi de prelucrare ş.a.	-	-	
	3.1.6.Modalitatea arhivării documentelor.	-	-	
3.2.	*Compararea atribuțiilor privind implementarea sistemului IT cuprinse în proceduri cu cele din fişele posturilor şi evaluarea completitudinii preluării acestora*	-	-	
3.3.	*Examinarea cunoaşterii procedurilor privind implementarea sistemului IT de către responsabilii cu realizarea acestei activități*	-	-	
3.4.	*Aprecierea calității procedurilor de către personalul de execuție responsabil cu implementarea sistemului IT:*	-	-	
	a. consideră procedurile corespunzătoare?	-	-	

Nr. crt.	ACTIVITATEA DE AUDIT	DA	NU	OBS.
	b. constatată disfuncționalități în timpul aplicării practice?	-	-	
	c. există propuneri de perfecționare a procedurilor	-	-	
	d. modul de soluționare a propunerilor de perfecționare a procedurilor	-	-	
3.5.	*Gradul de realizare al subsistemelor IT stabilite prin plan*	**X**		
	a. Examinați existența unui sistem procedurat de realizare a subsistemelor IT	**X**		**Interviu nr. 3.5.** **FIAP nr. 3.5.**
	b. Verificați dacă realizarea subsistemelor IT a fost planificată		**X**	
	c. Verificați dacă au fost stabilite persoanele responsabile		**X**	
	d. Verificați dacă subsistemele IT au fost realizate la termenele stabilite		**X**	
	e. Examinați modul de alocare a resurselor necesare realizării subsistemelor IT	**X**		
	f. Analizați activitatea de monitorizare a implementării subsistemelor IT		**X**	
3.6.	*Verificați existența controalelor generale de sistem la nivelul subsistemelor IT:*	**X**		
	a. Controlul datelor introduse în aplicații;		**X**	**Test nr. 3.6.** **Foaie de lucru nr. 3.6.** **Listă de control nr. 3.6.** **FIAP nr. 3.6.**
	b. Controlul pe parcursul procesării datelor şi rapoartele produse în caz de nerealizarea procesării (întreruperi, transfer).		**X**	
	c. Controlul datelor rezultate în urma procesării, astfel încât să se asigure că aceste date sunt complecte		**X**	
	d. Validarea datelor transferate din alte aplicații		**X**	
	e. Controalelor care verifică înregistrările duble;		**X**	
	f. Autorizarea electronică şi/sau manuală a tranzacțiilor		**X**	
	g. Efectuarea tranzacțiilor numai de la computere definite în prealabil		**X**	
	h. Păstrarea integrală a înregistrărilor astfel încât să se poată urmări tranzacțiile efectuate din faza de inițiere până la finalizarea lor;	**X**		
	i. Modul de raportare a schimbărilor operate la nivelul datelor salvate;	**-**	**-**	

Nr. crt.	ACTIVITATEA DE AUDIT	DA	NU	OBS.
	j. Înțelegerea controalelor implementate de către utilizatori.	**X**		
3.7.	*Funcționalitatea subsistemelor IT în rețea*	**-**	**-**	
	- Verificați existența protocoalelor de transmitere a datelor în rețea	**-**	**-**	
	- Verificați dacă subsistemele IT realizate respectă cerințele stabilite prin politica, procedurile şi studiile de fezabilitate întocmite	**-**	**-**	
3.8.	*Situația licențelor pentru programele de calculator*	**X**		**Test nr. 3.8.** **Foaie de lucru nr. 3.8.** **Listă de control nr. 3.8.** **FIAP nr. 3.8.**
	a. Verificați situația licențelor deținute atât pentru sistemul de operare Windows		**X**	
	b. Verificați situația licențelor deținute atât pentru pachetul de programe Microsoft Office		**X**	
	c. Verificați dacă entitatea publică a achiziționat licențe pentru programele utilizate	**-**	**-**	
	d. Identificați eventualele limitări bugetare în privința achiziționării licențelor	**-**	**-**	
	e. Analizați eventualele disfuncționalități apărute în procesul de achiziționare a licențelor	**-**	**-**	
	f. Verificați existența soft-urilor nelicențiate instalate de utilizatori			
	g. Verificați desemnarea responsabilităților privind achiziționarea licențelor pentru programele de calculator	**-**	**-**	
	h. Verificați existența controalelor de sistem ce alertează administratorul în cazul utilizării de soft-uri pentru care nu s-au achiziționat licențe		**X**	
3.9.	*Asigurarea integrării subsistemelor componente*			
	a. Stabilirea prin proceduri a necesității integrării subsistemelor IT	**-**	**-**	
	b. Verificați desemnarea responsabilităților privind realizarea şi monitorizarea integrării subsistemelor IT	**-**	**-**	
	c. Modificările cadrului legal au influențat integrarea subsistemelor IT	**-**	**-**	
	d. Evoluțiile tehnologice au influențat integrarea subsistemelor IT	**-**	**-**	

Nr. crt.	ACTIVITATEA DE AUDIT	DA	NU	OBS.
	e. Analizați eventualele disfuncționalități apărute privind integrarea subsistemelor IT	-	-	
	f. Analizați modul de soluționare a neconcordanțelor apărute în integrarea subsistemelor	-	-	
3.10	*Elaborarea manualelor de utilizare şi a manualelor de operare*			
	- Verificați suficiența numărului de manuale de utilizare şi de operare	-	-	
	- Analizați comprehensivitatea manualelor de utilizare şi de operare şi dacă acestea corespund nevoilor utilizatorilor	-	-	
	- Examinați existența unui sistem de actualizare sistematică a manualelor	-	-	
	- Analizați dacă manualele de utilizare şi de operare sunt actualizate	-	-	
3.11	*Instruirea utilizatorilor sistemelor IT*	X		
	a. Elaborarea sistematică a programelor de pregătire profesională	-	-	**Notă de relații nr. 3.11.**
	b. Verificați existența şi aprobarea programelor de instruire a utilizatorilor subsistemelor IT		X	
	c. Examinați concordanța programelor de pregătire cu politica şi procedurile IT ale entității publice	-	-	
	d. Desemnarea responsabilităților cu implementarea programelor de pregătire profesională	-	-	
	e. Analizați instruirea utilizărilor subsistemelor IT conform programelor elaborate.		X	

Data: 01.04.2005

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern

INTERVIU nr. 3.5.
privind Gradul de realizare al subsistemelor IT stabilite prin planul strategic
adresat
domnului Eleodor Darius, şef Serviciul analiza, proiectare şi programare

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005 - 31.12.2005

Nr. crt.	***Întrebări***	Da	Nu	Observații
1.	Există un sistem procedurat de realizare a subsistemelor IT	X		
2.	Sistemele implementate au fost stabilite prin planul strategic şi planurile anuale?		X	FIAP nr. 3.5.
3.	Există persoane responsabile de implementarea subsistemelor IT?		X	FIAP nr. 3.5.
4.	Subsistemele IT au fost realizate la termenele stabilite?		X	FIAP nr. 3.5.
5.	Există resurse alocate pentru realizarea subsistemelor IT?	X		
6.	Aveți o procedură pentru monitorizarea implementării subsistemelor IT?		X	FIAP nr. 3.5.
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	FIAP nr. 3.5.
8.	Nu mai aveți ceva de adăugat?	X		

Data: 03.04.2005

Intervievat,	Auditor,	Supervizor,
Eleodor Darius	Popescu Sorin	Dumitru Daniel

NOTA:
Pe baza răspunsurilor la interviu şi a documentelor transmise s-a hotărât ca pentru acest obiectiv să se elaboreze FIAP.
Informațiile primite prin documentele transmise în cadrul interviului vor fi utilizate la elaborarea Raportului de audit intern.

Procedura - P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI NR. 3.5.

Misiunea de audit: *Audit IT*
Perioada auditată:

PROBLEMA

Subsistemele IT nu au fost realizate la termenele stabilite.

CONSTATARE

Echipa de auditori, analizând implementarea subsistemelor IT, potrivit planului anual întocmit şi aprobat, a constatat că termenele stabilite nu sunt respectate, iar departamentele ce ar trebui să utilizeze deja noile aplicații IT întâmpină deficiențe în transmiterea datelor în format electronic celorlalte departamente care beneficiază deja de programe performante.

CAUZE

- Inexistența unei proceduri de monitorizare a implementării subsistemelor IT care fac dificilă monitorizarea activităților de către managementul general;
- Persoane implicate inițial în aceste activități au primit alte responsabilități şi nu au fost desemnate alți salariați pentru înlocuirea acestora.

CONSECINȚE

- Nerealizarea subsistemelor IT conform termenelor stabilite, ceea ce îngreuiază realizarea sarcinilor de serviciu în domenii cheie de activitate ale entității publice;
- Posibilitatea afectării gradului de realizare a obiectivelor entității publice.

RECOMANDĂRI

- Elaborarea procedurilor scrise şi formalizate pentru monitorizarea implementării subsistemelor IT
- Desemnarea responsabilității cu realizarea şi actualizarea procedurilor;
- Efectuarea unor inspecții pentru stabilirea stadiului în care se află implementarea subsistemelor IT specifice pe departamente;

Întocmit,	Supervizat,	Pentru conformitate,
Popescu Sorin	Dumitru Daniel	Eleodor Darius

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST NR. 3. 6.

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005- 31.12.2005

Obiectul testului

Existența controalelor generale la nivelul subsistemelor IT

Obiectivele testului

- Verificarea existenței unor controale generale implementate la nivelul subsistemelor IT

Descrierea testului

Populația statistică este reprezentată 15 subsisteme IT ce reprezintă numărul total al subsistemelor IT funcționale la nivelul entității publice. Eşantionarea va fi reprezentat de 5 elemente din întreaga populație, 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. 3.6*, şi anume:

- Controlul datelor introduse în aplicații;
- 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 complecte
- Validarea datelor transferate din alte aplicații
- Controalelor care verifică înregistrările duble;
- Autorizarea electronică şi/sau manuală a tranzacțiilor
- Efectuarea tranzacțiilor numai de la computere definite în prealabil
- Păstrarea integrală a înregistrărilor astfel încât să se poată urmări tranzacțiile efectuate din faza de inițiere până la finalizarea lor;
- Înțelegerea controalelor implementate de către utilizatori.

Testarea s-a concretizat în elaborarea *Listei de control nr. 3.6. privind existența controalelor generale la nivelul subsistemelor IT.*

Constatări

Din analiza *Listei de control nr. 3.6.*, s-a constat inexistența următoarelor controale generale:

- Controlul datelor introduse în aplicații;
- Controlul datelor rezultate în urma procesării astfel încât să se asigure că aceste date sunt complete;
- Controlul pe parcursul procesării datelor şi rapoartele produse în caz de nerealizarea procesării (întreruperi, transfer);
- Validarea datelor transferate din alte aplicații;
- Efectuarea tranzacțiilor numai de la computere definite în prealabil.

Concluzii

În acest caz se va elabora FIAP nr. 3.6.

Data: 01.04.2005

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

FOAIE DE LUCRU nr. 3.6.

Obiectul nr. 3: *Implementarea sistemului IT*

Obiectivul: *Verificarea existenței unor controale generale implementate la nivelul subsistemelor IT*

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

- populația 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 operațiuni financiare*
  - *Subsistemul IT pentru activitatea contabilă*
  - *Subsistemul IT pentru activitatea juridică*
  - *Subsistemul IT de coordonare a relațiilor 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: 08.04.2005

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

Lista control nr. 3.6.

privind Existența controalelor generale la nivelul subsistemelor IT

Nr. Crt.	**Elemente testate** **Eşantion**	Controlul datelor introduse în aplicații	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 complecte	Validarea datelor transferate din alte aplicații	Controale care verifică înregistrările duble	Autorizarea electronică şi/sau manuală a tranzacțiilor	Efectuarea tranzacțiilor numai de la computere definite în prealabil	Păstrarea integrală a înregistrărilor astfel încât să se poată urmări tranzacțiile efectuate din faza de inițiere până la finalizarea lor	Înțelegerea 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 operațiuni 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 relațiilor bugetare cu Uniunea Europeană*	X	X	X	FIAP	X	X	X	X	X

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

Procedura - P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Compartimentul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI NR. 3.6.

Misiunea de audit: *Audit IT*
Perioada auditată: 01.01.2005 – 01.01.2006

PROBLEMA: Inexistența controalelor generale implementate la nivelul subsistemelor IT.

CONSTATARE

Din evaluare, auditorii interni au constatat că nu există un sistem de controale generale care vor fi avute în vedere în procesul de proiectare, realizare, testare şi implementare al tuturor subsistemelor IT ce rulează pe echipamentele entității publice, astfel:

- Controlul datelor introduse în aplicații;
- 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 complecte;
- Validarea datelor transferate din alte aplicații;
- Efectuarea tranzacțiilor numai de la computere definite în prealabil.

CAUZE

- Inexistența procedurilor scrise şi formalizate;
- Neimplementarea controalelor generale.

CONSECINȚE

Inexistența 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.

RECOMANDĂRI

- Realizarea unui sistem de implementare al controalelor generale;
- Implementarea controalelor generale la nivelul tuturor subsistemelor IT pentru asigurarea unui grad de siguranță sporit al integrității datelor electronice;

- Stabilirea unui responsabil cu elaborarea sistemului de controale generale şi cu actualizarea periodică a acestuia;
- Coroborarea atribuțiilor stabilite cu fişele postului;
- Informarea echipei de auditori cu privire la controalele generale implementate.

Întocmit,	Supervizat,	Pentru conformitate,
Popescu Sorin	Dumitru Daniel	Pătrulescu George

FOAIE DE LUCRU NR. 3.8.

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: 08.04.2005

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

Procedura - P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Compartimentul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI NR. 3.8.

Misiunea de audit: *Audit IT*
Perioada auditată: 01.01.2005 – 01.01.2006

PROBLEMA

Utilizarea în cadrul entității publice a unor programe software fără licență.

CONSTATARE

- Din analiză s-a constatat că în cadrul unor departamente se folosesc programe aferente pachetului Microsoft Office fără ca pentru acestea entitatea publică să fi achiziționat licențe.
- Practic salariații au instalat programe utilizând CD-uri pirat.
- La nivelul sistemului IT al entității publice s-a constatat inexistența controalelor de sistem ce alertează administratorul în cazul utilizării de soft-uri pentru care nu s-au achiziționat licențe .

CAUZE

- Inexistența unor proceduri scrise şi formalizate
- Entitatea publică a achiziționat licențe pentru pachetul de programe Lotus. Salariații entității publice au observat că deşi programele Lotus le permit realizarea sarcinilor de serviciu, totuşi programele cuprinse în pachetul Microsoft Office sunt mai fiabile, mai flexibile, şi permit realizarea unui număr mai mare de operațiuni.
- De asemenea această situație a fost generată şi de primirea de la alte entități publice de fişiere electronice create cu programele din pachetul Microsoft Office.

CONSECINȚE

- Entitatea publică fiind pasibilă de amenzi pentru utilizarea unor programe fără licentă;
- Soft-urile nelicențiate instalate de utilizatori pot conține 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.

RECOMANDĂRI

- Elaborarea procedurilor pentru elaborarea programelor informatice pentru alertarea administratorilor de sistem;
- Stabilirea unui responsabil cu elaborarea procedurilor şi actualizarea lor;
- Coroborarea atribuțiilor din proceduri cu fişele posturilor;
- Inventarierea tuturor stațiilor de lucru pentru a stabili situația reală privind utilizarea programelor fără licență
- Dezinstalarea tuturor programelor din pachetul Microsoft Office instalate ilegal;
- Elaborarea unui angajament prin care toți salariații entității publice să-şi asume întreaga responsabilitate asupra urmărilor utilizării de soft-uri pirat;
- Realizarea unei analize complexe cost/calitate în urma căreia managementul entității publice să decidă dacă este necesară achiziționarea unui număr adecvat de licențe Microsoft Office.

Întocmit,	Supervizat,	Pentru conformitate,
Popescu Sorin	Dumitru Daniel	Pătrulescu George

Lista control nr. 3.8.

privind Situația licențelor pentru programele de calculator

Elemente Testate / Eşantion	**Verificarea situației licențelor deținute atât pentru sistemul de operare Windows NT**	**Verificarea situației licențelor deținute atât pentru pachetul de programe Microsoft Office**	**Verificarea existenței soft-urilor nelicențiate instalate de utilizatori**	**Verificarea existenței controalelor de sistem ce alertează administratorul în cazul utilizării de soft-uri pentru care nu s-au achiziționat licențe**
*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

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

Procedura - P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Compartimentul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI NR. 3.8.

Misiunea de audit: *Audit IT*
Perioada auditată: 01.01.2005 – 01.01.2006

PROBLEMA

Utilizarea în cadrul entității publice a unor programe software fără licență.

CONSTATARE

- Din analiză s-a constatat că în cadrul unor departamente se folosesc programe aferente pachetului Microsoft Office fără ca pentru acestea entitatea publică să fi achiziționat licențe.
- Practic salariații au instalat programe utilizând CD-uri pirat.
- La nivelul sistemului IT al entității publice s-a constatat inexistența controalelor de sistem ce alertează administratorul în cazul utilizării de soft-uri pentru care nu s-au achiziționat licențe .

CAUZE

- Inexistența unor proceduri scrise şi formalizate
- Entitatea publică a achiziționat licențe pentru pachetul de programe Lotus. Salariații entității publice au observat că deşi programele Lotus le permit realizarea sarcinilor de serviciu, totuşi programele cuprinse în pachetul Microsoft Office sunt mai fiabile, mai flexibile, şi permit realizarea unui număr mai mare de operațiuni.
- De asemenea această situație a fost generată şi de primirea de la alte entități publice de fişiere electronice create cu programele din pachetul Microsoft Office.

CONSECINȚE

- Entitatea publică fiind pasibilă de amenzi pentru utilizarea unor programe fără licentă;
- Soft-urile nelicențiate instalate de utilizatori pot conține 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.

RECOMANDĂRI

- Elaborarea procedurilor pentru elaborarea programelor informatice pentru alertarea administratorilor de sistem;
- Stabilirea unui responsabil cu elaborarea procedurilor şi actualizarea lor;

- Coroborarea atribuțiilor din proceduri cu fişele posturilor;
- Inventarierea tuturor stațiilor de lucru pentru a stabili situația reală privind utilizarea programelor fără licență
- Dezinstalarea tuturor programelor din pachetul Microsoft Office instalate ilegal;
- Elaborarea unui angajament prin care toți salariații entității publice să-şi asume întreaga responsabilitate asupra urmărilor utilizării de soft-uri pirat;
- Realizarea unei analize complexe cost/calitate în urma căreia managementul entității publice să decidă dacă este necesară achiziționarea unui număr adecvat de licențe Microsoft Office.

Întocmit,	Supervizat,	Pentru conformitate,
Popescu Sorin	Dumitru Daniel	Pătrulescu George

ENTITATEA PUBLICĂ
Serviciul Audit Intern

NOTĂ DE RELAȚII NR. 3.11.

privind respectarea cadrului normativ referitor la
instruirea utilzatorilor sistemului IT
adresat
domnului Pătrulescu George, conducător Direcția IT

Întrebarea nr. 1: *Au fost întocmite programe de instruire a utilizatorilor subsistemelor IT?*
Răspuns nr. 1: *În cadrul Departamentului IT au fost elaborate programe de instruire pentru utilizatorii fiecărui sub-sistem pus în funcțiune. Practic, o parte din utilizatori cunosc subsistemul IT înainte de a fi dat în funcționare, fiind implicați în realizarea subsistemului încă din fazele incipiente (studiu de fezabilitate, testare) ei fiind cei mai în măsură să exprime o părere pertinentă, pe baza experienței acumulate, asupra cerințelor practice ce trebuiesc îndeplinite de programele informatice. Sunt organizate seminarii pentru prezentarea aplicațiilor utilizatorilor.*

Întrebarea nr. 2: Sunt identificate nevoile de pregătire profesională a utilizatorilor?
Răspuns nr. 2: Pe baza obiectivelor ce trebuiesc îndeplinite de programele informatice şi a documentației tehnice elaborate, echipa ce a realizat aplicația stabileşte în faza post-implementare cerințele specifice de pregătire profesională a utilizatorilor. *Aceste cerințe sunt luate în considerație în etapa de elaborare a documentației-suport de curs.*

Întrebarea nr. 3: Sunt testate cunoştințele utilizatorilor acumulate în timpul seminariilor de prezentare a aplicației realizate?
Răspuns nr. 3: Nu.

Întrebarea nr. 4: Sunt participanții la seminarii invitați să-şi exprime opinia asupra utilității cunoştințelor profesionale prezentate?
Răspuns nr. 4: *Nu.*

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

Auditor intern,
Popescu Sorin

Supervizor,
Dumitru Daniel

Nota :
Pe baza Notei de relații nr. 3.4. nu se va elabora FIAP, dar aspectele negative constatate vor fi menționate în Raportul de audit intern.

LISTA DE VERIFICARE NR. 4

Obiectivul IV. SECURITATEA IT

Nr. crt.	ACTIVITATEA DE AUDIT	DA	NU	OBS.
4.1.	*Examinarea procedurilor privind securitatea IT*			
	4.1.1. Verificarea gradului de acoperire prin proceduri a activităților realizate	-	-	
	a. Aprobarea procedurilor de către persoanele competente;	-	-	
	b. Stabilirea modelelor de formulare specifice;	-	-	
	a. Precizarea modalităților de complectare a modelelor;	-	-	
	d. Oferirea unor exemple în acest sens;	-	-	
	e. Actualizarea sistematică a procedurilor;	-	-	
	f. Conformitatea procedurilor cu politica IT;	-	-	
	4.1.2.Înglobarea activităților de control intern în punctele cheie ale procesului;	-	-	
	4.1.3. Respectarea principiul dublei semnături;	-	-	
	4.1.4. Stabilirea responsabilităților persoanelor implicate în activitatea de securitate IT;	-	-	
	4.1.5. Asigurarea transpunerii prelucrărilor într-un sistem informatizat, respectiv realizarea codificării modelelor de formulare şi informațiile activităților, algoritmi de prelucrare ş.a.	-	-	
	4.1.6. Modalitatea arhivării documentelor.	-	-	
4.2.	*Compararea atribuțiilor cuprinse în proceduri cu cele din fişele posturilor*	-	-	
4.3.	*Examinarea cunoaşterii procedurilor de către responsabilii cu realizarea acestei activități*	-	-	
4.3.	*Aprecierea calității procedurilor de către personalul de execuție:*			
	a) consideră procedurile corespunzătoare?	-	-	
	b) constatată disfuncționalități în timpul aplicării practice?	-	-	
	c) există propuneri de perfecționare a procedurilor	-	-	
	d) modul de soluționare a propunerilor de perfecționare a procedurilor	-	-	
4.5.	*Politica de securitate IT*	**X**		
	Verificați existența politicii de securitate IT	**X**		
	Verificați actualizarea politicii de securitate IT	**X**		**Interviu nr. 4.5.**
4.6.	*Monitorizarea implementării politicii de securitate IT*	**X**		
	Verificați desemnarea unui responsabil cu monitorizarea implementării politicii de securitate IT	**X**		
	Analizați întocmirea şi transmiterea sistematică a rapoartelor de monitorizare			

Nr. crt.	ACTIVITATEA DE AUDIT	DA	NU	OBS.
4.7.	*Evaluarea controalelor fizice în domeniul IT*	**X**		
	a. Verificaţi efectuarea controalelor fizice conform procedurilor	-	-	**Test nr. 4.7.** **Listă de control nr. 4.7.**
	b. Verificaţi existenţa surselor alternative de energie electrică	-	-	
	c. Verificaţi realizarea sistematică a serviciilor de mentenanţă	-	-	
	d. Verificaţi restricţionarea accesul la servere-le IT numai al persoanelor autorizate, ţinând cont de pericolul deteriorării acestor echipamentelor IT sau al datelor critice pe care le procesează;	-	-	
	e. Verificaţi dotarea 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;		**X**	
	- senzori de mişcare;		**X**	
	- sistem de alarmă în caz de incendiu;	**X**		
	- sistem de stingere a incendiilor;	**X**		
	- echipamente de aer condiţionat;	**X**		
	- uşi neinflamabile echipate cu încuietori adecvate.		**X**	
4.8.	*Siguranţa accesului la reţea şi a comunicării datelor în reţea*	**X**		
	Verificarea alocării numelui de utilizator şi parolei aferente pentru accesul la reţea		**X**	**Test nr. 4.8.** **Foaie de lucru nr. 4.8.** **Listă de control nr. 4.8.** **FIAP nr. 4.8.**
	Monitorizarea conectării la reţea conform listei de logg-are	**X**		
	Analizaţi dacă a fost elaborată documentaţia tehnică adecvată privind conectarea la Internet.	-	-	
	Verificaţi dacă această documentaţie este adecvată şi actualizată sistematic.	-	-	
	Determinaţi dacă manualele de utilizare a reţelei au în vedere asigurarea securităţii comunicării datelor în reţea.	-	-	
	Analizaţi acţiunile întreprinse în cazurile în care este ameninţată integritatea şi eficacitatea transmiterii datelor în reţea.	-	-	
	Analizaţi rapoartele de monitorizare a traficului datelor în reţea.	-	-	
4.9.	*Programele anti-virus*	**X**		
	Verificaţi implementarea programelor anti-virus conform procedurilor:	**X**		**Test nr. 4.9.** **Foaie de lucru nr. 4.9.** **Listă de control nr. 4.9.** **FIAP nr. 4.9.**
	- instalarea unui program anti-virus adecvat necesităţilor utilizatorilor staţiilor de lucru;		**X**	
	- programul anti-virus să verifice staţia de lucru la pornire;		**X**	
	- programul anti-virus să monitorizeze toate programele şi aplicaţiile active, mesajele primite şi să verifice automat actualizările la intervale regulate (zilnic);		**X**	
	- programul anti-virus să se actualizeze în reţea, astfel încât să protejeze eficient datele electronice împotriva viruşilor nou-apăruţi		**X**	
	Monitorizarea sistematică a funcţionalităţii programelor anti-virus	**X**		

Nr. crt.	ACTIVITATEA DE AUDIT	DA	NU	OBS.
	Verificați sistemul de actualizare a programelor anti-virus	**X**		
4.10.	*Recuperarea datelor în caz de dezastru*	**X**		
	Elaborarea planului de recuperare a datelor în caz de dezastru.	**X**		**Interviu nr. 4.10.** **FIAP nr. 4.10.**
	a. Aprobarea planului de recuperare a datelor în caz de dezastru.	**X**		
	b. Desemnarea echipei de implementare a planului şi a responsabilităților adecvate membrilor echipei	**X**		
	c. Comunicarea planului personalului cu responsabilități în punerea în aplicare a acestuia în caz de dezastru.		**X**	
	d. Analizați dacă planul de recuperare a datelor a fost testat şi modificat periodic în baza rezultatelor obținute în urma testării		**X**	
	e. Cuprinderea tuturor domeniilor de acțiune importante ale entității publice în structura planului.	**X**		
	f. Identificarea principalele procese şi aplicații IT ce trebuiesc recuperate	**X**		
	g. Analizarea implementării cerințelor specifice privind recuperarea datelor în caz de dezastru la nivelul sistemului IT.	**X**		
	Verificați desemnarea responsabililor cu monitorizarea implementării procedurilor privind recuperarea datelor în caz de dezastru	**X**		
	Verificați efectuarea monitorizării sistematice	**X**		
	Verificați luarea măsurilor necesare privind recuperarea datelor în caz de dezastru conform procedurilor	**X**		
	a. Verificați dacă datele stocate pentru a fi recuperate în caz de dezastru sunt actualizate sistematic.	**X**		
	b. Stabiliți dacă locația în care sunt stocate datele pentru a fi recuperate în caz de dezastru este adecvată		**X**	
4.11.	*Sistemul de arhivare*	**-**	**-**	
	Verificarea modului de arhivare a datelor	**-**	**-**	
	Verificați evaluarea periodică a activității de arhivare	**-**	**-**	

Data: 01.04.2005

Auditor intern,
Radu George

Supervizor,
Dumitru Daniel

ENTITATEA PUBLICĂ
Serviciul Audit Intern

INTERVIU nr. 4.5.
privind Politica de securitate IT
adresat
domnului Pătrulescu George, Director Direcția IT

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005 - 31.12.2005

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 aveți ceva de adăugat?		X	

Data: 03.04.2005 Auditori, Intervievat,

NOTA:
Pe baza răspunsurilor la interviu şi a documentelor transmise s-a hotărât ca pentru acest obiectiv să nu se elaboreze FIAP.
Informațiile primite în cadrul interviului vor fi utilizate la elaborarea Raportului de audit intern.

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

TEST NR. 4.7.

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005- 31.12.2005

Obiectul testului : *Securitatea IT*.

Obiectivele testului: Verificați efectuarea controalelor fizice conform procedurilor

Descrierea testului

Populația statistică a fost constituită din cele 15 direcții generale ale unității identificate ca urmare a analizei organigramei entității publice.

Eşantionul a fost constituit prin selectarea aleatoare a Direcției IT precum şi a Departamentului Financiar Contabil şi a Departamentului Resurse Umane unde sunt localizate servere ce deservesc necesitățile lor specifice, respectiv 20% din totalul populației.

Testarea a constat în examinarea următoarelor elemente stabilite prin *Lista de verificare nr. 4, poz. 4.7, litera e)*, şi anume:

- Verificați dotarea 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 condiționat;
  - uşi neinflamabile echipate cu încuietori adecvate.

Testarea s-a concretizat în elaborarea *Listei de control nr. 1 privind Efectuarea controalelor fizice*.

Constatări

Din analiza *Listei de control* rezultate, s-au constatat mai multe disfuncționalități:

- accesul necontrolat la toate cele trei locații selectate (Centrul IT, Departamentului Financiar Contabil, Departamentul Resurse Umane) atât al persoanelor din cadrul altor departamente cât şi alte persoane din afara entității publice;

- deşi au fost instalate camere de supraveghere acestea nu sunt permanent monitorizate;
- deseori, camerele în care sunt localizate serverele sunt lăsate descuiate şi nesupravegheate, deşi sunt echipate cu încuietori adecvate;

Din analiza, am constatat că nu există obligativitatea prezentării unei autorizații scrise pentru a scoate echipamente IT din clădirea entității publice. Considerăm că această situație trebuie urgent remediată pentru a se evita furtul echipamentelor IT.

Concluzii

În acest caz nu se va elabora FIAP.

Data: 01.04.2005

Auditor intern, Supervizor,

Lista control nr. 4.7.

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 condiționat	Uşi neinflamabile echipate cu încuietori adecvate
Direcția 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

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 precum şi nici senzori de mişcare la nivelul Departamentul Resurse Umane. În prezenta Listă de control auditorii au punctat lipsa acestor controale cu mențiunea "Nu" deoarece situația a fost remediată în timpul misiunii de audit şi nu s-a mai întocmit FIAP, dar aspectele negative constatate vor fi menționate în Raportul de audit intern.

Auditor,
Radu George

Supervizor,
Dumitru Daniel

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

TEST NR. 4.8.

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005- 31.12.2005

Obiectul testului: *Securitatea IT.*

Obiectivele testului: *Siguranța accesului la rețea şi a comunicării datelor în rețea*

Descrierea testului

Populația statistică a fost constituită din cele 250 de calculatoare existente la nivelul entității publice, conform *Listei de inventariere a calculatoarelor personale*.

Eşantionul pentru realizarea testării siguranței accesului la rețea a fost stabilit pe baza unui procent de 2%, din totalul populației statistice, respectiv 5 calculatoare personale, conform *Foii de lucru nr. 4.2.*

Testarea a constat în examinarea următoarelor elemente stabilite prin *Lista de verificare nr. 4, poz. 4.8*, şi anume:

- Verificați modul de alocare a numelui de utilizator şi parolei aferente pentru accesul la rețea ;
- Monitorizarea conectării la rețea conform listei de logg-are.

Testarea s-a concretizat în elaborarea *Listei de control nr. 4.2. privind Accesul şi comunicarea datelor în rețea*.

Constatări

Din analiza *Listei de control nr. 4.2.* rezultate, s-a constatat că:

a. majoritatea salariaților din cadrul entității 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.
b. datorită numărului mare de parole ce trebuiesc utilizate de salariați, deseori aceştia notează parolele pe documente lăsate pe birou. Astfel salariații 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 funcții principale de restricționare a accesului persoanelor nepotrivite ci îngreunează funcționarea sistemului.
d. în situația apariției unor incidente nu se pot stabili responsabilitățile adecvate.

Concluzii

În acest caz se va elabora FIAP nr. 4.8.

Data: 01.04.2005

Auditor intern,
Georgescu Ion

Supervizor,
Ionescu Mircea

FOAIE DE LUCRU NR. 4.8.

Obiectul 4.: *Securitatea IT*

Obiectivul : Siguranța accesului la rețea şi a comunicării datelor în rețea

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

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

Data: 08.04.2005

Auditor,
Radu George

Supervizor,
Dumitru Daniel

Lista control nr. 4.8.

privind Accesul şi comunicarea datelor în rețea

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

Auditor,
Radu George

Supervizor,
Dumitru Daniel

Procedura - P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Compartimentul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI NR. 4.8.

Misiunea de audit: *Audit IT*
Perioada auditată: 01.01.2005 – 01.01.2006

PROBLEMA

Neutilizarea unui singur nume de utilizator şi unei singure parole pentru accesul la sistemul IT.

CONSTATARE

Din evaluare s-a constatat că majoritatea salariaților din cadrul entității 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.

CAUZE

- Inexistența unor proceduri adecvate de conectare a utilizatorilor la rețea;
- Lipsă corelării dintre atribuțiile de serviciu şi fişele de post ale salariaților.

CONSECINȚE

- Datorită numărului mare de parole ce trebuiesc utilizate de salariați, deseori aceştia notează parolele pe documente lăsate pe birou. Astfel salariații 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.

- Practic, sistemul de parole nu mai are funcții principale de restricționare a accesului persoanelor nepotrivite ci îngreunează funcționarea sistemului.

- În situația apariției unor incidente nu se pot stabili responsabilitățile adecvate.

RECOMANDĂRI

- Realizarea unui proces de reenginering la nivelul sistemului IT din cadrul entității publice, astfel încât salariații să poată accesa subsistemele IT de care au nevoie utilizând un singur nume de utilizator şi o singură parolă;
- Stabilirea unui responsabil pentru derularea acestui proces reenginering al sistemului IT
- Implementarea unui sistem de raportare potrivit căruia responsabilul desemnat să întocmească periodic rapoarte de activitate către managementul general al entității publice prin care să specifice acțiunile întreprinse;
- Instruirea adecvată a salariaților ce utilizează sistemul IT;
- Informarea echipei de auditori în privința stadiului elaborării, însuşirii şi monitorizării riscurilor.

Întocmit,	Supervizat,	Pentru conformitate,
Radu George	Dumitru Daniel	Eleodor Darius

Procedura P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Public Intern

TEST NR. 4.9.

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005- 31.12.2005

Obiectul testului: *Securitatea IT.*

Obiectivele testului: *Programele 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, conform *Foii de lucru nr. 4.9.*

Testarea a constat în examinarea următoarelor elemente stabilite prin *Lista de verificare nr. 4, poz. 4.9*, şi anume:

- Verificarea implementarea 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.
- Monitorizarea sistematică a funcţionalităţii programelor anti-virus;
- Verificaţi sistemul de actualizare a programelor anti-virus.

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).

Echipa de auditori a verificat 5 de staţii de lucru, selectate din cadrul tuturor departamentelor.

Din analiza *Listei de control nr. 4.9.* rezultate, s-a constatat că:

- În cazul a 2 calculatoare din cadrul entității publice configurația programului anti-virus a fost modificată pentru a întrerupe monitorizarea întregii activități 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 performanței sistemului;
- Urmare acestei constatări, am verificat respectivele stații de lucru pentru a descoperi prezența viruşilor şi am descoperit că toate erau infectate cu viruşi.

Concluzii

În acest caz se va elabora FIAP.

Data: 01.04.2005

Auditor intern, Supervizor,

FOAIE DE LUCRU NR. 4.9.

Obiectul 4. : *SECURITATEA IT*

Obiectivul : *Programele anti-virus*

Testarea se va realiza pe un eşantion care a fost constituit astfel:
- populația totală este de 250 calculatoare personale;
- eşantionul va fi de 2%, respectiv 250 x 2% = 5 calculatoare personale;
- pasul de selecție va fi 250 : 5 = 50;
- eşantionul se va constitui din calculatoarele existente în Lista IP-urilor calculatoarelor ce se conectează la rețeaua entității publice la pozițiile:
  11, 61, 111, 161, 211
  conform celor prezentate în Lista de control anexată la Testul nr. 4.9.:
- eşantionul constituit va fi verificat integral;
- în urma verificării se va întocmi un test.

Data: 08.04.2005

Auditor,
Radu George

Supervizor,
Dumitru Daniel

Lista control nr. 4.9.

privind Programele anti-virus

Elemente Testate / **Eşantion**	Verificarea implementarea programelor anti-virus conform procedurilor				Monitorizarea sistematică a funcționalității programelor anti-virus	Verificarea sistemului de actualizare a programelor anti-virus
	Instalarea unui program anti-virus adecvat necesităților utilizatorilor stațiilor de lucru	Programul anti-virus să verifică stația de lucru la pornire	Programul anti-virus monitorizează toate programele şi aplicațiile active, mesajele primite şi verifică automat actualizările la intervale regulate (zilnic)	Programul anti-virus se actualizează în rețea, astfel încât să protejeze eficient datele electronice împotriva viruşilor nou-apăruți		
Computer aflat la poziția 11	X	X	**X**	**X**	X	X
Computer aflat la poziția 61	X	X	**X**	X	X	X
Computer aflat la poziția 111	FIAP	FIAP	FIAP	FIAP	FIAP	FIAP
Computer aflat la poziția 161	FIAP	FIAP	FIAP	FIAP	FIAP	FIAP
Computer aflat la poziția 211	NU	X	**X**	X	X	X

Auditor,
Radu George

Supervizor,
Dumitru Daniel

Procedura - P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI NR. 4.9.

Misiunea de audit: *Audit IT*
Perioada auditată:

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.

CONSTATARE

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 15 de staţii de lucru, selectate în mod aleator, din cadrul tuturor departamentelor şi a constatat următoarele:

- În 5 departamente 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 descoperit că toate erau infectate cu viruşi.

CAUZE

- Inexistenţa unei proceduri pentru aplicarea în mod unitar a politicii de securitate IT;
- Lipsa procedurilor formalizate care să prevadă acţiunile ce trebuiesc întreprinse în cazul modificării configuraţiei programului anti-virus.

CONSECINŢE

- Prezenţa viruşilor şi a altor programe dăunătoare pe staţiile de lucru afectează în mod negativ activitatea utilizatorilor din cadrul departamentelor.
- Existenţa viruşilor ridică numeroase semne de întrebare în privinţa exactităţii datelor stocate în sistemul IT.

RECOMANDĂRI

- Elaborarea procedurilor formalizate care să prevadă acțiunile ce trebuiesc întreprinse în cazul modificării configurației programului anti-virus;
- Stabilirea unui responsabil pentru elaborarea şi actualizarea procedurilor;
- Coroborarea atribuțiilor şi responsabilităților stabilite prin fişele posturilor cu sarcinile stabilite prin proceduri;
- Monitorizarea aplicării în mod unitar a politicii de securitate IT;
- Constituirea unor echipe pentru efectuarea de verificări anti-virus la nivelul tuturor stațiilor de lucru din cadrul entității publice;

Întocmit,	Supervizat,	Pentru conformitate,
Radu George	Dumitru Daniel	Eleodor Darius

ENTITATEA PUBLICĂ
Serviciul Audit Intern

INTERVIU nr. 4.10.
privind recuperarea datelor în caz de dezastru
adresat
domnului Bălăşoiu Gheorghe, şef Serviciul Asistenţă Tehnică

Misiunea de audit: Audit IT
Perioada auditată: 01.01.2005 - 31.12.2005

Nr. crt.	*Întrebări*	Da	Nu	Obs.
1.	Elaborarea planului de recuperare a datelor în caz de dezastru.	X		
	a. Aprobarea planului de recuperare a datelor în caz de dezastru.	X		
	b. Desemnarea echipei de implementare a planului şi a responsabilităţilor adecvate membrilor echipei	X		
	c. Comunicarea planului personalului cu responsabilităţi în punerea în aplicare a acestuia în caz de dezastru.		X	*FIAP nr. 4.10.*
	d. Analizaţi dacă planul de recuperare a datelor a fost testat şi modificat periodic în baza rezultatelor obţinute în urma testării		X	*FIAP nr. 4.10.*
	e. Cuprinderea tuturor domeniilor de acţiune importante ale entităţii publice în structura planului.	X		
	f. Identificarea principalele procese şi aplicaţii IT ce trebuiesc recuperate	X		
	g. Analizarea implementării cerinţelor specifice privind recuperarea datelor în caz de dezastru la nivelul sistemului IT.	X		
2.	Desemnarea responsabililor cu monitorizarea implementării procedurilor privind recuperarea datelor în caz de dezastru	X		
3.	Luarea măsurilor necesare privind recuperarea datelor în caz de dezastru conform procedurilor	X		
	a. Verificaţi dacă datele stocate pentru a fi recuperate în caz de dezastru sunt actualizate sistematic.	X		
	b. Stabiliţi dacă locaţia în care sunt stocate datele pentru a fi recuperate în caz de dezastru este adecvată		X	*FIAP nr. 4.10.*

Data: 03.04.2005 Auditori, Intervievat,

NOTA:
Pe baza răspunsurilor la interviu şi a documentelor transmise s-a hotărât ca pentru acest obiectiv să se elaboreze FIAP nr. 4.4. Informaţiile primite prin documentele transmise în cadrul interviului vor fi utilizate la elaborarea Raportului de audit intern.

Procedura - P08: Colectarea dovezilor

ENTITATEA PUBLICĂ
Serviciul Audit Intern

FIŞĂ DE IDENTIFICARE ŞI ANALIZĂ A PROBLEMEI NR. 4.10.

Misiunea de audit: *Audit IT*
Perioada auditată:

PROBLEMA

Nerecuperarea datelor în cazul producerii unui eventual dezastru.

CONSTATARE

Echipa de auditori a constatat că deşi există un Plan de recuperare în caz de dezastru aprobat, acesta nu a fost niciodată nici testat, nici comunicat membrilor cheie ai entității publice, cărora li se va cere să pună planul în aplicare în caz de dezastru. Este posibil ca datele de rezervă să nu fie nici disponibile, nici utilizabile conform planificării, în cazul în care ar fi necesare pentru a realiza o recuperare.

Din analiză, a rezultat că deşi au fost amenajate facilități în aşteptare de recuperare a datelor în caz de dezastru, acestea nu au fost testate pentru a se garanta că sunt eficiente, funcționabile şi actualizate pentru a face față cerințelor impuse de schimbările tehnologice implementate.

CAUZE

- Inexistența unei proceduri pentru testarea Planului de recuperare a datelor în caz de dezastru;
- Neaplicarea în mod unitar a procedurilor privind recuperarea datelor în caz de dezastru.

CONSECINȚE

- Incapacitatea de recuperare completă a datelor în caz de dezastru, conform cerințelor planificate;
- Într-o situația producerii unui dezastru activitățile stabilite prin planul de recuperare a datelor se pot dovedi insuficiente pentru atingerea obiectivelor stabilite.

RECOMANDĂRI

- Alocarea de roluri şi responsabilități, iar Planul a datelor în caz de dezastru trebuie comunicat tuturor persoanelor responsabile;
- Testarea şi apoi actualizarea planului astfel încât să faciliteze recuperarea datelor cu succes.
- Back-up-urile trebuie stocate în siguranță în afara sediului.
- Verificarea tuturor exemplarele de rezervă înainte de fi depozitate;
- Monitorizarea sistematică de către management a modului în care sunt aplicate procedurilor privind recuperarea datelor în caz de dezastru.

Întocmit,	Supervizat,	Pentru conformitate,
Radu George	Dumitru Daniel	Badea Ştefan

Procedura – P11: Şedința de închidere

ENTITATEA PUBLICĂ
Compartimentul Audit Intern

MINUTA ŞEDINȚEI DE ÎNCHIDERE

Misiunea de audit: Tehnologia Informației
Perioada auditată: 01.01.2005-01.01.2006
Întocmit: Popescu Sorin/Radu George Data: 15.03.2006
Avizat: Dumitru Daniel Data: 15.03.2006

***Lista participanților*:**

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

Stenograma şedinței:

- Prezentarea obiectivelor auditate si constatărilor pentru fiecare obiect auditat; a fost discutată fiecare deficiență în parte, au fost analizate cauzele care au contribuit la realizarea disfunctionalității, au fost prezentate recomandările care urmează a fi implementate pentru eliminarea deficiențelor constatate.
- In cadrul Sedintei de inchidere structura auditata si-a insusit in totalitate constatarile si recomandarile formulate de echipa de auditori.
- In consecinta, *proiectul Raportului de audit intern* devine *Raport de audit intern final* care va fi pregatit pentru aprobare si transmitere structurii auditate. Raportul de audit intern va fi insotit de o SINTEZA care va contine concluziile echipei de auditori interni cu prezentarea principalelor recomandari si opinia generala a acesteia.
- Structura auditata se angajeaza sa completeze *Planul de actiune si calendarul implementarii recomandarilor*, cu termenele de realizare si persoanele responsabile cu implementare acestora, pe care il vor discuta cu echipa de auditori.

ENTITATEA PUBLICA
Compartimentul Audit Intern **PROIECT**

RAPORT DE AUDIT INTERN

STRUCTURA AUDITATĂ:
DIRECȚIA TEHNOLOGIA INFORMAȚIEI

MISIUNEA DE AUDIT INTERN
PRIVIND
SISTEMUL INFORMATIC

BUCURESTI
2006

I. INTRODUCERE

Echipa de auditare a fost formata din :

- Popescu Sorin - auditor superior, cooordonator al misiunii;
- Radu George - auditor superior.

Auditorii fac parte din Compartimentul de Audit Intern al entitatii publice.

Ordinul de efectuare a misiunii de audit - Ordinul de serviciu nr. 25/08.01.2006 aprobat de conducătorul entității publice.

Baza legală a acțiunii de auditare:

- Planul de audit intern pentru anul 2006, aprobat de conducerea instituției;
- Legea nr. 672/2002 privind auditul public intern, cu modificarile si completarile ulterioare;
- OMFP nr. 38/15.01.2003 prin care se aproba Normele metodologice de aplicare a Legii nr. 672/2002, cu modificarile si completarile ulterioare;
- Ordinul prin care se aproba Normele proprii de exercitare a auditului intern în cadrul entitatii publice.

Durata acțiunii de auditare – 25.01.2006 – 17.04.2006.

Perioada supusă auditării – 01.01.2005 – 31.12.2005

Scopul misiunii de audit intern este acela de evaluare a activității IT de la nivelul entitatii publice, in ceea ce priveste respectarea conditiilor de legalitate, economicitate, eficacitate, de a adauga valoare prin formularea recomandarilor, iar in cazul identificarii unor probleme/iregularități, de corectare a acestora.

Obiectivele misiunii de audit intern:

- ***Planul strategic;***
- *Organizarea şi funcționarea Departamentului IT;*
- *Implementarea sistemului IT;*
- *Securitatea IT.*

Tipul de auditare – Echipa de auditori interni a efectuat un audit de conformitate/regularitate privind respectarea principiilor, regulilor metodologice si procedurale in ceea ce priveste activitatea IT de la nivelul entității publice.

Principalele tehnici si instrumente de audit utilizate:

- *interviul* pentru lămurirea de aspecte legate de organizarea şi desfăşurarea activităților;
- *testarea* pentru urmairea detectarii erorilor sau a iregularitatilor;
- *eşantionarea* pentru analiza întocmirii documentelor şi efectuarea plăților;
- *observarea fizică* în vederea formării unei păreri proprii privind modul de întocmire şi emitere a documentelor;

- *liste de verificare* pentru a stabili condițiile pe care trebuie să le îndeplinească fiecare domeniu auditabil;
- *liste de control*;
- *chestionare*;
- *FIAP-uri* intocmite pentru fiecare disfunctionalitate constatata;

Documente şi materiale examinate în cadrul Direcției IT - verificarea la fața locului a vizat următoarele materiale şi documente:

- Politica entității publice în domeniul IT;
- Planul strategic şi planurile anuale privind sistemul IT întocmite şi aprobate;
- Organigrama entității publice;
- Regulamentul de Organizare şi Funcționare si fisele posturilor;
- legislatia in vigoare privind activitatea IT;
- manuale de utilizare şi manuale de operare;
- planul de recuperare în caz de dezastru;
- procedurile aplicabile activității IT;
- alte documente.

Materialele întocmite pe timpul auditării au fost următoarele:

- teste si foi de lucru privind descrierea activităților auditate;
- fişe de identificare si analiză a problemelor constatate (FIAP);
- liste de verificare pe obiective (LV);
- documente de lucru;
- tabel *Puncte tari şi puncte slabe*,
- Tematica in detaliu;
- Programul de audit, Programul intervenției la fața locului;
- Chestionarul de control intern;
- raport de audit, minutele şedințelor de deschidere, închidere etc.

Departamentul IT este organizat ca direcție generală în cadrul entității publice având un număr de 7 servicii de specialitate. Organizarea şi funcționarea serviciului au fost conforme organigramei şi Regulamentului de organizare şi funcționare.

Pentru toți salariații sunt întocmite fişele posturilor prin care sunt stabilite relațiile ierarhice de subordonare şi sarcinile de serviciu.

Activități desfăşurate în cadrul Departamentului IT:

- *tehnoredactare şi dezvoltare aplicații multimedia;*
- *comunicații date în format electronic;*
- *analiza, proiectare şi programare a sistemului IT;*
- *administrare retele calculatoare;*
- *asistență tehnică a utilizatorilor.*

II. CONSTATĂRI SI RECOMANDARI

Evaluarea respectarii conditiilor de conformitate si regularitate a activității de tehnologie a informației la nivelul entității publice a pornint de la elaborarea planului strategic, defalcarea acestuia în planuri anuale, organizarea şi funcționarea departamentului IT, implementarea

sistemului informatic si securitatea datelor din acest sistem şi s-a materializat in elaborarea listelor de verificare, testelor bazate pe esantionare, verificarilor prin listele de control, observari fizice pe teren, interviurilor care au condus la solicitarea unor note de relatii, prin care s-au identificat o serie de probleme si defcienţelor care au fost inscrise in formularele de constatare (FIAP-uri).

Analiza activitatii de achizitii publice a impus evaluarea cadrului procedural existent care sta la baza organizarii si functionarii sistemului.

In continuare, prezentam principalele constatari, consecintele care s-au produs sau care ar putea sa apara in perioada imediat urmatoare, precum si recomandarile formulate in vederea corectarii disfunctionalitatilor semnalate sau ale celor care pot sa survina urmare acestora, diminuarii riscurilor existente si imbunatatirii sistemelor de management si control intern al activitatilor auditate cu scopul facilitarii atingerii obiectivelor prestabilite.

1. Plan strategic

1.1. Procedurile specifice care reglementeaza activitatea de achizitii publice

Pentru realizarea obiectivelor trebuie sa se asigure un echilibru intre sarcini, competente (autoritate decizionala conferita prin delegare) si responsabilitati (obligatia de a realiza obiectivele) si sa se defineasca **proceduri**.

Procedurile reprezinta pasii ce trebuie urmati si cuprind algoritmul pentru realizarea sarcinilor, exercitarea competentelor, existenta activitatilor de control in punctele cheie si angajarea responsabilitatilor.

Pe baza procedurilor, se monitorizeaza existenta si functionalitatea controlului intern, ceea ce ne va da posibilitatea sa constatam daca:

- este integrat in sistemul de management al fiecarei componente structurale a entitatii publice;
- intra in grija personalului de la toate nivelurile;
- ofera o asigurare rezonabila atingerii obiectivelor, incepand cu cele individuale si terminand cu cele generale.

In practica, există două categorii de proceduri:

- *procedurile generale* date de cadrul normativ, respectiv de legi, norme metodologice, precizări/instrucţiuni, elaborate de către entitatea publică, in vederea organizarii aplicării unor reglementări de rang superior, aprobate de către conducătorul entităţii publice sau chiar de către Guvern;
- *proceduri specifice* pentru fiecare activitate a entitatii publice sub forma metodologiilor de lucru, care trebuie să fie:
    - *scrise si formalizate* pe suport de hartie si/sau electronic, care sa contina pe fluxurile operatiilor, activitati de control, responsabilitati, modele de documente cu exemplificari respectiv formalizate, cunoştinţele individuale şi colective care trebuie stocate şi puse în ordinea care sa corespunda scopurilor entităţii publice si *aprobate de management*;
    - *simple şi specifice*, pentru ca executanţii să le poata utiliza cu respectarea cadrului normativ, pentru fiecare domeniu al entităţii publice;
    - *completate si actualizate în mod permanent*, în funcţie de evoluţia reglementărilor si practicii în materie;
    - *aduse la cunoştinţa executanţilor* pentru a putea fi discutate, insusite si aplicabile in mod uniform.

Echipa de auditori interni, din analiza a constatat ca in cadrul *Departamentului IT* atribuirea responsabilitatilor, separarea sarcinilor si delegarea autoritatilor nu sunt stabilite prin proceduri scrise si formalizate, care inca nu sunt elaborate, dar pasii care trebuie parcursi si algoritmurile de calcul sunt cunoscute de catre salariati si se regasesc in ROF si in fisele posturilor.

Totusi, fisele posturilor desi exista si sunt semnate, sunt prea generale, fara specificarea, pentru fiecare post, a atributiilor ce le revin, in conformitate cu cadrul normativ.

Persoanele implicate in realizarea actvității IT sunt informate despre sarcinile care le revin, dar nu sunt familiarizati cu desfasurarea activitatii pe baza de proceduri specifice fiecarei activitati.

Din aceste considerente, pe parcursul evaluarii, nu au fost testate procedurile de lucru pentru desfasurarea activitatilor specifice privind activitatea IT, desi au fost cuprinse in listele de verificate realizate pe obiectivele misiunii de audit intern, ci au fost urmarite operatiile si activitatile auditabile.

In baza acestor observatii, se regaseste ca o recomandare generala la toate obiectivele misiunii de audit intern, necesitatea elaborarii procedurilor scrise si formalizate.

1.2. Politica entității publice în domeniul IT

Auditorii interni au analizat atât politica entității publice în domeniul IT cât şi dacă aceasta asigură atingerea obiectivelor entității publice. În acest sens a fost examinat modul în care politica entității publice în domeniul IT se reflectă în planul strategic şi în planurile anuale, fără a fi constatate deficiențe majore.

1.3. Elaborarea planului strategic şi a planurilor anuale

Activitatea de auditare privind activitatea IT a analizat planificarea realizării sistemului IT prin planuri strategice şi planuri anuale. In acest sens, s-au inventariat documentele oficiale prin care au fost desemnate persoanele responsabile cu elaborarea şi actualizarea planului, examinându-se dacă responsabilitățile sunt clar definite.

Evaluarea activității de elaborarea a planului strategic a fost efectuată pe baza analizei sistemului de fundamentare al acestuia şi a sistemului de prioritizare al activităților cuprinse în plan, fără a fi constatate aspecte negative.

1.4. Subsistemele IT pentru funcțiile principale

A fost verificat modul de elaborare a subsistemelor IT pentru funcțiile principale ale entității publice, corelarea termenelor de realizare a subsistemelor precum şi întocmirea şi realizarea programului de instruire a utilizatorilor fiecărui subsistem în parte.

Echipa de auditori a constatat existența unor departamente care nu dispun de subsisteme IT specifice activităților care se desfăşoară în cadrul entității publice. Astfel, din analiză a rezultat că în cadrul entității publice există structuri nou-înființate ca urmare a recomandărilor Comisiei Europene şi a schimbărilor legislative, care nu au notificat departamentul IT în privința nevoilor lor de aplicații informatice specifice. În acelaşi timp, s-au constatat şi departamente nou înființate care au fost solicitate să-şi exprime nevoile pentru realizarea subsistemelor IT specifice activității lor, dar care nu s-au realizat conform planificării.

Această situație se datorează pe de o parte inexistenței la nivelul entității publice a unor proceduri complete de elaborare a strategiei IT care să permită actualizarea sistematica, functie de schimbările legislative iar pe de altă parte insuficienței personalului de specialitate.

Echipa de auditori consideră că domenii importante de activitate ale entității publice pentru care nu s-a realizat implementarea subsistemelor IT necesare pentru desfăşurarea activității au randamente scăzute, ceea ce afectează ansamblul entității publice.

Pentru îmbunătățirea activității desfățurate şi eliminarea defcienţelor constatate, au fost elaborate următoarele recomandări:

- Elaborarea unei proceduri scrise şi formalizate pentru actualizarea strategia IT la nivelul entității publice pentru departamentele nou-create;
- Stabilirea responsabilității pentru actualizarea strategiei IT;
- Preocupare pentru angajarea personalului de specialitate şi ocuparea posturilor vacante;
- Coroborarea atribuțiilor prezentate prin proceduri cu cele stabilite prin fişele posturilor;
- Inventarierea stadiului implementării subsistemelor IT la nivelul departamentelor entității publice şi stabilirea necesităților IT care trebuiesc incluse în strategia IT.

2. Organizarea şi funcționarea departamentului IT

2.1. Organizarea departamentului IT

Conform ogranigramei aprobate la nivelul conducerii entității publice, departamentul este constituit din şapte servicii de specialitate, astfel:

- *Serviciul de tehnoredactare şi dezvoltare aplicații multimedia*
- *Serviciul comunicații date*
- *Serviciul exploatarea echipamentelor*
- *Serviciul analiza, proiectare şi programare*
- *Serviciul retele calculatoare*
- *Serviciul sinteză dezvoltare*
- *Serviciul asistență tehnică.*

Echipa de auditori interni a analizat atât număr total de posturi de conducere şi numărul de posturi de conducere ocupate cu delegație, cât şi număr total de posturi de execuție şi numărul de posturi de execuție vacante.

Din analiza a rezultat ca şi deficiență existența unui număr mare de posturi de execuție vacante şi a unui număr mare de posturi de conducere deținute cu delegație. S-a constatat că datorită numărului mare de posturi vacante existente şi utilizării sistemului de delegare a personalului specializat pentru exercitarea funcțiilor de conducere, aceştia trebuie să-şi îndeplinească sarcinile de serviciu ce le revin ca urmare a delegării, dar şi sarcinile curente de serviciu, ceea ce afectează îndeplinirea atribuțiilor de serviciu şi calitatea acestora.

Această sitauție a fost creată ca urmare a inexistenței atât a unei strategii la nivelul entității publice pentru ocuparea posturilor vacante şi mai ales a celor de conducere cât şi a unor proceduri pentru suplinirea posturilor vacante şi pentru delegarea funcțiilor de conducere.

Astfel, activitatea din cadrul unor departamente nu se desfăşoară la parametrii stabiliți, constatându-se frecvent întârzieri în implementarea diferitelor aplicații, nerealizarea testărilor finale la termenele planificate, precum şi netransmiterea rapoartelor periodice de monitorizare. Din practică se demonstrează că persoanele cu delegație nu au întotdeauna acelaşi nivel de implicare pentru soluționarea problemelor care apar comparativ cu titularii posturilor.

Pentru îmbunătățirea activității desfățurate şi eliminarea defcienţelor constatate, au fost elaborate următoarele recomandări:

- Elaborarea procedurilor scrise şi formalizate pentru suplinirea posturilor vacante şi delegarea funcțiilor de conducere precum şi stabilirea responsabililor pentru elaborarea şi actualizarea acestor proceduri;

- Realizarea unui program de pregătire profesională a persoanelor delegate pe funcții de conducere la nivelul entității publice.
  identificate

2.2. Analizarea pregătirii profesionale continue a salariaților

Echipa de auditori interni a analizat realizarea pregătirii profesionale a salariaților conform atribuțiilor şi responsabilităților stabilite prin fişa postului, existența unui sistem de indicatori de performanță pentru evaluarea gradului de pregătire profesională a acestora precum şi existența planului de pregătire profesională continuă.

Din analiză s-a constatat inexistența unui sistem de pregătire profesională continuă a salariaților departamentului IT. Astfel, aproximativ 20% dintre angajații care au acces la sistemul IT implementat au fost angajați în cadrul entității publice în ultimele 3 luni şi nu au primit o pregătire profesională adecvată privind modul de utilizare a acestuia. Din totalul personalului angajat s-a constatat că doar utilizatorii inițiali au primit instruire în acest sens.

De asemenea, instrucțiunile de utilizare pentru sistemul IT nu sunt prezentate într-un format adecvat, respectiv nu există manuale de utilizare, în documentația pusă la dispoziția departamentului. Astfel, majoritatea angajaților nu au instrucțiuni clare cu privire la modul de operare a sistemului, ceea ce duce la comiterea de erori.

Această situație se datorează inexistenței unui plan de pregătire profesională continuă şi a procedurilor scrise şi formalizate cu pregătirea profesională continuă.

Deşi până în prezent nu au apărut erori cu grave implicații financiare, totuşi există pericolul apariției unor probleme/disfuncționalități datorate pregătirii profesionale a salariaților.

Pentru îmbunătățirea activității desfăşurate şi eliminarea defcienţelor constatate, au fost elaborate următoarele recomandări:

- Elaborarea unui sistem de pregătire profesională continuă a salariaților;
- Elaborarea procedurilor scrise şi formalizate pentru pregătirea profesională continuă;
- Stabilirea unor responsabilități cu elaborarea procedurilor şi actualizarea acestora;
- Coroborarea atribuțiilor şi responsabilităților stabilite prin proceduri cu fişele posturilor;
- Analiza planului de pregătire profesională continuă şi al gradului de realizare al acestuia în vederea elaborării planului pentru anul viitor;
- Stabilirea responsabilităților cu monitorizarea acestora, o atenție deosebită fiind pentru utilizatorii noi care trebuie să primească instruire specială pentru toate subsistemele IT pe care le vor utiliza, conform unui program bine stabilit.

2.3. Examinarea sistemului de gestionare a riscurilor generale

Echipa de auditori interni a verificat existența unei politici unitare privind gestionarea riscurilor, constatând inexistența unui sistem de identificare, evaluare şi management al riscurilor la nivelul entității publice.

Din analiză a reieşit că nu există preocupări pentru gestionarea riscurilor din cadrul entității şi nu a fost ținut Registrul riscurilor cuprinzând riscurile potențiale şi istoricul acestora, cu efectele şi consecințele lor, precum şi activitățile de control intern asociate pentru limitarea riscurilor. De asemenea, s-a evidențiat neacordarea atenției cuvenite managementului riscurilor de către personalul entității publice, fapt ce ar putea avea drept consecință producerea unor evenimente nedorite pentru care entitatea publică nu este pregătită să acționeze. Mai mult, există pericolul de a nu fi identificate riscuri majore şi de a nu fi asociate controale interne adecvate pentru reducerea efectului riscurilor la un nivel acceptabil pentru entitatea publică.

Pentru îmbunătățirea activității desfățurate şi eliminarea defcienţelor constatate, au fost elaborate următoarele recomandări:

- Stabilirea unei strategii de gestionare a riscurilor la nivelul entității publice;
- Stabilirea responsabililor pentru elaborarea şi actualizarea sistematică a procedurilor privind întocmirea Registrului riscurilor;
- Coroborarea atribuțiilor şi responsabilităților din proceduri cu cele din fişa postului referitor la gestionarea riscurilor;
- Organizarea şi ținerea la zi a Registrului riscurilor cuprinzând măsurile de control intern care sunt luate pentru limitarea acestora;
- Monitorizarea sistematică, la cererea managerului responsabil cu probleme administrative, a modului de respectare în activitatea zilnică a procedurilor scrise şi formalizate menite să asigure gestionare a riscului;
- Instruirea personalului pentru complectarea Registrului Riscurilor de către responsabilul cu ținerea acestuia;
- Informarea echipei de auditori în privința stadiului elaborării, însuşirii şi monitorizării riscurilor.

3. Implementarea sistemului IT

3.1. Gradul de realizare al subsistemelor IT stabilite prin plan

Echipa de auditori a constatat că subsistemele IT nu au fost realizate la termenele stabilite.

Din analiza modului de implementare a subsistemelor IT, potrivit planului anual întocmit şi aprobat, s-a constatat că termenele stabilite nu sunt respectate, iar departamentele ce ar trebui să utilizeze deja noile aplicații IT întâmpină deficiențe în transmiterea datelor în format electronic celorlalte departamente care beneficiază deja de programe performante. Persoane implicate inițial în aceste activități au primit alte responsabilități şi nu au fost desemnate alți salariați pentru înlocuirea acestora, iar inexistența unei proceduri de monitorizare a implementării subsistemelor IT face dificilă monitorizarea activităților de către managementul general;

Deficienâele constatate au dus la nerealizarea subsistemelor IT la termenele stabilite, ceea ce îngreuiază realizarea sarcinilor de serviciu în domenii cheie de activitate ale entității publice, existând posibilitatea afectării gradului de realizare a obiectivelor entității publice.

Pentru îmbunătățirea activității desfățurate şi eliminarea defcienţelor constatate, au fost elaborate următoarele recomandări:

- Elaborarea procedurilor scrise şi formalizate pentru monitorizarea implementării subsistemelor IT
- Desemnarea responsabilității cu realizarea şi actualizarea procedurilor;
- Efectuarea unor inspecții pentru stabilirea stadiului în care se află implementarea subsistemelor IT specifice pe departamente;

3.2. Verificați existența controalelor generale de sistem la nivelul subsistemelor IT

Echipa de auditori a analizat:

- Controlul datelor introduse în aplicații,
- 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 complecte,

- Validarea datelor transferate din alte aplicații,
- Controalelor care verifică înregistrările duble;
- Autorizarea electronică şi/sau manuală a tranzacțiilor
- Efectuarea tranzacțiilor numai de la computere definite în prealabil
- Păstrarea integrală a înregistrărilor astfel încât să se poată urmări tranzacțiile efectuate din faza de inițiere până la finalizarea lor;
- Înțelegerea controalelor implementate de către utilizatori

Din analiză s-a constatat inexistența controalelor generale implementate la nivelul subsistemelor IT.

Din evaluare, a reieşit că nu există un sistem de controale generale care vor fi avute în vedere în procesul de proiectare, realizare, testare şi implementare al tuturor subsistemelor IT ce rulează pe echipamentele entității publice, astfel:

- Controlul datelor introduse în aplicații;
- 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 complecte;
- Validarea datelor transferate din alte aplicații;
- Efectuarea tranzacțiilor numai de la computere definite în prealabil.

Practic, deşi sunt implementate anumite controale generale proprii fiecărui subsistem, nu există un set unitar de controale generale implementat la nivelul programelor şi aplicațiilor ce rulează în cadrul sistemului IT. În fapt inexistența procedurilor scrise şi formalizate privind implementarea unui set unitar de controalele generale încă din faza de proiecare a programelor şi/sau aplicațiilor lasă la latitudinea programatorilor implementare controalelor pe care aceştia le consideră necesare.

Inexistența 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.

Pentru îmbunătățirea activității desfăşurate şi eliminarea defcienţelor constatate, au fost elaborate următoarele recomandări:

- Realizarea unui sistem de implementare al controalelor generale;
- Implementarea controalelor generale la nivelul tuturor subsistemelor IT pentru asigurarea unui grad de siguranță sporit al integrității datelor electronice;
- Stabilirea unui responsabil cu elaborarea sistemului de controale generale şi cu actualizarea periodică a acestuia;
- Coroborarea atribuțiilor stabilite cu fişele postului;
- Informarea echipei de auditori cu privire la controalele generale implementate.

3.3. Situația licențelor pentru programele de calculator

Echipa de auditori a analizat situația licențelor deținute atât pentru sistemul de operare Windows cât şi pentru pachetul de programe Microsoft Office. De asemenea, s-a urmărit identificarea eventualele limitări bugetare în privința achiziționării licențelor, evaluarea eventualelor disfuncționalități apărute în procesul de achiziționare a licențelor, precum şi implementarea controalelor de sistem menite să alerteze administratorul în cazul utilizării de soft-uri pentru care nu s-au achiziționat licențe.

S-a constatat utilizarea în cadrul entității publice a unor programe software fără licență. Din analiză a reieşit că în cadrul unor departamente se folosesc programe aferente pachetului

Microsoft Office fără ca pentru acestea entitatea publică să fi achiziționat licențe. De asemenea, la nivelul sistemului IT al entității publice s-a constatat inexistența controalelor de sistem menite să alerteze administratorul în cazul utilizării de soft-uri pentru care nu s-au achiziționat licențe.

Entitatea publică a achiziționat licențe pentru pachetul de programe Lotus. Salariații entității publice au observat că deşi programele Lotus le permit realizarea sarcinilor de serviciu, totuşi programele cuprinse în pachetul Microsoft Office sunt mai fiabile, mai flexibile, şi permit realizarea unui număr mai mare de operațiuni. De asemenea, această situație a fost generată şi de primirea de la alte entități publice de fişiere electronice create cu programele din pachetul Microsoft Office.

Soft-urile nelicențiate instalate de utilizatori pot conține 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. Perpetuarea situației prezentate face entitatea publică pasibilă de amenzi pentru utilizarea unor programe fără licentă. Pentru îmbunătățirea activității desfățurate şi eliminarea defcienţelor constatate, au fost elaborate următoarele recomandări:

- Elaborarea procedurilor pentru elaborarea programelor informatice pentru alertarea administratorilor de sistem;
- Stabilirea unui responsabil cu elaborarea procedurilor şi actualizarea lor;
- Coroborarea atribuțiilor din proceduri cu fişele posturilor;
- Inventarierea tuturor stațiilor de lucru pentru a stabili situația reală privind utilizarea programelor fără licență
- Dezinstalarea tuturor programelor din pachetul Microsoft Office instalate ilegal;
- Elaborarea unui angajament prin care toți salariații entității publice să-şi asume întreaga responsabilitate asupra urmărilor utilizării de soft-uri pirat;
- Realizarea unei analize complexe cost/calitate în urma căreia managementul entității publice să decidă dacă este necesară achiziționarea unui număr adecvat de licențe Microsoft Office.

4. Lansarea procedurii de licitatie deschisa pentru atribuirea contractului de achizitie publica

4.1. Evaluarea controalelor fizice în domeniul IT

Pentru protecția echipamentelor IT precum şi a datelor în format electronic prelucrate, transferate şi/sau stocate la nivelul acestor echipamente în cadrul entității publice au fost implementate controale fizice, 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 condiționat;
- uşi neinflamabile echipate cu încuietori adecvate.

Practic s-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 precum şi nici senzori de mişcare la nivelul Departamentul Resurse Umane. Acastă situație a fost remediată în timpul misiunii de audit.

4.2. Siguranța accesului la rețea şi a comunicării datelor în rețea

În urma misiunii de audit efectuate, s-a constatat că majoritatea salariaților din cadrul entității publice, prin natura sarcinilor de serviciu, trebuie să acceseze mai multe subsisteme IT, fapt pentru 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.

Datorită numărului mare de parole ce trebuiesc utilizate de salariați, deseori aceştia notează parolele pe documente lăsate pe birou. Astfel salariații 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.

Practic, sistemul de parole nu mai are funcții principale de restricționare a accesului persoanelor nepotrivite ci îngreunează funcționarea sistemului, iar în situația apariției unor incidente nu se pot stabili responsabilitățile adecvate.

Pentru îmbunătățirea activității desfățurate şi eliminarea defcienţelor constatate, au fost elaborate următoarele recomandări:

- Realizarea unui proces de reenginering la nivelul sistemului IT din cadrul entității publice, astfel încât salariații să poată accesa subsistemele IT de care au nevoie utilizând un singur nume de utilizator şi o singură parolă;
- Stabilirea unui responsabil pentru derularea acestui proces reenginering al sistemului IT
- Implementarea unui sistem de raportare potrivit căruia responsabilul desemnat să întocmească periodic rapoarte de activitate către managementul general al entității publice prin care să specifice acțiunile întreprinse;
- Instruirea adecvată a salariaților ce utilizează sistemul IT;
- Informarea echipei de auditori în privința stadiului elaborării, însuşirii şi monitorizării riscurilor.

4.3. Programele anti-virus

Echipa de auditori interni a verificat:

- instalarea unui program anti-virus adecvat necesităților utilizatorilor stațiilor de lucru;
- dacă programul anti-virus verifică stația de lucru la pornire;
- dacă programul anti-virus monitorizează toate programele şi aplicațiile active, mesajele primite şi verifică automat actualizările la intervale regulate (zilnic);
- dacă programul anti-virus să se actualizează în rețea, astfel încât să protejeze eficient datele electronice împotriva viruşilor nou-apăruți.

De asemenea a fost analizat modul de monitorizare sistematică a funcționalității programelor anti-virus.

S-a constatat neaplicarea în mod unitar a politicii de securitate IT, fapt ce a condus la infectarea cu viruşi a unor stații de lucru din sistemul IT al entității publice. O politică adecvată de securitate IT trebuie să prevadă instalarea unui program anti-virus pe toate stațiile de lucru, ca acesta să verifice stația de lucru la pornire, să monitorizeze toate programele de aplicații active, mesajele primite şi să verifice automat actualizările la intervale regulate (poate chiar zilnic).

În urma verificării la fața locului a unui eşantion din stațiile de lucru ce funcâionează în sistemul IT al entității publice, s-au constatat următoarele deficiențe:

- În 5 departamente din cadrul entității publice configurația programului anti-virus a fost modificată pentru a întrerupe monitorizarea întregii activități 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 performanței sistemului;
- Urmare acestei constatări, am verificat respectivele stații de lucru pentru a descoperi prezența viruşilor şi am descoperit că toate erau infectate cu viruşi.

Considerăm că aspectele negative constatate se datorează lipsei procedurilor formalizate care să prevadă acțiunile ce trebuiesc întreprinse în cazul modificării configurației programului anti-virus.

Practic, prezența viruşilor şi a altor programe dăunătoare pe stațiile de lucru afectează în mod negativ activitatea utilizatorilor din cadrul departamentelor. De asemenea, existența viruşilor ridică numeroase semne de întrebare în privința exactității datelor stocate în sistemul IT.

Pentru îmbunătățirea activității desfăşurate şi eliminarea defcienţelor constatate, au fost elaborate următoarele recomandări:

- Elaborarea procedurilor formalizate care să prevadă acțiunile ce trebuiesc întreprinse în cazul modificării configurației programului anti-virus;
- Stabilirea unui responsabil pentru elaborarea şi actualizarea procedurilor;
- Coroborarea atribuțiilor şi responsabilităților stabilite prin fişele posturilor cu sarcinile stabilite prin proceduri;
- Monitorizarea aplicării în mod unitar a politicii de securitate IT;
- Constituirea unor echipe pentru efectuarea de verificări anti-virus la nivelul tuturor stațiilor de lucru din cadrul entității publice;

4.4. Recuperarea datelor în caz de dezastru

Echipa de auditori a constatat că deşi există un Plan de recuperare în caz de dezastru aprobat, acesta nu a fost niciodată nici testat, nici comunicat membrilor cheie ai entității publice, cărora li se va cere să pună planul în aplicare în caz de dezastru. Astfel, este posibil ca datele de rezervă să nu fie nici disponibile, nici utilizabile conform planificării, în cazul în care ar fi necesare pentru a realiza o recuperare.

Din analiză, a rezultat că deşi au fost amenajate facilități în aşteptare de recuperare a datelor în caz de dezastru, acestea nu au fost testate pentru a se garanta că sunt eficiente, funcționabile şi actualizate pentru a face față cerințelor impuse de schimbările tehnologice implementate.

Practic, inexistența unei proceduri pentru testarea Planului de recuperare a datelor în caz de dezastru face posibilă neaplicarea în mod unitar a procedurilor privind recuperarea datelor în caz de dezastru. Din aceste considerente în situația producerii unui dezastru activitățile stabilite prin plan se pot dovedi insuficiente pentru atingerea obiectivelor stabilite.

Pentru îmbunătățirea activității desfăşurate şi eliminarea defcienţelor constatate, au fost elaborate următoarele recomandări:

- Alocarea de roluri şi responsabilități, iar Planul a datelor în caz de dezastru trebuie comunicat tuturor persoanelor responsabile;
- Testarea şi apoi actualizarea planului astfel încât să faciliteze recuperarea datelor cu succes.
- Back-up-urile trebuie stocate în siguranță în afara sediului.
- Verificarea tuturor exemplarele de rezervă înainte de fi depozitate;

- Monitorizarea sistematică de către management a modului în care sunt aplicate procedurilor privind recuperarea datelor în caz de dezastru.

III. CONCLUZII

Prezentul *proiect de Raport de audit intern* a fost întocmit în baza Listei centralizatoare a obiectelor auditabile, a Programului de audit şi a Programuui de intervenţie la faţa locului, a constatărilor efectuate, în timpul colectării şi prelucrării informaţiilor, şi în timpul muncii pe teren. Toate constatările au la baza probe de audit obtinute pe baza testelor efectuate consemnate in documentele de lucru (liste de control, foi de lucru, interviuri, note de relatii) intocmite de auditorii interni si insusite de factorii de management ai entitatii.

Evaluarea are la baza discutiile care au avut loc, cu privire la recomandarile auditorilor interni, in sedinţa de inchidere a misiunii, apreciate de catre participanti, ca fiind realiste si fezabile.

De asemenea, consideram ca rezultatele evaluarii auditorilor interni privind **Activitatea IT** se inscriu in parametri normali pentru aceasta perioada de implementare a functiei de tehnologia informaţiei în entităţile publice.

În consecinta, apreciem ca prin implementarea recomandarilor echipei de audit intern acivitatea IT va cunoaste o ameliorare semnificativa.

Structura auditată are obligaţia să întocmească *Programul de acţiune în vederea implementării recomandărilor* şi să raporteze echipei de auditori interni, periodic, stadiul de implementare al acestora.

Data: 15.03.2006

Auditori interni,

Popescu Sorin
Radu George

Supervizat,

Dumitru Daniel

S I N T E Z A

RAPORTULUI DE AUDIT INTERN

I. INTRODUCERE

Misiunea de audit intern privind *Activitatea IT* din cadrul entitatii publice s-a desfasurat conform prevederilor *Legii nr. 672/2002 privind auditul public intern, Normelor generale privind exercitarea activitatii de audit public intern, aprobate prin OMFP nr. 38/2003* si a *Normelor specifice aprobate de conducerea entitatii.* Misiunea a fost cuprinsa in *Planul de audit intern pe anul 2006*, si a fost realizata de auditorii interni: Popescu Sorin, auditor superior si Radu George, auditor superior.

II. CONCLUZII

Echipa de auditori interni in baza *Programului de audit intern*, a testarilor si analizei efectuate evalueaza *Activitatea de achizitii publice* din cadrul entitatii, dupa cum urmeaza:

Nr. crt.	OBIECTIVUL	APRECIERE		
		FUNCTIONAL	DE IMBUNATATIT	CRITIC
1.	*PLAN STRATEGIC*	X		
2.	*ORGANIZAREA ŞI FUNCŢIONAREA DEPARTAMENTULUI IT*		X	
3.	*IMPLEMENTAREA SISTEMULUI IT*		X	
4.	*SECURITATEA IT*		X	

III. CONSTATARI SI RECOMANDARI

Principalele constatari si recomandari rezultate din realizarea misiunii de audit sunt:

- CONSTATARE nr. 1:

  Din analiză s-a constatat c 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 au fost solicitate să-şi exprime nevoile pentru realizarea subsistemelor IT specifice activităţii lor, dar care nu s-au realizat conform planificării. *(FIAP nr. 1.1.)*

RECOMANDARE nr. 1:

- Inventarierea stadiului implementării subsistemelor IT la nivelul departamentelor entității publice şi stabilirea necesităților IT care trebuiesc incluse în strategia IT.

- CONSTATARE nr. 2:

Din analiză s-a constatat că nu există preocupări pentru gestionarea riscurilor din cadrul entității şi nu a fost ținut Registrul riscurilor cuprinzând riscurile potențiale şi istoricul acestora, cu efectele şi consecințele lor, precum şi activitățile de control intern asociate pentru limitarea riscurilor.

RECOMANDARE nr. 2:

- Stabilirea unei strategii de gestionare a riscurilor la nivelul entității publice;
- Organizarea şi ținerea la zi a Registrului riscurilor cuprinzând măsurile de control intern care sunt luate pentru limitarea acestora;

- CONSTATARE nr. 3:

Din analiză s-a constatat că în cadrul unor departamente se folosesc programe aferente pachetului Microsoft Office fără ca pentru acestea entitatea publică să fi achiziționat licențe.

RECOMANDARE nr. 3:

- Inventarierea tuturor stațiilor de lucru pentru a stabili situația reală privind utilizarea programelor fără licență
- Dezinstalarea tuturor programelor din pachetul Microsoft Office instalate ilegal;
- Elaborarea unui angajament prin care toți salariații entității publice să-şi asume întreaga responsabilitate asupra urmărilor utilizării de soft-uri pirat;
- Realizarea unei analize complexe cost/calitate în urma căreia managementul entității publice să decidă dacă este necesară achiziționarea unui număr adecvat de licențe Microsoft Office.

- CONSTATARE nr. 4:

O politică adecvată de securitate IT trebuie să prevadă instalarea unui program anti-virus pe toate stațiile de lucru, ca acesta să verifice stația de lucru la pornire, să monitorizeze toate programele de aplicații active, mesajele primite şi să verifice automat actualizările la intervale regulate (poate chiar zilnic).

Echipa de auditori a verificat 15 de stații de lucru, selectate în mod aleator, din cadrul tuturor departamentelor şi a constatat următoarele:

- În 5 departamente din cadrul entității publice configurația programului anti-virus a fost modificată pentru a întrerupe monitorizarea întregii activități 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 performanței sistemului;
- Urmare acestei constatări, am verificat respectivele stații de lucru pentru a descoperi prezența viruşilor şi am descoperit că toate erau infectate cu viruşi.

RECOMANDARE nr. 4:

- Monitorizarea aplicării în mod unitar a politicii de securitate IT;
- Constituirea unor echipe pentru efectuarea de verificări anti-virus la nivelul tuturor stațiilor de lucru din cadrul entității publice;

- CONSTATARE nr. 5:

Echipa de auditori a constatat că deşi există un Plan de recuperare în caz de dezastru aprobat, acesta nu a fost niciodată nici testat, nici comunicat membrilor cheie ai entității publice, cărora li se va cere să pună planul în aplicare în caz de dezastru. Este posibil ca datele de rezervă să nu fie nici disponibile, nici utilizabile conform planificării, în cazul în care ar fi necesare pentru a realiza o recuperare.

Din analiză, a rezultat că deşi au fost amenajate facilități în aşteptare de recuperare a datelor în caz de dezastru, acestea nu au fost testate pentru a se garanta că sunt eficiente, funcționabile şi actualizate pentru a face față cerințelor impuse de schimbările tehnologice implementate.

RECOMANDARE nr. 5:

- Testarea şi apoi actualizarea planului astfel încât să faciliteze recuperarea datelor cu succes.

- ***Recomandare generala***

Elaborarea procedurilor, scrise si formalizate, pentru toate activitatile care se desfasoara in cadrul *Departamentului IT*. De asemenea, pentru activitatile de elaborare a procedurilor sa se stabileasca responsabilii cu realizarea, monitorizarea implementarii lor si actualizarea periodica.

Precizam ca in *Sinteza* au fost prezentate FIAP-urile reprezentative, in numar de cinci, dar *Raportul de audit intern* cuprinde 10 FIAP-uri.

Data: 15.03.2006

Auditori interni,
Popescu Sorin
Radu George

Supervizat,
Dumitru Daniel

ENTITATEA PUBLICA
Serviciul Audit Intern

PLANUL DE ACȚIUNE
ŞI
CALENDARUL IMPLEMENTĂRII RECOMANDĂRILOR

Nr. ob.	Recomandarea	Plan de acțiune	Calendarul implementării	Responsabil cu implementarea
1.	Elaborarea unei proceduri scrise şi formalizate pentru actualizarea strategia IT la nivelul entității publice pentru departamentele nou-create	Elaborarea procedurii pentru actualizarea strategia IT pentru departamentele nou-create	31.05.2006	Eleodor Darius, Serviciul analiza, proiectare şi programare
	Stabilirea responsabilității pentru actualizarea strategiei IT	Desemnarea persoanelor responsabile cu actualizarea strategiei IT	18.04.2006	Pătrulescu Ştefan, director Direcția Tehnologia Informației
	Preocupare pentru angajarea personalului de specialitate şi ocuparea posturilor vacante	Notificarea Departamentului Resurse Umane pentru organizarea concursurilor în vederea ocupării posturilor vacante	18.04.2006	Pătrulescu Ştefan, director Direcția Tehnologia Informației
	Coroborarea atribuțiilor prezentate prin proceduri cu cele stabilite prin fişele posturilor	Analiza procedurilor şi a fişelor de post şi actualizarea fişelor	28.07.2006	Păun Elena, Serviciul sinteză dezvoltare
	Inventarierea stadiului implementării subsistemelor IT la nivelul departamentelor entității publice şi stabilirea necesităților IT care trebuiesc incluse în strategia IT	Realizarea inventarierii stadiului implementării subsistemelor IT şi formularea propunerilor de modificare a strategiei IT	31.05.2006	Păun Elena, Serviciul sinteză dezvoltare
2.	Elaborarea procedurilor scrise şi formalizate pentru suplinirea posturilor vacante şi delegarea funcțiilor de	Elaborarea procedurilor şi stabilirea persoanelor responsabile cu actualizarea	01.06.2006	Păun Elena, Serviciul sinteză dezvoltare

	conducere precum şi stabilirea responsabililor pentru elaborarea şi actualizarea acestor proceduri	acestora		
	Realizarea unui program de pregătire profesională a persoanelor delegate pe funcţii de conducere la nivelul entităţii publice	Realizarea programului	02.05.2006	Pătrulescu Ştefan, director Direcţia Tehnologia Informaţiei
	Realizarea unei strategii de ocupare a posturilor de conducere deţinute cu delegaţie şi a celor de execuţie vacante	Elaborarea strategiei	12.05.2006	Păun Elena, Serviciul sinteză dezvoltare
	Elaborarea unui sistem de pregătire profesională continuă a salariaţilor şi numirea unui responsabil cu realizarea acestuia	Analizarea necesităţilor de pregătire profesională	19.05.2006	Păun Elena, Serviciul sinteză dezvoltare
	Elaborarea procedurilor scrise şi formalizate pentru pregătirea profesională continuă	Elaborarea procedurilor	19.05.2006	Păun Elena, Serviciul sinteză dezvoltare
	Stabilirea unor responsabilităţi cu elaborarea procedurilor şi actualizarea acestora	Stabilirea responsabilităţilor	04.05.2006	Pătrulescu Ştefan, director Direcţia Tehnologia Informaţiei
	Coroborarea atribuţiilor şi responsabilităţilor stabilite prin proceduri cu fişele posturilor	Analiza procedurilor şi a fişelor de post şi actualizarea fişelor	28.07.2006	Păun Elena, Serviciul sinteză dezvoltare
	Analiza planului de pregătire profesională continuă şi al gradului de realizare al acestuia în vederea elaborării planului pentru anul viitor	Elaborarea planului de pregătire profesională continuă	11.06.2006	Pătrulescu Ştefan, director Direcţia Tehnologia Informaţiei
	Stabilirea responsabilităţilor cu monitorizarea pregătirii profesionale, o atenţie deosebită fiind pentru utilizatorii noi care trebuie să primească instruire specială pentru toate subsistemele IT pe care le vor utiliza, conform unui program bine stabilit	Stabilirea persoanelor responsabile cu monitorizarea	18.04.2006	Pătrulescu Ştefan, director Direcţia Tehnologia Informaţiei

	Stabilirea unei strategii de gestionare a riscurilor la nivelul entității publice	Elaborarea strategiei	14.05.2006	Pătrulescu Ştefan, director Direcţia Tehnologia Informaţiei
	Stabilirea responsabililor pentru elaborarea şi actualizarea sistematică a procedurilor privind întocmirea Registrului riscurilor	Stabilirea responsabililor	18.04.2006	Pătrulescu Ştefan, director Direcţia Tehnologia Informaţiei
	Coroborarea atribuţiilor şi responsabilităţilor din proceduri cu cele din fişa postului referitor la gestionarea riscurilor	Analiza procedurilor şi a fişelor de post şi actualizarea fişelor	28.07.2006	Păun Elena, Serviciul sinteză dezvoltare
	Organizarea şi ţinerea la zi a Registrului riscurilor cuprinzând măsurile de control intern care sunt luate pentru limitarea acestora	Elaborarea Registrului Riscurilor	10.05.2006	Teodorescu Rodica, Serviciul exploatarea echipamentelor
	Monitorizarea sistematică, la cererea managerului responsabil cu probleme administrative, a modului de respectare în activitatea zilnică a procedurilor scrise şi formalizate menite să asigure gestionare a riscului	Realizarea monitorizării	Trimestrial, la solicitarea managerului	Teodorescu Rodica, Serviciul exploatarea echipamentelor
	Instruirea personalului pentru complectarea Registrului Riscurilor de către responsabilul cu ţinerea acestuia	Realizarea instruirii	15.05.2006	Teodorescu Rodica, Serviciul exploatarea echipamentelor
	Informarea echipei de auditori în privinţa stadiului elaborării, însuşirii şi monitorizării riscurilor	Notificarea periodică a echipei de auditori asupra stadiului implementării recomandărilor	lunar	Pătrulescu Ştefan, director Direcţia Tehnologia Informaţiei
3.	Elaborarea procedurilor scrise şi formalizate pentru monitorizarea implementării subsistemelor IT	Elaborarea procedurilor	31.05.2006	Eleodor Darius, Serviciul analiza, proiectare şi programare
	Efectuarea unor inspecţii pentru stabilirea stadiului în care se află implementarea subsistemelor IT specifice pe departamente.	Efectuarea inspecţiilor	01.06.2006	Badea Ştefan, Serviciul asistenţă tehnică

	Realizarea unui sistem de implementare al controalelor generale	Elaborarea sistemului de controale generale	02.05.2006	Eleodor Darius, Serviciul analiza, proiectare şi programare
	Implementarea controalelor generale la nivelul tuturor subsistemelor IT pentru asigurarea unui grad de siguranță sporit al integrității datelor electronice;	Implementarea sistemului de controale generale	31.05.2006	Eleodor Darius, Serviciul analiza, proiectare şi programare
	Stabilirea unui responsabil cu elaborarea sistemului de controale generale şi cu actualizarea periodică a acestuia	Stabilirea responsabilului	20.04.2006	Eleodor Darius, Serviciul analiza, proiectare şi programare
	Coroborarea atribuțiilor stabilite cu fişele postului	Analiza şi actualizarea fişelor de post	15.05.2006	Eleodor Darius, Serviciul analiza, proiectare şi programare
	Informarea echipei de auditori cu privire la controalele generale implementate	Notificarea periodică a echipei de auditori asupra stadiului implementării recomandărilor	lunar	Pătrulescu Ştefan, director Direcţia Tehnologia Informației
	Elaborarea procedurilor pentru elaborarea programelor informatice pentru alertarea administratorilor de sistem	Elaborarea procedurilor	03.05.2006	Păun Elena, Serviciul sinteză dezvoltare
	Stabilirea unui responsabil cu elaborarea procedurilor şi actualizarea lor	Stabilirea responsabilului	20.04.2006	Păun Elena, Serviciul sinteză dezvoltare
	Coroborarea atribuțiilor din proceduri cu fişele posturilor	Analiza şi actualizarea fişelor de post	25.04.2006	Păun Elena, Serviciul sinteză dezvoltare
	Inventarierea tuturor stațiilor de lucru pentru a stabili situația reală privind utilizarea programelor fără licență	Efectuarea inventarierii	02.05.2006	Teodorescu Rodica, Serviciul exploatarea echipamentelor
	Dezinstalarea tuturor programelor din pachetul Microsoft Office instalate ilegal	Dezinstalarea programelor din pachetul Microsoft Office instalate ilegal	02.05.2006	Teodorescu Rodica, Serviciul exploatarea echipamentelor
	Elaborarea unui angajament prin care toți salariații entității publice să-şi asume întreaga responsabilitate asupra	Elaborarea angajamentului	20.04.2006	Pătrulescu Ştefan, director Direcţia Tehnologia Informației

	urmărilor utilizării de soft-uri pirat			
	Realizarea unei analize complexe cost/calitate în urma căreia managementul entității publice să decidă dacă este necesară achiziționarea unui număr adecvat de licențe Microsoft Office	Realizarea analizei cost/calitate şi comunicarea rezultatelor managementului entității publice	15.05.2006	Pătrulescu Ştefan, director Direcția Tehnologia Informației
4.	Realizarea unui proces de reenginering la nivelul sistemului IT din cadrul entității publice, astfel încât salariații 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 sistemului IT	08.05.2006	Badea Ştefan, Serviciul asistență tehnică
	Stabilirea unui responsabil pentru derularea acestui proces reenginering al sistemului IT	Stabilirea responsabilului	20.04.2006	Badea Ştefan, Serviciul asistență tehnică
	Implementarea unui sistem de raportare potrivit căruia responsabilul desemnat să întocmească periodic rapoarte de activitate către managementul general al entității publice prin care să specifice acțiunile întreprinse pentru facilitarea accesului la subsistemele IT	Implementarea sistemului de raportare	27.04.2006	Pătrulescu Ştefan, director Direcția Tehnologia Informației
	Instruirea adecvată a salariaților ce utilizează sistemul IT	Realizarea instruirii utilizatorilor	30.11.2006	Pătrulescu Ştefan, director Direcția Tehnologia Informației
	Elaborarea procedurilor formalizate care să prevadă acțiunile ce trebuiesc întreprinse în cazul modificării configurației programului antivirus	Elaborarea procedurilor	02.05.2006	Teodorescu Rodica, Serviciul exploatarea echipamentelor
	Stabilirea unui responsabil pentru elaborarea şi actualizarea procedurilor	Stabilirea responsabilului	20.04.2006	Teodorescu Rodica, Serviciul exploatarea echipamentelor
	Coroborarea atribuțiilor şi	Analiza şi actualizarea fişelor	25.04.2006	Teodorescu Rodica,

	responsabilităţilor stabilite prin fişele posturilor cu sarcinile stabilite prin proceduri	de post		Serviciul exploatarea echipamentelor
	Monitorizarea aplicării în mod unitar a politicii de securitate IT	Efectuarea monitorizării	30.11.2006	Teodorescu Rodica, Serviciul exploatarea echipamentelor
	Constituirea unor echipe pentru efectuarea de verificări anti-virus la nivelul tuturor staţiilor de lucru din cadrul entităţii publice	Stabilirea echipelor	25.04.2006	Teodorescu Rodica, Serviciul exploatarea echipamentelor
	Alocarea de roluri şi responsabilităţi, şi comunicarea Planului de recuperare a datelor în caz de dezastru tuturor persoanelor responsabile	Alocarea rolurilor şi responsabilităţilor şi comunicarea planului	15.05.2006	Voiculescu Alin, Serviciul de tehnoredactare şi dezvoltare aplicaţii multimedia
	Testarea şi apoi actualizarea planului astfel încât să faciliteze recuperarea datelor cu succes	Testarea şi actualizarea planului	01.06.2006	Voiculescu Alin, Serviciul de tehnoredactare şi dezvoltare aplicaţii multimedia
	Back-up-urile trebuie stocate în siguranţă în afara sediului	Alegerea unei locaţii pentru stocarea back-up-urilor	28.04.2006	Pătrulescu Ştefan, director Direcţia Tehnologia Informaţiei
	Verificarea tuturor exemplarelor de rezervă înainte de fi depozitate	Verificarea tuturor exemplarelor de rezervă	permanent	Voiculescu Alin, Serviciul de tehnoredactare şi dezvoltare aplicaţii multimedia
	Monitorizarea sistematică de către management a modului în care sunt aplicate procedurilor privind recuperarea datelor în caz de dezastru	Efecturea monitorizării în mod sistematic	trimestrial	Pătrulescu Ştefan, director Direcţia Tehnologia Informaţiei

Director Direcţia Tehnologia Informaţiei,
Pătrulescu Ştefan