ICS 35.040

SRISO/CEI27001

STANDARD ROMAN

Septembrie 2006

Tehnologia informației
Tehnici de securitate
Sisteme de management ai securității informației
Cerințe

Information technology. Security techniques. Information security management systems. Requirements

Technologies de ('information. Techniques de securite. Systemes de gestion de securite de l'information. Exigences

APROBARE — Aprobat Directorul General al ASRO la 29 septembrie 2006
Standardul internațional ISO/CEI 27001:2005 are statutul unui standard român

CORESPONDENTĂ — Acest standard este identic cu standardul internațional ISO/CEI 27001:2005

This standard is identical with the International Standard ISO/CEI 27001:2005

La presente norme est identique â la Norme internationale ISO/CEI 27001:2005

Preambul național

Acest standard reprezintă versiunea română a textului în limba engleză a standardului internațional ISO/CEI 27001:2005.

Acest standard a fost elaborat pentru a furniza un model pentru stabilirea, implementarea, funcționarea, monitorizarea, revizuirea, întreținerea și îmbunătățirea unui Sistem de Management pentru Securitatea Informației (SMSI).

Acest standard se aplică în toate tipurile de organizații (de exemplu: societăți comerciale, agenții guvernamentale, organizații non-profit). El specifică cerințele pentru implementarea măsurilor de securitate adaptate la nevoile individuale ale organizației sau ale unor părți din aceasta.

Sistemul de management al securității informației este conceput în așa fel încât să asigure selectarea adecvată și proporțională a măsurilor de securitate care protejează resursele informatice și să asigure încrederea părților implicate.

La data adoptării acestui standard, standardul de referință menționat în text, ISO/CEI 17799:2005, nu este adoptat ca standard român.

Cuprins

Preambul

ISO (Organizaţia Internaţională de Standardizare) şi CEI (Comisia Electrotehnică Internaţională) formează sistemul internaţional specializat pentru standardizare. Organismele naţionale care sunt membre ale ISO sau CEI participă la dezvoltarea standardelor internaţionale prin comitetele tehnice stabilite de respectiva organizaţie pe domenii specifice de activitate tehnică. Comitetele tehnice ISO şi CEI colaborează în domenii de interes reciproc. La această acţiune participă şi alte organizaţii internaţionale, guvernamentale şi neguvernamentale, în colaborare cu ISO şi CEI. în domeniul tehnologiei informaţiei, ISO şi CEI au stabilit un comitet tehnic comun ISO/IEC JTC 1.

Standardele internaţionale sunt elaborate în conformitate cu reglementările cuprinse în Directivele ISO/CEI, Partea 2.

Principala sarcina a comitetului tehnic comun este pregătirea standardelor internaţionale. Proiectele standardelor internaţionale adoptate de comitetul tehnic comun sunt transmise către organismele naţionale în vederea votării lor. Publicarea ca standard internaţional necesită aprobarea a cel puţin 75% din organismele naţionale participante la vot.

Se atrage atenţia asupra posibilităţii ca unele dintre elementele acestui document să cadă sub incidenţa unor drepturi de brevet. ISO şi CEI nu sunt responsabile de identificarea oricăror astfel de drepturi de brevet.

Standardul internaţional ISO/IEC 27001 a fost elaborat de Comitetul tehnic comun ISO/CEI JTC 1, *Information technology,* Subcomitetul SC 27, *IT Security techniques.*

0 Introducere

0.1 Generalităţi

Acest standard internaţional a fost elaborat pentru a furniza un model pentru stabilirea, implementarea, funcţionarea, monitorizarea, revizuirea, întreţinerea şi îmbunătăţirea unui Sistem de Management pentru Securitatea Informaţiei (SMSI). Adoptarea SMSI trebuie să fie o decizie strategica pentru o organizaţie. Proiectarea şi implementarea unui SMSI intr-o organizaţie este influenţată de nevoile şi obiectivele acesteia, cerinţele de securitate, procesele existente şi mărimea şi structura organizaţiei. Acestea, împreună cu sistemele lor de suport se pot schimba de-a lungul timpului. Este de aşteptat ca implementarea SMSI să fie dimensionată în conformitate cu nevoile organizaţiei, de exemplu o situaţie simplă necesitând o soluţie simplă SMSI.

Acest standard internaţional poate fi folosit pentru evaluarea conformităţii de către părţile interesate, atât din interiorul organizaţiei, cât şi din exteriorul acesteia.

0.2 Abordare bazată pe proces

Acest standard internaţional adoptă o abordare bazată pe proces pentru stabilirea, implementarea, funcţionarea, monitorizarea, evaluarea, întreţinerea şi îmbunătăţirea SMSI al unei organizaţii.

Pentru ca o organizaţie să funcţioneze în mod eficient ea trebuie să identifice şi să conducă numeroase activităţi. Orice activitate care foloseşte resurse şi este condusă pentru a permite transformarea intrărilor în ieşiri, poate fi considerată un proces. Adesea o ieşire dintr-un proces reprezintă în mod direct intrarea procesului următor.

Aplicarea unui sistem de procese în cadrul unei organizaţii, împreună cu identificarea şi interacţiunea acestor procese şi managementul acestora poate fi considerata ca fiind "o abordare bazată pe proces".

Abordarea bazată pe proces pentru managementul securităţii informaţiei prezentată în acest standard internaţional încurajează utilizatorii acestuia să accentueze importanta următoarelor aspecte:

a) înţelegerea cerinţelor de securitate a informaţiei ale unei organizaţii şi nevoia de a stabili politici şi obiective pentru securitatea informaţiei;

b) implementarea şi utilizarea măsurilor pentru a administra riscurile securităţii informaţiei în contextul riscurilor de ansamblu ale afacerii;

c) monitorizarea şi evaluarea performantei şi eficientei SMSI; si

d) îmbunătăţirea continua bazata pe măsurarea obiectiva.

Acest standard internaţional adoptă modelul "Plan-Do-Check-Act" (PDCA)[N1]>, care este aplicat pentru a structura toate procesele SMSI. Figura 1 ilustrează felul în care un SMSI ia ca date de intrare cerinţele de securitate a informaţiei şi aşteptările părţilor interesate si, prin acţiunile şi procesele necesare obţine rezultate de securitate a informaţiei care îndeplinesc aceste cerinţe şi aşteptări. De asemenea, figura 1 ilustrează legăturile în procesele prezentate în articolele 4, 5, 6, 7 şi 8.

Adoptarea modelului PDCA trebuie să reflecte, de asemenea, principiile care guvernează securitatea sistemelor informaţionale şi a reţelelor aşa cum sunt ele exprimate în Liniile Generale ale OECD

[N1]) NOTĂ NAŢIONALĂ: Planifică - Implementează - Verifică - Acţionează.

(2002)[1]". Acest standard internațional asigura un model robust pentru implementarea principiilor în acele linii generale care guvernează analiza riscului, planificarea și implementarea securității, managementul securității și reevaluarea.

EXEMPLUL 1 - Una din cerințe poate fi ca breșele de securitate a informației să nu cauzeze pierderi financiare importante pentru o organizație si/sau să cauzeze dificultăți organizației.

EXEMPLUL 2 - In cazul în care are loc un incident important - ca de exemplu atacarea site-ului de eBusiness al unei organizații - ar trebui să existe oameni cu pregătire suficienta legata de procedurile corespunzătoare pentru a minimiza impactul acestui incident.

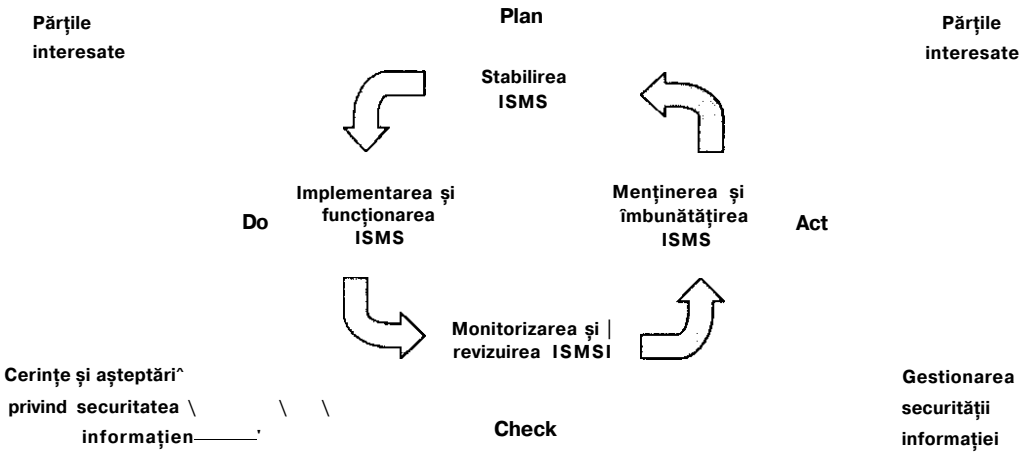

Figura 1 — Modelul PDCA aplicat proceselor SMSI

[1] **OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org**

Plan (stabilirea SMSI)	Stabilirea politicii SMSI, a obiectivelor, proceselor și procedurilor relevante pentru managementul riscului și îmbunătățirea securității informației pentru a furniza rezultate în conformitate cu politicile și obiectivele de ansamblu ale organizației.
Do (implementarea și funcționarea SMSI)	Implementarea și funcționarea politicilor SMSI, măsurilor de securitate, a proceselor și procedurilor.
Check (monitorizarea și revizuirea SMSI)	Evaluarea si, acolo unde este aplicabil, măsurarea performantei procesului în raport cu politica SMSI, obiectivele și experiența practica și raportarea rezultatelor către echipa de management pentru revizuire.
Act (menținerea și îmbunătățirea SMSI)	Deciderea de acțiuni corective și preventive, bazate pe rezultatele auditului intern SMSI și revizuirile managementului sau alte informații relevante pentru a obține o îmbunătățire continua a SMSI.

0.3 Compatibilitate cu alte sisteme de management

Acest standard internațional este aliniat la ISO 9001:2000 și ISO 14001:2004 pentru a susține o implementare coerentă și integrată și funcționarea corelată cu standardele de management adiacente. Un sistem de management proiectat corespunzător poate îndeplini cerințele tuturor acestor standarde. Tabelul C.1 ilustrează relația între clauzele acestui standard internațional, ISO 9001:2000 și ISO 14001:2004.

Acest standard internațional este elaborat pentru a permite unei organizații să alinieze sau să integreze SMSI cu cerințele similare ale altor sisteme de management.

IMPORTANT— Această publicație nu pretinde că include toate prevederile necesare ale unui contract. Utilizatorii sunt responsabili pentru aplicarea ei în mod corect. Conformitatea cu un standard internațional nu conferă imunitate în sine față de cerințele legale.

1 Domeniu de aplicare

1.1 Generalități

Acest standard internațional acoperă toate tipurile de organizații (de exemplu: societăți comerciale, agenții guvernamentale, organizații non-profit). Acest standard internațional specifica cerințele pentru stabilirea, implementarea, funcționarea, monitorizarea, revizuirea, menținerea și îmbunătățirea unui SMSI documentat în contextul general al riscurilor de afaceri ale organizației. El specifica cerințele pentru implementarea măsurilor de securitate adaptate la nevoile individuale ale organizației sau ale unor părți din aceasta.

SMSI este conceput pentru a asigura selectarea adecvată și proporțională a măsurilor de securitate care protejează resursele informatice și asigură încrederea părților implicate.

NOTA **1** - Referințele la "afacere" în acest standard internațional trebuie interpretate în sens larg pentru a se referi la acele activități care sunt esențiale scopului pentru care este înființată organizația.

NOTA **2** - ISO/CEI **17799** furnizează îndrumări pentru implementare, care pot fi folosite atunci când sunt proiectate măsurile de securitate.

1.2 Aplicare

Cerințele stabilite în acest standard internațional sunt generice și sunt destinate a fi aplicate de către toate organizațiile, indiferent de tip, mărime și natură. Excluderea oricăreia dintre cerințele specificate în articolele 4, 5, 6, 7 și 8, nu este acceptabilă pentru ca o organizație să pretindă conformitatea cu acest standard internațional.

Orice excludere a măsurilor de securitate care sunt necesare pentru a satisface criteriile de acceptare a riscului trebuie să fie justificată și trebuie furnizate dovezi că riscurile asociate au fost acceptate de către persoanele responsabile. Atunci când oricare dintre măsuri este exclusă, pretențiile de conformitate cu acest standard internațional nu sunt acceptabile decât dacă asemenea excluderi nu afectează capacitatea organizației si/sau responsabilitatea de a furniza o securitate a informației care să îndeplinească cerințele de securitate determinate de evaluarea riscului și cerințelor legale sau a reglementarilor aplicabile.

NOTĂ - Dacă o organizație are deja implementat un sistem de management al procesului afacerii (de exemplu în raport cu ISO **9001** sau ISO **14001),** este de preferat în cele mai multe cazuri să se încerce satisfacerea cerințelor acestui standard internațional în cadrul sistemului de management existent.

2 Referințe normative

Următoarele documente de referință sunt indispensabile pentru aplicarea acestui document. Pentru referințele datate, se aplică doar ediția citată. Pentru referințele care nu sunt datate, se aplică ultima ediție a documentului la care s-a făcut referire (inclusiv amendamentele).

ISO/IEC 17799:2005, *Information Technology - Security Techniques - Code of practice for information security management*

3 Termeni și definiții

Pentru aplicarea acestui document, se aplică următorii termeni și definiții.

3.1
resurse
orice prezintă valoare pentru organizație

[ISO/IEC 13335-1:2004]

3.2
disponibilitate

proprietatea de a fi accesibil și utilizabil la cerere de către o entitate autorizată

[ISO/IEC 13335-1:2004]

3.3
confidențialitate
proprietatea ca informația să nu fie făcută disponibilă sau divulgată persoanelor, entităților sau proceselor neautorizate
[ISO/IEC 13335-1:2004]

3.4
securitatea informației
păstrarea confidențialității, integrității și a disponibilității informației; în plus, alte proprietăți precum autenticitatea, responsabilitatea, non-repudierea și fiabilitatea pot fi de asemenea implicate

[ISO/IEC 17799:2005]

3.5
eveniment de securitate a informațiilor
situație identificată în legătură cu un sistem, un serviciu sau o rețea care indică o posibilă încălcare a politicii de securitate a informațiilor, un eșec al măsurilor de protecție sau o situație ignorată anterior, dar relevantă din punct de vedere al securității.

[ISO/IEC TR 18044:2004]

3.6
incident privind securitatea informației
Un eveniment sau o serie de evenimente de securitate a informației care au o probabilitate semnificativa de a compromite activitățile organizației și de a aduce amenințări la securitatea informației.

[ISO/IEC TR 18044:2004]

3.7
sistem de management al securității informației
SMSI
partea din întreg sistemul de management, bazată pe o abordare a riscului afacerii, folosită pentru a stabili, implementa, funcționa, monitoriza, revizui, menține și îmbunătăți securitatea informației

NOTĂ - Sistemul de management include structuri organizaționale, politici, activități de planificare, responsabilități, practici, proceduri, procese și resurse.

3.8
integritate

proprietatea de a păstra acuratețea și deplinătatea resurselor

[ISO/IEC 13335-1:2004]

3.9
risc rezidual

riscul care rămâne după tratarea riscului

[ISO/IEC Guide 73:2002]

3.10
acceptarea riscului

decizie de acceptare a unui risc

[ISO/IEC Guide 73:2002]

3.11
analiza riscului
utilizarea sistematică a informației pentru a identifica sursele și pentru a estima riscul
[ISO/IEC Guide 73:2002]
3.12
determinarea riscului
procesul global de analiză și evaluare a riscului

[ISO/IEC Guide 73:2002]

3.13
evaluarea riscului
proces de comparare a riscului estimat cu criteriile de risc agreate în vederea stabilirii importanței riscului

[ISO/IEC Guide 73:2002]

3.14
managementul riscului

activități coordonate pentru îndrumarea și controlul unei organizații luând în considerare riscurile

[ISO/IEC Guide 73:2002]

3.15
tratarea riscului

proces de selecție și implementare a unor măsuri în vederea reducerii riscului.

[ISO/IEC Guide 73:2002]

NOTĂ - în acest standard internațional termenul de "control" este folosit ca sinonim pentru "măsură".

3.16

declarație de aplicabilitate

declarație documentată care descrie obiectivele de control și măsurile de securitate care sunt relevante și aplicabile SMSI al organizației.

NOTĂ - Obiectivele de control și măsurile sunt bazate pe rezultatele și concluziile analizei de risc și pe procesele de tratare a riscului, cerințe legale sau de reglementare, obligații contractuale și cerințele afacerii organizației pentru securitatea informației.

4 Sistem de management al securității informației

4.1 Cerințe generale

Organizația trebuie să stabilească, să implementeze, să facă să funcționeze, să monitorizeze, să revizuiască, să mențină și să îmbunătățească un SMSI documentat în contextul global al activităților de afaceri ale organizației și al riscurilor la care aceasta este expusă. Pentru aplicarea acestui standard internațional, procesul folosit se bazează pe modelul PDCA prezentat în figura 1.

4.2 Stabilirea și administrarea SMSI

4.2.1 Stabilirea SMSI

Organizația trebuie:

a) să definească domeniul de aplicare și limitele SMSI în raport cu caracteristicile afacerii, organizarea, locația, resurse și tehnologii, incluzând detaliile și justificarea pentru orice excludere din acest domeniu (a se vedea 1.2)

b) să definească politica SMSI în raport cu caracteristicile afacerii, organizarea, locația, resursele și tehnologiile care:

1) să includă un cadru de lucru pentru stabilirea obiectivelor și să stabilească o orientare generală și principii de acțiune cu privire la securitatea informației;

2) să ia în considerare afacerea și cerințele legale sau de reglementare, precum și obligațiile contractuale de securitate.

3) să se alinieze la contextul strategic al managementului riscului al organizației în care va avea loc stabilirea și menținerea SMSI.

4) să stabilească criteriile pe baza cărora riscul trebuie să fie evaluat (a se vedea 4.2.1c)); și

5) să fie aprobată de către echipa de conducere

NOTĂ - în sensul acestui standard internațional, politica SMSI este considerată ca fiind nivelul superior al politicilor de securitate a informației. Aceste politici pot fi menționate într-un singur document.

c) să definească abordarea pe care o adoptă organizația pentru analiza riscului:

1) să identifice o metodologie de determinare a riscului care este potrivită pentru SMSI precum și cerințele identificate de securitate a informației, cerințe legale și reglementări aplicabile

2) să definească criteriile pentru acceptarea riscului şi să identifice nivelurile de risc acceptabile (a se vedea 5.1f)).

Metodologia de evaluare a riscului aleasă trebuie să asigure că analizele de risc generează rezultate comparabile şi care pot fi reproduse.

NOTĂ: Există metodologii diferite de determinare a riscului. Exemple ale metodologiilor de evaluare a riscului sunt discutate în ISO/IEC TR 13335-3, *Information technology — Guidelines for the management of IT Security — Techniques for the management of IT Security*

d) să identifice riscurile.

1) să identifice resursele din cadrul SMSI şi deţinătorii ' acestor resurse

2) să identifice ameninţările asupra resurselor

3) să identifice vulnerabilităţile care pot fi exploatate de aceste ameninţări

4) să identifice impactul pe care pierderea confidenţialităţii, integrităţii şi disponibilităţii îl poate avea asupra resurselor.

e) să analizeze şi să evalueze riscul.

1) să evalueze impactul asupra afacerii organizaţiei care poate rezulta în urma unor incidente de securitate, ţinându-se cont de consecinţele pierderii confidenţialităţii, integrităţii sau disponibilităţii resurselor.

2) să evalueze probabilitatea realistă de apariţie a problemelor de securitate luând în considerare ameninţările şi vulnerabilităţile predominante, impactul asociat asupra resurselor şi măsurilor de securitate implementate în prezent.

3) să estimeze nivelurile de risc

4) să determine dacă riscurile sunt acceptabile sau necesită tratarea lor, folosind pentru aceasta criteriile de acceptare a riscului stabilite la 4.2.1c)2));

f) să identifice şi să evalueze opţiunile pentru tratarea riscului.

Acţiunile posibile includ:

1) aplicarea unor măsuri de securitate corespunzătoare;

2) acceptarea conştientă şi obiectivă a riscurilor, cu condiţia ca acestea să satisfacă în mod clar politicile şi criteriile de acceptare a riscurilor din cadrul organizaţiei (a se vedea 4.2.1c)2));

3) evitarea riscurilor; şi

4) transferarea riscurilor asociate afacerilor către alte părţi, de exemplu asigurători, furnizori.

g) să selecteze obiectivele de control şi măsurile pentru tratarea riscurilor.

[i] **Termenul de "deţinător" desemnează un individ sau entitate care are responsabilitatea aprobată de management pentru producţia, dezvoltarea, întreţinerea, utlizarea şi securitatea resurselor. Termenul de "deţinător" nu atribuie acestuia dreptul de proprietate asupra resursei.**

Obiectivele de control și măsurile trebuie selectate și implementate pentru a îndeplini cerințele identificate în urma analizei de risc și a procesului de tratare a riscului. Această selecție trebuie să țină seama de criteriile de acceptare a riscului (a se vedea 4.2.1c)2)) precum și de cerințele legale, de reglementare și contractuale.

Trebuie selectate obiectivele de control și măsurile corespunzătoare din anexa A pentru a acoperi cerințele identificate.

Obiectivele de control și măsurile listate în anexa A nu sunt exhaustive, putând fi, de asemenea, selectate obiective de control suplimentare și măsuri suplimentare.

NOTĂ - Anexa A conține o listă cuprinzătoare a obiectivelor de control și măsurilor care au fost identificate ca relevante în organizații. Utilizatorii acestui standard internațional trebuie să țină seama de anexa A ca punct de pornire pentru selectarea măsurilor de securitate pentru a se asigura că nici o opțiune importantă de control nu este trecută cu vederea.

h) să obțină aprobarea conducerii pentru riscurile reziduale propuse.

i) să obțină autorizarea conducerii pentru implementarea și funcționarea SMSI.

j) să pregătească o Declarație de Aplicabilitate.

O Declarație de Aplicabilitate trebuie elaborată astfel încât să includă următoarele:

1) obiectivele de control și măsurile selectate în 4.2.1g) și motivele pentru care au fost selectate.

2) obiectivele de control și măsurile implementate la momentul actual (a se vedea 4.2.1e)2));

3) excluderea oricăror obiective de control și măsurile din Anexa A și justificarea pentru excluderea lor.

NOTĂ - Declarația de Aplicabilitate furnizează un sumar al deciziilor cu privire la tratarea riscului. Justificarea excluderii furnizează o verificare încrucișată că nici o măsură de securitate nu a fost omisă din neglijență.

4.2.2 Implementarea şi funcţionarea SMSI

Organizația trebuie:

a) să formuleze un plan de tratare a riscului în care să identifice acțiunile corespunzătoare ce trebuie întreprinse de management, resursele, responsabilitățile și prioritățile pentru administrarea riscurilor de securitate a informației (a se vedea 5).

b) să implementeze planul de tratare a riscului pentru a obține obiectivele de control identificate care includ considerarea finanțării și alocarea rolurilor și responsabilităților.

c) să implementeze măsurile menționate în 4.2.1g) pentru a îndeplini obiectivele de control.

d) să definească modul de măsurare a eficienței pentru măsurile selectate sau pentru grupurile de măsuri și să specifice cum urmează să fie folosite aceste măsuri pentru a evalua eficiența măsurilor și pentru a produce rezultate comparabile și reproductibile (a se vedea 4.2.3c)).

NOTĂ - Măsurarea eficientei măsurilor de securitate permite managerilor și personalului să determine în ce măsura sunt atinse obiectivele de control planificate prin măsurile implementate.

e) să implementeze programe de instruire și de conștientizare (a se vedea 5.2.2).

f) să gestioneze funcționarea SMSI.

g) să administreze resursele alocate SMSI (a se vedea 5.2).

h) să implementeze procedurile şi alte măsuri capabile să permită detectarea promptă a evenimentelor de securitate şi răspunsul la incidente de securitate (a se vedea 4.2.3a)).

4.2.3 Monitorizarea şi revizuirea SMSI

Organizaţia trebuie:

a) să execute monitorizarea şi revizuirea procedurilor şi a altor măsuri de securitate pentru:

1) detectarea promptă a erorilor din rezultatele procesării;

2) identificarea promptă atât a tentativelor cât şi a încercărilor reuşite de penetrare a sistemului de securitate.

3) a da posibilitatea conducerii de a determina dacă activităţile de securitate delegate personalului sau implementate prin tehnologia informaţiei se desfăşoară conform aşteptărilor;

4) a ajuta detectarea evenimentelor de securitate şi prin acestea să prevină incidentele de securitate prin utilizarea indicatorilor; şi

5) a determina dacă acţiunile luate pentru a rezolva o breşă de securitate au fost eficiente.

b) să iniţieze evaluarea în mod periodic a eficientei SMSI (incluzând îndeplinirea politicii şi obiectivelor SMSI şi evaluarea măsurilor de securitate) luând în considerare rezultatele auditurilor de securitate, incidentelor, rezultatele măsurărilor de eficienţă, sugestii şi feedback din partea tuturor părţilor interesate.

c) să măsoare eficacitatea măsurilor de securitate pentru a verifica dacă cerinţele de securitate au fost îndeplinite.

d) să revizuiască analiza de risc la intervalele planificate şi să revizuiască riscurile reziduale şi nivelul de risc considerat ca fiind acceptabil, luând în considerare schimbările privind:

1) organizaţia;

2) tehnologia;

3) obiectivele afacerii şi procesele;

4) ameninţările identificate;

5) eficienţa măsurilor implementate;

6) evenimente externe, precum schimbările legate de mediul legal şi reglementari, obligaţiile contractuale modificate şi schimbările în climatul social.

e) să efectueze audituri interne ale SMSI la intervalele planificate(a se vedea 6).

NOTĂ - Auditurile interne, numite câteodată audituri de primă parte, sunt conduse de sau în numele organizaţiei pentru scopuri interne.

f) să iniţieze revizuiri manageriale regulate ale SMSI pentru a se asigura că domeniul de aplicabilitate rămâne adecvat şi sunt identificate îmbunătăţirile procesului SMSI (a se vedea 7.1).

g) să actualizeze planurile de securitate pentru a lua în considerare rezultatele activităţilor de monitorizare şi evaluare.

h) să înregistreze acţiunile şi evenimentele care pot avea un impact asupra eficienţei sau performanţelor SMSI (a se vedea 4.3.3).

4.2.4 Menţinerea şi îmbunătăţirea SMSI

Organizaţia trebuie în mod regulat:

a) să implementeze îmbunătăţirile identificate ale SMSI.

b) să ia măsuri corective şi preventive corespunzătoare în conformitate cu 8.2 şi 8.3. Să aplice lecţiile învăţate din experienţele de securitate ale altor organizaţii şi cele ale propriei organizaţii.

c) să comunice măsurile şi îmbunătăţirile tuturor părţilor interesate ţinând cont de detaliile corespunzătoare circumstanţelor şi, în funcţie de relevanţă, să cadă de acord cu acestea asupra modului în care trebuie să se procedeze.

d) să se asigure că îmbunătăţirile ating obiectivele planificate.

4.3 Cerinţe referitoare la documentaţie

4.3.1 Generalităţi

Documentaţia trebuie să includă înregistrări ale deciziilor de management, trebuie să asigure faptul că acţiunile pot fi urmărite până la deciziile şi politicile managementului şi trebuie să garanteze că rezultatele înregistrate sunt reproductibile.

Este important să poată demonstra relaţia dintre măsurile de securitate selectate, rezultatele procesului de determinare şi tratare a riscului şi ulterior cu politica şi obiectivele SMSI.

Documentaţia SMSI trebuie să includă:

a) enunţuri documentate ale politicii SMSI (a se vedea 4.2.1b)) şi obiective;

b) domeniul de aplicabilitate al SMSI (a se vedea 4.2.1a));

c) proceduri şi măsuri de securitate pentru susţinerea SMSI;

d) o descriere a metodologiei de analiza a riscului (a se vedea 4.2.1c));

e) raportul de analiza a riscului (a se vedea 4.2.1c pana la 4.2.1g));

f) planul de tratare a riscului (a se vedea 4.2.2b));

g) proceduri documentate de care are nevoie organizaţia pentru a asigura planificarea eficientă, funcţionarea şi controlul proceselor de securitate a informaţiei şi pentru a descrie cum se măsoară eficienţa măsurilor de securitate (a se vedea 4.2.3c));

h) înregistrările cerute de standardul internaţional (a se vedea 4.3.3) şi

i) Declaraţia de Aplicabilitate.

NOTA 1 - Atunci când apare termenul "procedură documentată" în cadrul acestui standard internaţional, aceasta înseamnă că procedura este stabilită, documentată, implementată şi menţinută.

NOTA 2 - Completitudinea documentației SMSI poate fi diferită de la o organizație la alta datorită:

mărimii organizației și tipurilor de activitate pe care le desfășoară; și

domeniului de aplicabilitate și complexității cerințelor de securitate și ale sistemului care este administrat.

NOTA 3 - Documentele și înregistrările pot fi în orice format sau pe orice tip de suport.

4.3.2 Controlul documentelor

Documentele cerute de SMSI trebuie să fie protejate și controlate. Trebuie stabilită o procedură documentată pentru a defini acțiunile conducerii pentru:

a) a aproba documentele privind adecvarea înainte de a le emite;

b) a revizui și actualiza documentele în funcție de necesitate și a reaproba documentele;

c) a asigura faptul că schimbările și revizia curentă a documentelor sunt identificate;

d) a asigura faptul ca versiunile relevante ale documentelor aplicabile sunt disponibile la punctele de utilizare;

e) a asigura faptul ca documentele rămân inteligibile și pot fi identificate imediat;

f) a asigura faptul ca documentele sunt disponibile celor care au nevoie de ele și sunt transferate, depozitate și distruse în conformitate cu procedurile aplicabile nivelului lor de clasificare;

g) a asigura faptul ca documentele de origine externă sunt identificate;

h) a asigura faptul ca distribuția documentelor este controlată;

i) a preveni utilizarea neintenționată a documentelor care nu mai sunt actuale; și

j) a aplica mijloace de identificare adecvată a acestora dacă acestea sunt păstrate pentru orice alt scop.

4.3.3 Controlul înregistrărilor

înregistrările trebuie să fie stabilite și menținute pentru a asigura dovada conformității cu cerințele și operarea efectiva a SMSI. Acestea trebuie protejate și controlate. SMSI trebuie să țină cont de orice cerințe legale și de reglementare relevante și obligații contractuale. înregistrările trebuie să rămână inteligibile, identificabile imediat și recuperabile. Controalele necesare pentru identificare, depozitare, protecție, recuperare, perioadă de reținere și distrugere a înregistrărilor trebuie documentate și implementate.

înregistrările privind performanta procesului trebuie păstrate așa cum este subliniat în paragraful 4.2 împreună cu toate incidentele de securitate semnificative apărute în cadrul SMSI.

EXEMPLU - Exemple de înregistrări sunt registrul de intrare a vizitatorilor, rapoartele de audit și formularele de autorizație de acces completate.

5 Responsabilitatea managementului

5.1 Angajamentul managementului

Managementul trebuie să furnizeze dovezi ale angajamentului său față de instituirea, implementarea, funcționarea, monitorizarea, revizuirea, menținerea și îmbunătățirea SMSI prin:

a) stabilirea politicii SMSI;

b) asigurarea faptului ca obiectivele și planurile SMSI sunt stabilite;

c) stabilirea rolurilor și responsabilităților privind securitatea informației;

d) comunicarea către organizație a importanței îndeplinirii obiectivelor de securitate a informației și conformării cu politica de securitate a informației, responsabilitățile legale și nevoia continuă de îmbunătățire.

e) asigurarea de resurse suficiente pentru stabilirea, implementarea, funcționarea, monitorizarea, revizuirea, menținerea și îmbunătățirea SMSI (a se vedea 5.2.1.)

f) stabilirea criteriilor de acceptare a riscurilor și a nivelurilor acceptabile de risc;

g) asigurarea că auditurile interne ale SMSI se desfășoară (a se vedea 6); și

h) realizarea analizelor de management ale SMSI (a se vedea 7).

5.2 Managementul resurselor

5.2.1 Asigurarea resurselor

Organizația trebuie să determine și să asigure resursele necesare pentru:

a) stabilirea, implementarea, funcționarea, monitorizarea, revizuirea, menținerea și îmbunătățirea SMSI;

b) asigurarea că procedurile de securitate a informației susțin cerințele afacerii;

c) identificarea și tratarea cerințelor legale și de reglementare și a obligațiilor de securitate contractuale;

d) menținerea unui sistem de securitate adecvat prin aplicarea corectă a tuturor măsurilor implementate;

e) efectuarea revizuirilor atunci când este necesar și reacția corespunzătoare față de rezultatele acestor revizuiri; și

f) atunci când este necesar, îmbunătățirea eficientei SMSI.

5.2.2 Instruire, conștientizare și competențe

Organizația trebuie să se asigure că personalul căruia îi sunt desemnate responsabilități definite în SMSI este competent să îndeplinească cerințele cerute prin:

a) determinarea competentelor necesare pentru personal în vederea îndeplinirii acestor sarcini;

b) asigurarea instruirii sau luarea altor acțiuni (de exemplu angajarea personalului competent) pentru a satisface aceste nevoi;

c) evaluarea eficienței măsurilor care au fost luate; și

d) menținerea înregistrărilor cu privire la educație, instruire, aptitudini, experiență și calificări (a se vedea 4.3.3)

Organizația trebuie să se asigure că personalul implicat este conștient de relevanța și importanța activităților de securitate a informației și de modul în care el contribuie la obținerea obiectivelor SMSI.

6 Audituri interne ale SMSI

Organizația trebuie să efectueze audituri interne ale SMSI la intervale planificate pentru a determina dacă obiectivele de control, măsurile, procesele și procedurile SMSI:

a) se conformează cerințelor acestui standard internațional și legislației sau reglementărilor relevante;

b) se conformează cerințelor identificate de securitate a informației;

c) sunt implementate eficient și menținute; și

d) sunt îndeplinite așa cum se aștepta.

Programul de audit trebuie planificat luând în considerare poziția și importanta proceselor și zonelor care urmează să fie auditate precum și rezultatele auditurilor anterioare. Criteriile de audit, aplicabilitatea, frecvența și metodele trebuie definite. Selectarea auditorilor și efectuarea auditurilor trebuie să asigure obiectivitatea și imparțialitatea procesului de audit. Auditorii nu își vor audita propria lor muncă.

Responsabilitățile și cerințele pentru planificarea și efectuarea de audituri și pentru raportarea rezultatelor și păstrarea înregistrărilor (a se vedea paragraful 4.3.3) trebuie definite printr-o procedură documentată.

Echipa de management care este responsabilă pentru domeniul care este auditat trebuie să se asigure că acțiunile necesare sunt luate fără întârzieri neprevăzute pentru a elimina neconformitățile detectate și cauzele acestora. Activitățile de urmărire trebuie să includă verificarea măsurilor luate și raportarea rezultatelor acestei verificări (a se vedea 8).

NOTĂ - ISO **19011:2002,** *Guidelines for quality and/or environmental management systems auditing,* poate furniza un îndrumar folositor pentru efectuarea auditurilor interne ale SMSI.

7 Analizele de management pentru SMSI

7.1 Generalități

Managementul trebuie să revizuiască SMSI al organizației la intervalele planificate (cel puțin o dată pe an) pentru a asigura continua adecvare, conformitate și eficiență. Aceasta revizuire trebuie să includă evaluarea oportunităților pentru îmbunătățire și nevoia de schimbări în cadrul SMSI, incluzând politica de securitate a informației și obiectivele de securitate a informației. Rezultatele revizuirilor trebuie documentate clar, iar înregistrările trebuie păstrate (a se vedea 4.3.3).

7.2 Elemente de intrare ale analizei

Elementele de intrare ale unei analize de management trebuie să includă:

a) rezultatele auditurilor și evaluărilor SMSI;

b) feedback din partea părților interesate;

c) tehnici, produse sau proceduri care pot fi utilizate în cadrul organizației pentru a îmbunătăți performanța și eficiența SMSI;

d) starea acțiunilor preventive și corective;

e) vulnerabilitățile și amenințările care nu au fost tratate în analiza de risc anterioară;

f) rezultatele care țin de eficienta măsurărilor;

g) acțiunile de urmărit de la analizele de management anterioare;

h) orice schimbări care pot afecta SMSI; și

i) recomandări pentru îmbunătățire

7.3 Elemente de ieșire ale analizei

Elementele de ieșire ale analizei de management trebuie să includă orice decizie sau acțiuni legate de următoarele:

a) îmbunătățirea eficienței SMSI.

b) actualizarea analizei de risc și a planului de tratare al riscului.

c) modificarea procedurilor și măsurilor care afectează securitatea informației, după cum este necesar, pentru a răspunde evenimentelor interne sau externe care pot avea impact asupra SMSI, incluzând schimbările în ceea ce privește:

1) cerințele afacerii;

2) cerințele de securitate;

3) procesele afacerii care afectează cerințele existente ale afacerii;

4) cerințele legale sau de reglementare;

5) obligații contractuale; și

6) nivelurile de risc si/sau criteriile pentru acceptarea riscului.

d) nevoi de resurse;

e) îmbunătățirea modului în care se măsoară eficiența măsurilor de securitate.

8 îmbunătățirea SMSI

8.1 îmbunătățire continuă

Organizația trebuie să îmbunătățească în mod continuu eficiența SMSI prin utilizarea politicii de securitate a informației, obiectivele securității informației, rezultatele auditului, analiza evenimentelor monitorizate, acțiunile corective și preventive și revizuirile manageriale (a se vedea 7).

8.2 Acțiune corectivă

Organizația trebuie să ia măsuri pentru a elimina cauza neconformității cu cerințele SMSI pentru a preveni recidiva. Procedura documentată pentru acțiunea corectivă trebuie să definească cerințele pentru:

a) identificarea neconformităţilor;

b) determinarea cauzelor neconformităţilor;

c) evaluarea necesităţii întreprinderii de acţiuni pentru a se asigura că neconformităţile nu reapar;

d) determinarea şi implementarea acţiunii corective necesare;

e) înregistrarea rezultatelor acţiunii întreprinse (a se vedea 4.3.3); şi

f) analiza acţiunii corective întreprinse.

8.3 Acţiune preventivă

Organizaţia trebuie să determine acţiunile necesare pentru a elimina cauza potenţialelor neconformităţi cu cerinţele SMSI în scopul prevenirii apariţiei lor. Măsurile preventive luate trebuie să fie adecvate faţă de impactul problemelor potenţiale. Procedura documentată pentru acţiunea preventivă trebuie să definească cerinţele pentru:

a) identificarea potenţialelor neconformităţii şi a cauzelor acestora;

b) evaluarea nevoii de acţiune pentru a preveni apariţia neconformităţilor;

c) determinarea şi implementarea acţiunii preventive necesare;

d) înregistrarea rezultatelor acţiunilor întreprinse (a se vedea 4.3.3); şi

e) analiza acţiunii preventive întreprinse.

Organizaţia trebuie să identifice riscurile ce s-au modificat precum şi cerinţele acţiunii preventive care se axează pe riscurile modificate semnificativ.

Prioritatea acţiunilor preventive trebuie să fi determinată pe baza rezultatelor analizei de risc.

NOTĂ - Acţiunea de prevenire a neconformităţilor este de cele mai multe ori mai eficientă din punct de vedere al costurilor decât acţiunea corectivă.

Anexa A
(normativă)
Obiective de control și măsuri de securitate

Obiectivele de control și măsurile enumerate în tabelul A.1 sunt derivate direct și în conformitate cu cele enumerate ISO/IEC 17799:2005 articolele 5-15. Listele din tabelul A.1 nu sunt exhaustive, iar o organizație poate considera că sunt necesare obiective de control și măsuri adiționale. Obiectivele de control și măsurile din aceste tabele trebuie selectate ca parte a procesului de implementare a SMSI specificat în 4.2.1.

Articolele de la 5 la 15 din ISO/CEI 17799:2005 asigură linii directoare și îndrumări de implementare pentru cele mai bune practici în vederea susținerii măsurilor de securitate specificate în A.5 - A.15.

Tabelul A.1 - Obiective de control și măsuri de securitate

A.5 Politica de securitate		
A.5.1 Politica de securitate a informației *Obiectiv:* Să asigure orientarea generală de management și sprijinul pentru securitatea informației în conformitate cu cerințele afacerii, legislația și reglementările aplicabile.		
A.5.1.1	Document de politică a securității informației	*Măsură de securitate* Documentul de politică a securității informației trebuie să fie aprobat de către management, trebuie să fie publicat și comunicat tuturor angajaților și terților părți relevante.
A.5.1.2	Revizuirea politicii de securitate a informației	*Măsură de securitate* Politica de securitate a informației trebuie să fie revizuită la intervalele planificate sau atunci când apar schimbări semnificative, pentru a se asigura permanenta ei adecvare, compatibilitate și eficiența.
A.6 Organizarea securității informației		
A.6.1 Organizarea interna *Obiectiv:* Să administreze securitatea informației în cadrul organizației.		
A.6.1.1	Angajamentul echipei de management privind securitatea informației	*Măsură de securitate* Managementul trebuie să susțină în mod activ securitatea informației în cadrul organizației prin direcție clară, angajament demonstrat, atribuții explicite și asumarea responsabilităților în ceea ce privește securitatea informației.
A.6.1.2	Coordonarea securității informației	*Măsură de securitate* Activitățile de asigurare a securității informației trebuie să fie coordonate de reprezentanți din diferite sectoare ale organizației cu roluri și funcții adecvate.

A.6.1.3	Alocarea responsabilităţilor pentru securitatea informaţiei	*Măsură de securitate* Toate responsabilităţile pentru securitatea informaţiei trebuie să fie în mod clar definite.
A.6.1.4	Procesul de autorizare pentru sistemele de procesare a informaţiei.	*Măsură de securitate* Pentru noile sisteme de procesare a informaţiei trebuie să fie definit şi implementat un proces formal de autorizare de către management.
A.6.1.5	Acorduri de confidenţialitate	*Măsură de securitate* Cerinţele organizaţiei de protejare a informaţiei prin contracte de confidenţialitate şi/sau nedivulgare trebuie să fie identificate şi revizuite periodic.
A.6.1.6	Contactul cu autorităţile	*Măsură de securitate* Trebuie să fie menţinute contacte corespunzătoare cu autorităţile competente.
A.6.1.7	Contactul cu grupuri specializate de interes	*Măsură de securitate* Contactele corespunzătoare cu grupurile specializate de interes sau cu alte forumuri de specialişti în securitate şi asociaţii profesionale trebuie menţinute.
A.6.1.8	Revizuirea independentă a securităţii informaţiei	*Măsură de securitate* Abordarea organizaţiei pentru managementul securităţii informaţiei şi a implementării acestuia (obiective de Măsură de securitate, măsuri de securitate, politici, procese şi proceduri pentru securitatea informaţiei) trebuie să fie evaluată independent la intervalele stabilite sau atunci când apar schimbări semnificative cu privire la implementarea securităţii.
A.6.2 Părţi externe *Obiectiv:* Să menţină securitatea informaţiei în cadrul organizaţiei şi a sistemelor de procesare a informaţiei care sunt accesate, procesate, comunicate către sau administrate de părţi externe.		
A.6.2.1	Identificarea riscurilor legate de părţile din afara organizaţiei	*Măsură de securitate* Riscurile pentru informaţia din cadrul organizaţiei şi pentru sistemele de procesare a informaţiei din cadrul proceselor afacerii care implică părţi din afara organizaţiei trebuie să fie identificate şi înainte de acordarea accesului să fie implementate măsuri de securitate corespunzătoare.
A.6.2.2	Respectarea cerinţelor de securitate în activităţile care implică clienţii	*Măsură de securitate* înainte de a permite accesul clienţilor la informaţia din cadrul organizaţiei sau la resursele acesteia, trebuie să fie identificate şi îndeplinite toate cerinţele de securitate necesare.

A.6.2.3	Respectarea cerinţelor de securitate în acordurile cu terţii	*Măsură de securitate* Acordurile cu părţile terţe care implică accesarea, procesarea, comunicarea sau administrarea informaţiei din cadrul organizaţiei sau a sistemelor de procesare a informaţiei, sau adăugarea de produse şi servicii la sistemele de procesare a informaţiei trebuie să acopere toate cerinţele de securitate relevante.
A.7 **Managementul resurselor**		
A.7.1 Responsabilitatea pentru resurse *Obiectiv:* Să obţină şi să menţină o protecţie corespunzătoare a resurselor organizaţionale.		
A.7.1.1	Inventarul resurselor	*Măsură de securitate* Toate resursele trebuie să fie identificate în mod clar şi trebuie întocmit şi menţinut un inventar al tuturor resurselor importante.
A.7.1.2	Deţinerea resurselor	*Măsură de securitate* Toate informaţiile şi resursele asociate cu sistemele de procesare a informaţiei trebuie să fie "deţinute"[3]) de o parte desemnată de către organizaţie.
A.7.1.3	Utilizarea în mod acceptabil a resurselor	*Măsură de securitate* Regulile pentru utilizarea în mod acceptabil a informaţiei şi resurselor asociate sistemelor de procesare a informaţiei trebuie să fie identificate, documentate şi implementate.
A.7.2 Clasificarea informaţiei *Obiectiv:* Să asigure faptul ca informaţia beneficiază de un nivel de protecţie adecvat.		
A.7.2.1	îndrumări de clasificare	*Măsură de securitate* Informaţia trebuie să fie clasificată în funcţie de valoare, cerinţe legale, importanta şi nivel de criticalitate pentru organizaţie.
A.7.2.2	Etichetarea şi manipularea informaţiei	*Măsură de securitate* Un set corespunzător de proceduri pentru etichetarea informaţiei şi manipularea acesteia trebuie să fie dezvoltat şi implementat în conformitate cu schema de clasificare adoptată de către organizaţie.

[3]) **Explicaţie: Termenul de "deţinător" desemnează un individ sau o entitate care are responsabilitatea aprobată de management pentru a controla producţia, dezvoltarea şi întreţinerea, utlizarea şi securitatea resurselor. Termenul de "deţinător" nu atribuie neapărat acestuia dreptul de proprietate asupra resursei.**

A.8 Securitatea resurselor umane		
A.8.1 înaintea angajării [4] *1* *Obiectiv:* Să se asigure că angajaţii, contractanţii şi utilizatorii terţi înţeleg responsabilităţile care le revin şi sunt corespunzători pentru rolurile pentru care sunt alocaţi precum şi să reducă riscul de furt, fraudă sau de folosire necorespunzătoare a sistemelor.		
A.8.1.1	Roluri şi responsabilităţi	*Măsură de securitate* Rolurile şi responsabilităţile angajaţilor, contractanţilor şi utilizatorilor terţi privind securitatea informaţiei trebuie să fie definite şi documentate în conformitate cu politica de securitate a informaţiei din cadrul organizaţiei.
A.8.1.2	Verificare	*Măsură de securitate* Pentru toţi candidaţii pentru angajare, contractanţii şi utilizatorii terţi trebuie să se efectueze controale de verificare de fond în conformitate cu legile aplicabile, reglementări şi etică, proporţionale cu cerinţele afacerii, clasificarea informaţiei la care urmează să aibă acces şi riscurile percepute.
A.8.1.3	Cerinţe şi condiţii de angajare	*Măsură de securitate* Ca parte a obligaţiilor contractuale, angajaţii, contractanţii şi utilizatorii terţi trebuie să fie de acord şi să semneze cerinţele şi condiţiile contractului de angajare, care trebuie să precizeze responsabilităţile lor şi ale organizaţiei pentru securitatea informaţiei.
A.8.2 In timpul perioadei de angajare *Obiectiv:* Să asigure faptul că toţi angajaţii, contractanţii şi utilizatorii terţi sunt conştienţi de ameninţările privind securitatea informaţiei, responsabilităţile şi răspunderile juridice ale acestora şi sunt pregătiţi să susţină politica de securitate organizaţională pe durata contractului de muncă şi să asigure reducerea riscului erorilor umane.		
A.8.2.1	Responsabilităţile managementului	*Măsură de securitate* Managementul trebuie să ceară angajaţilor, contractanţilor şi utilizatorilor terţi să aplice măsurile de securitate în conformitate cu politicile stabilite şi cu procedurile organizaţiei.
A.8.2.2	Gradul de calificare, educaţie şi instruire	*Măsură de securitate* Toţi angajaţii organizaţiei şi, acolo unde este relevant, contractanţii şi utilizatorii terţi, trebuie să primească o instruire corespunzătoare şi actualizări periodice în ceea ce priveşte politicile şi procedurile organizaţionale, în funcţie de atribuţiile specifice funcţiei lor.

[4] Explicaţie: Termenul de "angajare" are aici semnificaţia de a acoperi următoarele situaţii diferite: angajarea personalului (temporar sau pe durata îndelungată), repartizarea funcţiilor, schimbarea funcţiilor, repartizarea contractelor şi finalizarea acestor aranjamente.

A.8.2.3	Procesul disciplinar	*Măsură de securitate* Trebuie să existe un proces formal disciplinar pentru angajaţii care produc o încălcare a securităţii informaţiei
A.8.3 încetarea contractului sau schimbarea locului de munca *Obiectiv:* Să asigure faptul că angajaţii, contractanţii şi utilizatorii terţi părăsesc organizaţia sau schimbă locul de muncă într-o manieră reglementată.		
A.8.3.1	Responsabilităţile privind terminarea contractului	*Măsură de securitate* Responsabilităţile privind încetarea contractului de muncă sau schimbarea locului de muncă trebuie să fie în mod clar definite şi alocate.
A.8.3.2	Returnarea resurselor	*Măsură de securitate* Toţi angajaţii, contractanţii şi utilizatorii terţi trebuie să înapoieze organizaţiei resursele pe care le deţin la încetarea angajării, contractului de muncă sau acordului de muncă.
A.8.3.3	înlăturarea drepturilor de acces	*Măsură de securitate* Drepturile de acces la informaţie şi la sistemele de procesare a informaţiei ale tuturor angajaţilor, contractanţilor şi utilizatorilor terţi trebuie să fie revocate la terminarea angajării, contractului de muncă sau acordului de muncă sau ajustate în funcţie de schimbări.
A.9 Securitatea fizica şi a mediului de lucru		
A.9.1 Zone de securitate *Obiectiv:* Să prevină accesul fizic neautorizat, distrugerile şi pătrunderea în interiorul organizaţiei precum şi accesul la informaţii.		
A.9.1.1	Perimetrul fizic de securitate	*Măsură de securitate* Pentru a proteja zonele care conţin informaţii şi sisteme de procesare a informaţiei trebuie folosite perimetre de securitate (bariere precum pereţi, porţi de acces controlat pe baza de card sau birouri de recepţie cu personal de securitate).
A.9.1.2	Controlul accesului fizic	*Măsură de securitate* Zonele de securitate trebuie protejate prin controale adecvate ale accesului fizic pentru a se asigura că accesul este permis doar personalului autorizat.
A.9.1.3	Securizarea birourilor, încăperilor şi a sistemelor informaţionale	*Măsură de securitate* Organizaţia trebuie să proiecteze şi să implementeze măsuri pentru securizarea fizică a birourilor, încăperilor şi a sistemelor informaţionale.

A.9.1.4	Protejarea împotriva amenințărilor externe și de mediu	*Măsură de securitate* Organizația trebuie să proiecteze și să aplice măsuri de protecție fizică împotriva incendiilor, inundațiilor, cutremurelor, exploziilor, revoltelor publice și a oricăror alte forme de dezastre naturale sau produse de oameni.
A.9.1.5	Desfășurarea activității în zone de securitate	*Măsură de securitate* Organizația trebuie să proiecteze și să aplice măsuri și ghiduri pentru protecția fizica și pentru desfășurarea activității în zone de securitate
A.9.1.6	Zone de acces public, punctele de livrare și încărcare	*Măsură de securitate* Punctele de acces precum punctele de livrare și încărcare sau alte puncte pe unde persoanele care nu sunt autorizate pot intra în interior trebuie controlate și, dacă este posibil, izolate de sistemele de procesare a informației pentru a se evita accesul neautorizat.
A.9.2 Securitatea echipamentelor *Obiectiv:* Să prevină pierderea, avarierea, furtul sau compromiterea resurselor și întreruperea activităților din cadrul organizației.		
A.9.2.1	Amplasarea și protejarea echipamentelor	*Măsură de securitate* Echipamentele trebuie să fie amplasate și protejate astfel încât să se reducă riscurile față de amenințările și pericolele de mediu și față de posibilitatea de acces neautorizat.
A.9.2.2	Utilitățile suport pentru afacere	*Măsură de securitate* Echipamentele trebuie să fie protejate împotriva penelor de curent sau a altor întreruperi cauzate de probleme ale utilităților suport.
A.9.2.3	Securitatea rețelelor de cablu	*Măsură de securitate* Cablurile de energie și rețelele de telecomunicații purtătoare de date sau servicii de suport pentru informație trebuie protejate față de interceptări sau avarii.
A.9.2.4	întreținerea echipamentelor	*Măsură de securitate* Echipamentele trebuie să fie corect întreținute pentru a se asigura disponibilitatea continuă și integritatea acestora.
A.9.2.5	Securitatea echipamentului în afara locației	*Măsură de securitate* Pentru echipamentele scoase în afara locației trebuie să fie asigurată o securitate corespunzătoare, ținându-se cont de riscurile diferite pentru activitățile care se desfășoară în afara locației.

A.9.2.6	Scoaterea din uz sau reutilizarea în condiții de siguranță	*Măsură de securitate* Toate părțile din echipament care conțin medii de stocare trebuie verificate pentru a se asigura că orice date importante sau produse software licențiate au fost înlăturate sau suprascrise într-un mod sigur înainte de distrugere.
A.9.2.7	Scoaterea activelor	*Măsură de securitate* Echipamentele, informațiile sau produsele software nu trebuie scoase în afara spațiului de lucru fără o autorizare prealabilă.
A.10 Managementul comunicațiilor și operațiunilor		
A.10.1 Proceduri operaționale și responsabilități *Obiectiv:* Să asigure operarea corectă și în condiții de securitate a sistemelor de procesare a informației.		
A.10.1.1	Proceduri de operare documentate	*Măsură de securitate* Procedurile de operare trebuie să fie documentate, păstrate și puse la dispoziția tuturor celor care au nevoie de ele.
A.10.1.2	Managementul schimbărilor	*Măsură de securitate* Toate schimbările privind sistemele de procesare a informațiilor trebuie să se facă într-un mod controlat.
A.10.1.3	Separarea atribuțiilor	*Măsură de securitate* Atribuțiile și domeniile de responsabilitate trebuie separate pentru a reduce posibilitatea de modificări neautorizate sau neintenționate sau folosirea într-un mod greșit a resurselor din cadrul organizației.
A.10.1.4	Separarea sistemelor de dezvoltare, testare și a sistemelor operaționale	*Măsură de securitate* Sistemele de dezvoltare, testare și sistemele operaționale trebuie să fie separate pentru a reduce riscurile accesului neautorizat sau schimbărilor asupra sistemelor operaționale.
A.10.2 Managementul serviciilor furnizate de terți *Obiectiv:* Să implementeze și să mențină un nivel corespunzător al securității informației și al livrării serviciilor în concordanta cu acordurile de furnizare de către terți.		
A.10.2.1	Furnizarea serviciilor	*Măsură de securitate* Trebuie asigurat faptul că măsurile de securitate, definițiile serviciilor și parametrii de furnizare incluse în acordurile de furnizare de către terți sunt implementate, operate și întreținute corespunzător de către partea terță.

A.10.2.2	Monitorizarea și evaluarea serviciilor terților	*Măsură de securitate* Serviciile, rapoartele și înregistrările furnizate de partea terță trebuie monitorizate și evaluate în mod periodic iar, auditarea lor trebuie efectuată în mod regulat.
A.10.2.3	Managementul modificărilor în cazul serviciilor terților	*Măsură de securitate* Modificările privind furnizarea serviciilor, inclusiv întreținerea și îmbunătățirea politicilor existente de securitate a informației, procedurilor și măsurilor de securitate trebuie să se facă într-un mod controlat, ținând cont de gradul de criticalitate al sistemelor și proceselor de afaceri și de reevaluarea riscurilor.
A70.3 ***Planificarea şi acceptanţa sistemelor*** *Obiectiv:* Să reducă riscurile de disfuncționalități ale sistemelor.		
A.10.3.1	Managementul capacității	*Măsură de securitate* în vederea asigurării nivelului de performanță cerut de sistem utilizarea resurselor trebuie să fie monitorizată și optimizată, iar necesitățile de capacitate viitoare trebuie să fie prevăzute.
A.10.3.2	Acceptanța sistemului	*Măsură de securitate* Criteriile de acceptanța pentru noi sisteme informatice, actualizări și noi versiuni trebuie clar stabilite, iar în timpul dezvoltării și înainte de acordarea acceptanței trebuie efectuate teste adecvate.
A.10.4 Protecţia împotriva codurilor mobile şi dăunătoare *Obiectiv:* Să asigure protejarea integrității software-ului și a informației.		
A.10.4.1	Măsurile de securitate împotriva codului mobil și a codurilor cu potențial dăunător	*Măsură de securitate* Pentru protecția împotriva codurilor cu potențial dăunător trebuie implementate măsuri de securitate pentru detectarea, prevenirea și recuperarea datelor și trebuie implementate procedurile corespunzătoare de avertizare a utilizatorilor.
A.10.4.2	Măsurile de securitate față de codul mobil	*Măsură de securitate* Atunci când utilizarea codului mobil este autorizată, felul în care este configurat sistemul trebuie să asigure faptul potrivit căruia codul mobil autorizat funcționează în conformitate cu o politică de securitate clar definită, iar codul mobil neautorizat trebuie să fie împiedicat să se execute.

A.10.5 Copie de siguranţă *Obiectiv:* Să menţină integritatea şi disponibilitatea informaţiei şi a sistemelor de procesare a informaţiei.		
A.10.5.1	Copii de siguranţă ale informaţiei	*Măsură de securitate* Copiile de siguranţă ale informaţiilor şi ale produselor software trebuie testate în mod regulat în conformitate cu politica de realizare de copii de siguranţa convenită.
A. 10.6 Managementul securităţii reţelei *Obiectiv:* Să asigure protecţia reţelelor de informaţii şi protecţia infrastructurii de suport.		
A.10.6.1	Măsuri de securitate a reţelelor	*Măsură de securitate* Reţelele trebuie administrate şi controlate în mod adecvat pentru a fi protejate în fata ameninţărilor şi pentru a menţine securitatea pentru sistemele şi aplicaţiile care utilizează reţelele, incluzând informaţia aflată în tranzit.
A.10.6.2	Securitatea serviciilor de reţea	*Măsură de securitate* Cerinţele de securitate, nivelul serviciilor şi cerinţele de management pentru serviciile de reţea trebuie identificate şi incluse în orice acord privind serviciile de reţea, indiferent dacă aceste servicii sunt oferite intern sau sunt externalizate.
A.10.7 Manipularea mediilor de stocare *Obiectiv:* Să prevină divulgarea neautorizată, modificarea, îndepărtarea sau distrugerea resurselor şi întreruperea activităţilor afacerii.		
A.10.7.1	Managementul mediilor de stocare amovibile	*Măsură de securitate* Pentru managementul adecvat al mediilor de stocare amovibil trebuie să existe proceduri specifice.
A.10.7.2	Distrugerea mediilor de stocare	*Măsură de securitate* Mediile de stocare trebuie distruse într-un mod securizat şi sigur atunci când acest lucru se impune, folosind proceduri formale pentru aceasta.
A.10.7.3	Proceduri de manipulare a informaţiei	*Măsură de securitate* Pentru a proteja informaţiile împotriva utilizării improprii sau divulgării neautorizate trebuie stabilite proceduri specifice de manipulare şi stocare a acestora.
A.10.7.4	Securitatea documentaţiei de sistem	*Măsură de securitate* Documentaţia de sistem trebuie protejată împotriva accesului neautorizat.

A.10.8 Schimbul de informaţii		
Obiectiv: Să menţină securitatea schimbului de informaţie şi software în interiorul unei organizaţii sau cu orice entitate externă.		
A.10.8.1	Proceduri şi politici pentru schimbul de informaţii	*Măsură de securitate* Pentru protejarea schimbului de informaţii folosind orice tip de dispozitiv de comunicare trebuie implementate politici, proceduri şi măsuri de securitate formalizate de schimb.
A.10.8.2	Acorduri de schimb	*Măsură de securitate* Pentru schimbul de informaţii şi software între organizaţie şi alte părţi trebuie să fie stabilite acorduri specifice.
A.10.8.3	Mediile fizice de stocare în tranzit	*Măsură de securitate* Mediile de stocare care conţin informaţii trebuie să fie protejate împotriva accesului neautorizat, utilizării necorespunzătoare sau falsificării în timpul transportării dincolo de graniţele fizice ale organizaţiei.
A.10.8.4	Mesageria electronica	*Măsură de securitate* Informaţia transmisă prin mesageria electronică trebuie protejată în mod corespunzător.
A.10.8.5	Sistemele de informaţii ale afacerii	*Măsură de securitate* Pentru a proteja informaţia trebuie dezvoltate şi implementate politici şi proceduri corespunzător modului de interconectare a sistemelor de informaţii ale afacerii.
A.10.9 Serviciile de comerţ electronic		
Obiectiv: Să asigure securitatea serviciilor de comerţ electronic şi utilizarea lor în condiţii de siguranţă.		
A.10.9.1	Comerţul electronic	*Măsură de securitate* Informaţia implicată în comerţul electronic care trece prin reţelele publice trebuie protejată împotriva oricăror activităţi de fraudare, dispute contractuale, divulgare neautorizată şi modificare.
A.10.9.2	Tranzacţiile on-line	*Măsură de securitate* Informaţia implicată în tranzacţiile on-line trebuie protejată pentru a preveni transmiterea incompletă, direcţionarea greşită, modificarea neautorizată a mesajului, divulgarea neautorizată, copierea neautorizată sau replicarea neautorizată.
A.10.9.3	Informaţie disponibilă în mod public	*Măsură de securitate* Integritatea informaţiei de pe un sistem disponibil public trebuie să fie protejată pentru a preveni modificarea neautorizată a acesteia.

A.10.10 Monitorizarea		
Obiectiv: Identificarea activităţilor neautorizate de procesare a informaţiei.		
A.10.10.1	Jurnal de audit	*Măsură de securitate* Jurnalele de audit care înregistrează activităţile utilizatorului, excepţiile şi evenimentele de securitate a informaţiei trebuie produse şi păstrate pentru o perioadă de timp determinată pentru a facilita pe viitor investigaţiile şi pentru monitorizarea de control al accesului.
A.10.10.2	Monitorizarea utilizării sistemului	*Măsură de securitate* Trebuie stabilite proceduri pentru monitorizarea, utilizarea sistemelor de procesare a informaţiilor, iar rezultatele activităţilor de monitorizare trebuie revizuite în mod periodic.
A.10.10.3	Protecţia informaţiilor din jurnale	*Măsură de securitate* Sistemele de înregistrare şi jurnalele de informaţii trebuie protejate împotriva modificărilor şi accesului neautorizat.
A.10.10.4	Jurnalul activităţilor administratorului şi operatorului	*Măsură de securitate* Activităţile administratorului de sistem şi ale operatorului de sistem trebuie înregistrate.
A.10.10.5	înregistrarea erorilor şi deficienţelor în funcţionare	*Măsură de securitate* Erorile şi deficienţele în funcţionare trebuie înregistrate, analizate şi trebuie întreprinse acţiuni corespunzătoare.
A.10.10.6	Sincronizarea ceasului	*Măsură de securitate* Ceasurile tuturor sistemelor relevante de procesare a informaţiei din cadrul unei organizaţii sau dintr-un domeniu de securitate trebuie să fie sincronizate cu o sursă de referinţă temporală precisă agreată.
A.11 Controlul accesului		
A.11.1 Cerinţele afacerii pentru controlul accesului		
Obiectiv: Să controleze accesul la informaţie.		
A.11.1.1	Politica de control al accesului	*Măsură de securitate* Pe baza cerinţelor afacerii şi a cerinţelor de securitate trebuie stabilită, documentată şi revizuită o politică de control al accesului.

A.11.2 Managementul accesului utilizatorului *Obiectiv:* Să asigure accesul autorizat al utilizatorului și să prevină accesul neautorizat la sistemele de informații.		
A.11.2.1	înregistrarea utilizatorului	*Măsură de securitate* Trebuie să fie implementată o procedură formală de înregistrare a utilizatorului și de anulare a înregistrării pentru a garanta și pentru a revoca accesul la toate sistemele de informații și servicii.
A.11.2.2	Managementul privilegiilor	*Măsură de securitate* Alocarea și utilizarea privilegiilor trebuie restricționată și controlată.
A.11.2.3	Managementul parolei de utilizator	*Măsură de securitate* Alocarea parolelor trebuie controlată printr-un proces formal de management.
A.11.2.4	Revizuirea drepturilor de acces ale utilizatorului	*Măsură de securitate* Managementul trebuie să revizuiască drepturile de acces ale utilizatorilor la intervale regulate utilizând un proces formal pentru aceasta.
A.11.3 Responsabilitățile utilizatorului *Obiectiv:* Să prevină accesul neautorizat al utilizatorului precum și compromiterea sau furtul de informații și sisteme de procesare a informațiilor.		
A.11.3.1	Utilizarea parolei	*Măsură de securitate* Utilizatorilor trebuie să li se ceară să urmeze bunele practici de securitate în ceea ce privește selecția și utilizarea parolelor.
A.11.3.2	Echipamentul nesupravegheat de către utilizatori	*Măsură de securitate* Utilizatorii trebuie să se asigure că echipamentul lăsat nesupravegheat este protejat în mod corespunzător.
A.11.3.3	Politica biroului curat și a ecranului protejat	*Măsură de securitate* Trebuie adoptată o politică clară de folosire a cât mai puține documente și medii de stocare amovibile și o politică de păstrare a ecranului protejat pentru sistemele de procesare a informațiilor.
A.11.4 Controlul de acces la rețea *Obiectiv:* Să prevină accesul neautorizat la serviciile de rețea.		
A.11.4.1	Politica de utilizare a serviciilor de rețea	*Măsură de securitate* Utilizatorilor trebuie să li se furnizeze accesul doar pentru serviciile pentru care au fost autorizați în mod specific să le utilizeze.

A.11.4.2	Autentificarea utilizatorilor pentru conectarea din exterior	*Măsură de securitate* Pentru a controla accesul utilizatorilor la distanță trebuie utilizate metode de autentificare corespunzătoare.
A.11.4.3	Identificarea echipamentelor în rețea	*Măsură de securitate* Ca mijloc de a autentifica conexiunile și echipamentele din locații specifice trebuie luată în considerare identificarea automată a echipamentului respectiv.
A.11.4.4	Protecția porturilor de diagnoză la distantă și a celor de configurare	*Măsură de securitate* Accesul fizic și logic la porturile de diagnoză și de configurare trebuie să se facă în mod controlat
A.11.4.5	Separarea în interiorul rețelelor	*Măsură de securitate* Grupurile de servicii de informații, utilizatori și sisteme de informații trebuie să fie separate în interiorul rețelei.
A.11.4.6	Controlul conectării la rețea	*Măsură de securitate* Pentru rețele publice, în special cele care se întind dincolo de granițele organizației, capacitatea utilizatorilor de a se conecta la rețea trebuie restricționată în conformitate cu politica de control a accesului și cu cerințele aplicațiilor de afaceri (a se vedea 11.1).
A.11.4.7	Controlul de rutare în rețea	*Măsură de securitate* Trebuie implementate măsuri de securitate de rutare pentru rețele pentru a se asigura faptul că conexiunile computerului și fluxurile de informații nu încalcă politica de control al accesului pentru aplicațiile afacerii.
A.11.5 Controlul accesului la sistemul de operare *Obiectiv:* Să prevină accesul neautorizat la sistemele de operare.		
A.11.5.1	Proceduri de autentificare sigura	*Măsură de securitate* Accesul la sistemele de operare trebuie să se facă în mod controlat printr-o procedură sigură de logare.
A.11.5.2	Identificarea și autentificarea utilizatorului	*Măsură de securitate* Fiecare utilizator trebuie să aibă un identificator unic (ID-ul utilizatorului) numai pentru uz propriu și trebuie aleasă o tehnică de autentificare adecvată pentru a proba identitatea pe care utilizatorul pretinde că o are.
A.11.5.3	Sistemul de management al parolelor	*Măsură de securitate* Sistemele pentru managementul parolelor trebuie să fie interactive și să asigure calitatea parolelor.

A.11.5.4	Utilizarea programelor utilitare de sistem	*Măsură de securitate* Utilizarea programelor utilitare care pot fi capabile să depășească măsurile de securitate de sistem și de aplicații trebuie să fie restricționată și ferm controlată.
A.11.5.5	Pauza de sesiune	*Măsură de securitate* Sesiunile inactive trebuie închise după o perioadă definită de inactivitate.
A.11.5.6	Limitarea timpului de conectare	*Măsură de securitate* Pentru a furniza o securitate sporită a aplicațiilor cu grad ridicat de risc trebuie utilizate restricții cu privire la limitarea timpului de conectare.
A.11.6 Controlul accesului la aplicații și informații *Obiectiv:* Să prevină accesul neautorizat la informația deținută în sistemele de aplicații.		
A.11.6.1	Restricții de acces la informații	*Măsură de securitate* Accesul la informații și la funcțiile sistemului de aplicații de către utilizatori și personalul de suport trebuie restricționat în conformitate cu politica de control al accesului.
A. 11.6.2	Izolarea sistemelor critice	*Măsură de securitate* Sistemele critice pentru afacere trebuie să aibă alocat un spațiu dedicat (izolat) pentru desfășurarea proceselor.
A.11.7 Prelucrarea datelor folosind echipamente mobile și lucrul la distanță *Obiectiv:* Să asigure securitatea informației atunci când se folosesc sisteme pentru prelucrarea datelor folosind echipamente mobile și de lucru la distanță		
A.11.7.1	Prelucrarea datelor folosind echipamente și comunicații mobile	*Măsură de securitate* Pentru protecția împotriva riscurilor care decurg din folosirea echipamentelor și comunicațiilor mobile la distanță trebuie implementată o politică formală și trebuie luate măsuri de securitate corespunzătoare.
A.11.7.2	Lucrul la distanță	*Măsură de securitate* Pentru activitățile care se desfășoară la distanță trebuie dezvoltată și implementată o politică, planuri operaționale și proceduri specifice acestui tip de activități.

A.12 Achiziționarea, dezvoltarea și mentenanța sistemelor informatice		
A.12.1 Cerințe de securitate pentru sistemele informaționale *Obiectiv:* Să asigure faptul ca securitatea este parte integrantă a sistemelor informatice.		
A.12.1.1	Analiza și specificarea cerințelor de securitate	*Măsură de securitate* Cerințele de afaceri pentru noi sisteme informatice sau pentru îmbunătățirea sistemelor existente trebuie să cuprindă în mod specific cerințele pentru măsuri de securitate.
A.12.2 Procesarea corectă a datelor în cadrul aplicațiilor *Obiectiv:* Să prevină erorile, pierderile, modificările neautorizate sau folosirea greșită a informațiilor în cadrul aplicațiilor.		
A.12.2.1	Validarea datelor de intrare	*Măsură de securitate* Datele de intrare ale aplicațiilor trebuie validate pentru a se asigura că aceste date sunt corecte și corespunzătoare.
A.12.2.2	Controlul procesării interne	*Măsură de securitate* în cadrul aplicațiilor trebuie încorporate verificări de validare pentru a detecta orice modificare a informației prin procesarea eronată sau prin acte deliberate.
A.12.2.3	Integritatea mesajului	*Măsură de securitate* Cerințele pentru asigurarea autenticității și protejării integrității mesajelor în cadrul aplicațiilor trebuie să fie identificate și măsurile de securitate corespunzătoare trebuie identificate și implementate.
A.12.2.4	Validarea datelor de ieșire	*Măsură de securitate* Datele de ieșire din cadrul unei aplicații trebuie să fie validate pentru a se asigura că procesarea informației stocate este corect și adecvat circumstanțelor.
A.12.3 Măsuri criptografice *Obiectiv:* Să protejeze confidențialitatea, autenticitatea sau integritatea informației prin metode criptografice.		
A.12.3.1	Politica de utilizare a metodelor criptografice	*Măsură de securitate* Trebuie dezvoltată și implementată o politică în ceea ce privește utilizarea măsurilor criptografice pentru protecția informației.
A.12.3.2	Managementul cheilor criptografice	*Măsură de securitate* Pentru a susține utilizarea în cadrul organizației a tehnicilor criptografice trebuie implementat un management al cheilor criptografice.

A.12.4 Securitatea fişierelor de sistem *Obiectiv:* Să asigure securitatea fişierelor de sistem.		
A.12.4.1	Controlul software-ului operaţional	*Măsură de securitate* Pentru a controla instalarea de software pe sistemele operaţionale trebuie să fie implementate proceduri specifice
A.12.4.2	Protejarea datelor din sistemele de test	*Măsură de securitate* Datele de testare trebuie selectate cu grijă, protejate şi utilizate în mod controlat.
A.12.4.3	Controlul accesului la codul sursă al programelor	*Măsură de securitate* Accesul la codul sursă al programelor trebuie restricţionat.
A. 12.5 Securitatea în procesele de dezvoltare şi de suport *Obiectiv:* Să menţină securitatea produselor software de aplicaţii de sistem şi a informaţiei.		
A.12.5.1	Proceduri de control al modificărilor	*Măsură de securitate* Implementarea modificărilor trebuie controlată prin utilizarea de proceduri formale pentru controlul schimbărilor.
A.12.5.2	Revizuirea tehnică a aplicaţiilor după operarea modificărilor de sistem	*Măsură de securitate* Atunci când apar modificări asupra sistemelor de operare, aplicaţiile critice de afaceri trebuie revizuite şi testate pentru a se asigura că nu există un impact advers asupra operaţiunilor sau asupra securităţii organizaţionale.
A.12.5.3	Restricţii privind modificările asupra pachetelor software	*Măsură de securitate* Modificările asupra pachetelor software trebuie descurajate, limitate la modificările necesare, iar toate schimbările trebuie controlate în mod strict.
A.12.5.4	Scurgerea de informaţii	*Măsură de securitate* Posibilităţile de scurgeri de informaţii trebuie prevenite.
A.12.5.5	Externalizarea dezvoltării de software	*Măsură de securitate* Proiectele de dezvoltare externalizată de software trebuie să fie supravegheate şi monitorizate de către organizaţie.

A.12.6 Managementul vulnerabilităţilor tehnice		
Obiectiv: Să reducă riscurile care decurg din exploatarea vulnerabilităţilor tehnice publicate.		
A.12.6.1	Controlul vulnerabilităţilor tehnice	*Măsură de securitate* Trebuie să fie obţinute informaţii de actualitate în ceea ce priveşte vulnerabilităţile tehnice ale sistemelor de informaţii care pot fi folosite, trebuie evaluată expunerea organizaţiei faţă de aceste vulnerabilităţi şi trebuie luate măsuri corespunzătoare pentru a diminua riscul asociat.
A.13 Managementul incidentelor de securitate a informaţiei		
A.13.1 Raportarea evenimentelor produse şi a slăbiciunilor privind securitatea informaţiei		
Obiectiv: Să asigure faptul că evenimentele de securitate a informaţiei şi slăbiciunile asociate sistemelor informaţionale sunt comunicate de o manieră astfel încât să permită luarea de acţiuni corective la timp.		
A.13.1.1	Raportarea evenimentelor de securitate a informaţiei.	*Măsură de securitate* Evenimentele de securitate a informaţiei trebuie raportate prin canale de management corespunzătoare cât mai curând posibil.
A.13.1.2	Reportarea slăbiciunilor de securitate	*Măsură de securitate* Tuturor angajaţilor, contractanţilor şi utilizatorilor terţi ai sistemelor şi serviciilor informaţionale trebuie să li se ceară să raporteze şi să noteze orice slăbiciune de securitate observată sau suspectată în cadrul sistemelor sau a serviciilor.
A.13.2 Managementul incidentelor de securitate a informaţiei şi îmbunătăţiri		
Obiectiv: Să asigure faptul că pentru managementul incidentelor de securitate a informaţiei este aplicată o abordare consistentă şi eficientă.		
A.13.2.1	Responsabilităţi şi proceduri	*Măsură de securitate* Responsabilităţile şi procedurile de management trebuie stabilite pentru a asigura un răspuns rapid, eficient şi sistematic la incidentele de securitate a informaţiei.
A.13.2.2	învăţarea din incidentele de securitate a informaţiei	*Măsură de securitate* Trebuie implementate mecanisme pentru a autoriza cuantificarea şi monitorizarea tipului, volumului şi costurilor incidentelor de securitate a informaţiei.
A.13.2.3	Colectarea probelor	*Măsură de securitate* în cazurile în care o acţiune ulterioară împotriva unei persoane sau a unei organizaţii în urma unui incident de securitate a informaţiei implica o acţiune legală (civilă sau penală), trebuie colectate probe, iar acestea trebuie reţinute şi prezentate în conformitate cu regulile pentru colectarea probelor stabilite de legislaţia aplicabilă.

A.14 Managementul continuității afacerii		
A.14.1 Aspecte de securitate a informației a managementului continuității afacerii *Obiectiv:* Să contracareze orice discontinuități în activitățile afacerii și să protejeze procesele critice ale afacerii față de efectele căderilor majore ale sistemelor informaționale sau împotriva dezastrelor precum și să asigure reluarea acestora în timp optim.		
A.14.1.1	Includerea securității informației în procesul de management al continuității afacerii	*Măsură de securitate* Pentru continuitatea afacerii trebuie dezvoltat și menținut un proces administrat în cadrul organizației care să răspundă cerințelor de securitate a informației necesare pentru continuitatea afacerii organizației.
A.14.1.2	Continuitatea afacerii și evaluarea riscului	*Măsură de securitate* Evenimentele care pot cauza discontinuități proceselor afacerii trebuie identificate împreună cu probabilitatea și impactul unor asemenea discontinuități și împreună cu consecințele acestora pentru securitatea informației.
A.14.1.3	Dezvoltarea și implementarea planurilor de continuitate incluzând securitatea informației	*Măsură de securitate* Trebuie să fie dezvoltate și implementate planuri pentru a menține și restaura operațiunile și pentru a asigura disponibilitatea informației la nivelul cerut și în timpul cerut în urma întreruperii sau căderii proceselor critice ale afacerii.
A.14.1.4	Cadrul de planificare a continuității afacerii	*Măsură de securitate* Trebuie păstrată o structură unică pentru planurile de continuitate a afacerii în scopul asigurării continuității acestor planuri, al abordării consecvente a cerințelor de securitate a informațiilor și identificării priorităților de testare și întreținere.
A.14.1.5	Testarea, mentenanța și reevaluarea planurilor de continuitate a afacerii.	*Măsură de securitate* Planurile de continuitate a afacerii trebuie testate și actualizate în mod regulat pentru a se asigura că sunt eficiente și adecvate.
A.15 Conformitatea		
A.15.1 Conformitatea cu cerințele legale *Obiectiv:* Să evite încălcarea oricărei legi, obligații statuare, de reglementare sau contractuale sau a oricărei alte cerințe de securitate.		
A.15.1.1	Identificarea legislației aplicabile	*Măsură de securitate* Toate cerințele statutare, de reglementare și contractuale aplicabile și acțiunile organizației pentru a îndeplini aceste cerințe trebuie să fie definite în mod explicit, documentate și actualizate pentru fiecare sistem informațional și pentru organizație în ansamblu.

A.15.1.2	Drepturile de proprietate intelectuală (IPR)	*Măsură de securitate* Trebuie implementate proceduri corespunzătoare pentru a asigura conformitatea cu cerinţele legislative, de reglementare şi contractuale cu privire la utilizarea materialelor pentru care pot exista drepturi de proprietate intelectuală şi cu privire la utilizarea produselor software proprietare.
A.15.1.3	Protejarea înregistrărilor din cadrul organizaţiei	*Măsură de securitate* înregistrările importante trebuie protejate împotriva pierderii, distrugerii şi falsificării acestora în conformitate cu cerinţele statutare, de reglementare, contractuale şi de afaceri.
A.15.1.4	Protecţia datelor cu caracter personal şi confidenţialitatea informaţiilor personale	*Măsură de securitate* Protecţia datelor cu caracter personal şi confidenţialitatea acestora trebuie să fie asigurată aşa cum este specificat în legislaţia, regulamentele aplicabile şi, acolo unde este cazul, în clauzele contractuale.
A.15.1.5	Prevenirea utilizării în mod greşit a sistemelor de procesare a informaţiei	*Măsură de securitate* Utilizatorii trebuie împiedicaţi să folosească sistemele de procesare a informaţiilor în scopuri neautorizate.
A.15.1.6	Reglementări privind măsurile criptografice	*Măsură de securitate* Măsurile criptografice trebuie folosite în conformitate cu toate acordurile relevante, legile şi reglementările aplicabile.
A.15.2 Conformitatea cu standardele şi politicile de securitate şi conformitatea tehnică *Obectiv:* Să asigure conformitatea cu standardele şi politicile de securitate organizaţionale.		
A.15.2.1	Conformitatea cu standardele şi politicile de securitate	*Măsură de securitate* Managerii trebuie să se asigure că toate procedurile de securitate din domeniul lor de responsabilitate sunt respectate în mod corect pentru a obţine conformitatea cu standardele şi politicile de securitate.
A.15.2.2	Verificarea conformităţii tehnice	*Măsură de securitate* Sistemele informatice trebuie controlate în mod periodic pentru a fi conforme cu standardele de securitate implementate.

A.15.3 Considerații privind auditul asupra sistemelor informaționale *Obiectiv:* Să maximizeze eficiența procesului de audit și să minimizeze interferența acestuia asupra sistemelor informaționale.		
A.15.3.1	Controalele de audit al sistemelor informaționale	*Măsură de securitate* Cerințele de audit și activitățile care implică verificări asupra sistemelor operaționale trebuie să fie planificate cu grijă și trebuie convenite astfel încât să minimizeze riscul întreruperii proceselor de afaceri.
A. 15.3.2	Protecția instrumentelor de audit pentru sistemele informaționale	*Măsură de securitate* Accesul la instrumentele de audit pentru sistemele informaționale trebuie protejat pentru a preveni orice posibila utilizare greșită sau compromitere.

Anexa B
(informativ)

Principiile OECD și prezentul standard internațional

Aceste principii, stabilite în Ghidul OECD pentru Securitatea Sistemelor Informaționale și a Rețelelor, se aplică tuturor politicilor și nivelurilor operaționale care guvernează securitatea sistemelor informatice și a rețelelor. Acest standard internațional asigură un cadru al sistemului de management pentru securitatea informației în vederea implementării principiilor OECD utilizând modelul PDCA și procesele descrise în articolele 4, 5, 6 și 8 așa cum este indicat în tabelul B.1.

Tabelul B.1 — Principiile OECD și modelul PDCA

Principiul OECD	**Procesele SMSI corespunzătoare și stadiul PDCA**
Conștientizare Participanții trebuie să fie conștienți de nevoia de securitate pentru sistemele informatice și rețele și de ceea ce pot face pentru a întări securitatea.	Aceasta activitate face parte din faza **Do** (a se vedea 4.2.2 și 5.2.2).
Responsabilitate Toți participanții sunt responsabili pentru securitatea sistemelor de informații și a rețelelor.	Aceasta activitate face parte din faza **Do** (a se vedea 4.2.2 și 5.1).
Răspuns Participanții trebuie să acționeze la timp și într-un mod cooperativ pentru a preveni, detecta și a răspunde incidentelor de securitate.	Această parte este o activitate de monitorizare din faza **Check** (a se vedea 4.2.3 și 6 până la 7.3) și o activitate de răspuns din faza **Act** (a se vedea 4.2.4 și 8.1 pana la 8.3). Aceasta poate fi de asemenea cuprinsă de câteva aspecte din fazele **Plan** și **Check.**
Evaluarea riscului Participanții trebuie să efectueze analize de risc.	Aceasta activitate este parte a fazei **Plan** (a se vedea 4.2.1) și reevaluarea riscului este parte a fazei **Check** (a se vedea 4.2.3 și 6 până la 7.3)
Proiectarea și implementarea securității Participanții trebuie să încorporeze securitatea ca un element esențial al sistemelor de informații și al rețelelor.	Odată ce o analiza a riscului a fost finalizată, sunt selectate măsuri pentru tratarea riscurilor ca parte a fazei **Plan** (a se vedea 4.2.1). Faza **Do** (a se vedea 4.2.2 **și** 5.2) acoperă apoi implementarea și utilizarea operațională a acestor măsuri.
Managementul Securității Participanții trebuie să adopte o abordare cuprinzătoare față de managementul securității.	Managementul riscului este un proces care include prevenirea, detectarea și răspunsul față de incidente, întreținerea permanentă, revizuirea și auditul. Toate aceste aspecte fac parte din fazele **Plan, Do, Check și Act.**

Principiul OECD	Procesele SMSI corespunzătoare şi stadiul PDCA
Reevaluarea Participanţii trebuie să revizuiască şi să reevalueze securitatea sistemelor informaţionale şi trebuie să facă modificări corespunzătoare asupra politicilor de securitate, practicilor, măsurilor şi procedurilor.	Reevaluarea securităţii informaţiei face parte din faza Check (a se vedea 4.2.3 şi 6 până la 7.3) în care revizuirile trebuie întreprinse în mod regulat pentru a verifica eficienţa sistemului de management al securităţii informaţiei iar îmbunătăţirea securităţii este parte a fazei Act (a se vedea 4.2.4 şi 8.1 pană la 8.3).

Anexa C
(informativă)

Corespondența între ISO 9001:2000, ISO 14001:2004 și prezentul standard internațional

Tabelul C.1 prezintă corespondența între ISO 9001:2000, ISO 14001:2004 și prezentul standard internațional.

Tabelul C.1 — Corespondenta între ISO 9001:2000, ISO 14001:2004 și prezentul standard internațional

Prezentul standard internațional	**ISO 9001:2000**	**ISO 14001:2004**
0 Introducere	**0 Introducere**	**Introducere**
0.1 Generalități	0.1 Generalități	
0.2 Abordarea bazată pe proces	0.2 Abordare bazată pe proces	
	0.3 Relația cu ISO 9004	
0.3 Compatibilitate cu alte sisteme de management	0.4 Compatibilitate cu alte sisteme de management	
1 Domeniu de aplicare	**1 Domeniu de aplicare**	**1 Domeniu de aplicare**
1.1 Generalități	1.1 Generalități	
1.2 Aplicare	1.2 Aplicare	
2 Referințe normative	**2 Referințe normative**	**2 Referințe normative**
3 Termeni și definiții	**3 Termeni și definiții**	**3 Termeni și definiții**
4 Sistem de management ai securității informației	**4 Sistem de management al calității**	**4 Cerințe EMS**
4.1 Cerințe generale	4.1 Cerințe generale	4.1 Cerințe generale
4.2 Stabilirea și administrarea SMSI		
4.2.1 Stabilirea SMSI		
4.2.2 Implementarea și operarea SMSI		4.4 Implementarea și funcționarea
4.2.3 Monitorizarea și revizuirea SMSI	8.2.3 Monitorizarea și măsurarea proceselor	4.5.1 Monitorizarea și măsurarea
	8.2.4 Monitorizarea și măsurarea produsului	

Prezentul standard internațional	**ISO 9001:2000**	**ISO 14001:2004**
4.2.4 Menținerea și îmbunătățirea SMSI		
4.3 Cerințe referitoare la documentație 4.3.1 Generalități 4.3.2 Controlul documentelor 4.3.3 Controlul înregistrărilor	4.2 Cerințe referitoare la documentație 4.2.1 Generalități 4.2.2 Manualul calității 4.2.3 Controlul documentelor 4.2.4 Controlul înregistrărilor	 4.4.5 Controlul documentației 4.5.4 Controlul înregistrărilor
5 Responsabilitatea managementului 5.1 Angajamentul managementului	**5 Responsabilitatea managementului** 5.1 Angajamentul managementului 5.2 Orientare către client 5.3 Politica referitoare la calitate 5.4 Planificare 5.5 Responsabilitate, autoritate și comunicare	 4.2 Politica de mediu 4.3 Planificare
5.2 **Managementul resurselor** 5.2.1 Asigurarea resurselor 5.2.2 Instruire, conștientizare și competențe	**6 Managementul resurselor** 6.1 Asigurarea resurselor 6.2 Resurse umane 6.2.2 Competentă, conștientizare și instruire 6.3 Infrastructură 6.4 Mediu de lucru	 4.4.2 Competență, instructaj, și conștientizare
6 Audituri interne SMSI	8.2.2 Audit intern	4.5.5 Audit intern
7 **Analiza efectuată de management pentru SMSI** 7.1 Generalități 7.2 Elemente de intrare ale analizei	**5.6 Analiza efectuată de management** 5.6.1 Generalități 5.6.2 Elemente de intrare ale analizei	**4.6 Analiza efectuată de management**

Prezentul standard internațional	**ISO 9001:2000**	**ISO 14001:2004**
7.3 Elemente de ieșire ale analizei	**5.6.3** Elemente de ieșire ale analizei	
8 îmbunătățirea SMSI	**8.5 îmbunătățire**	
8.1 îmbunătățire continuă	**8.5.1** îmbunătățire continuă	
8.2 Acțiune corectivă	**8.5.3** Acțiune corectivă	**4.5.3** Neconformitate, acțiune corectivă și acțiune preventivă
8.3 Acțiune preventivă	**8.5.3** Acțiune preventivă	
Anexa A Obiective de control și măsuri de securitate		**Anexa A Ghid de utilizare a prezentului standard internațional**
Anexa B Principiile OECD și prezentul standard internațional		
Anexa C Corespondenta între ISO 9001:2000, ISO 14001:2004 și prezentul standard internațional	**Anexa A Corespondenta între ISO 9001:2000 și ISO 14001:1996**	**Anexa B Corespondenta între ISO 14001:2004 și ISO 9001:2000**

Bibliografie

Standarde

[1] ISO 9001:2000, *Quality management systems — Requirements*

[2] ISO/IEC 13335-1:2004, *Information technology— Security techniques— Management of information and communications technology security— Parti: Concepts and models for information and communications technology security management*

[3] ISO/IEC TR 13335-3:1998, *Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security*

[4] ISO/IEC TR 13335-4:2000, *Information technology— Guidelines for the management of IT Security — Part 4: Selection of safeguards*

[5] ISO 14001:2004, *Environmental management systems — Requirements with guidance for use*

[6] ISO/IEC TR 18044:2004, *Information technology— Security techniques— Information security incident management*

[7] ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*

[8] ISO/IEC Guide 62:1996, *General requirements for bodies operating assessment and certification/registration of quality systems*

[9] ISO/IEC Guide 73:2002, *Risk management — Vocabulary — Guidelines for use in standards*

Alte publicații

[1] OECD, *Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002.* www.oecd.org

[2] NIST SP 800-30, *Risk Management Guide for Information Technology Systems*

[3] Deming W.E., Out *of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study, 1986*

Standardul internațional ISO/CEI 27001:2005 a fost acceptat ca standard român de către comitetul tehnic CT 208 - *Tehnici de securitate în tehnologia informației.*

Membrii comitetului tehnic care au verificat versiunea română a acestui standard internațional:

dl.	**Victor Valeriu**	**PATRICIU**	**Academia Tehnică Militară, București**	**Președinte al comitetului tehnic CT 208 - *Tehnici de securitate în tehnologia informației***
dl.	**Teodor**	**STĂTESCU**	**ASRO**	**Secretar al comitetului tehnic CT 208 - *Tehnici de securitate în tehnologia informației*** **Membru al comitetului de lectură**
dl.	**Alexandru**	**ANDRIESCU**	**PROVISION, București**	
dl.	**Stelian**	**ARION**	**RASIROM, București**	
dl.	**Floarea**	**BAICU**	**CONSIS PROIECT, București**	
dl.	**Răzvan**	**BALINT**	**ROMSYM DATA, București**	
dna.	**Iulia -Theodora**	**BUMBAC**	**MCTI - Ministerul Comunicațiilor și Tehnologiei Informației**	
dl.	**Eugen**	**FUSEA**	**BUREAU VERITAS, București**	
dna.	**Florina**	**FUSU**	**TELEROM PROIECT, București**	
dl.	**Aurel**	**GRIGORE**	**PROVISION, București**	
dl.	**Andrei**	**HOHAN**	**FI ATEST, București**	
dl.	**Romulus**	**HOSSU**	**MAI - Ministerul Administrației și Internelor**	
dna.	**Rodica**	**HRIN**	**ICI - Institutul de Cercetări pentru Informatică, București**	
dl.	**Viorel**	**IONESCU**	**Academia Tehnică Militară, București**	
dl.	**Gabriel**	**IONIȚA**	**SOFTWIN, București**	
dl.	**Râzvan**	**MACOVEI**	**ING, București**	
dl.	**Liviu**	**NICOLESCU**	**MCTI - Ministerul Comunicațiilor și Tehnologiei Informației**	**Membru al comitetului de lectură**
dl.	**Mihail**	**SĂDEANU**	**S&T, București**	
dl.	**Nicolai**	**VĂCEANU**	**EFFICIENT COMPUTER ADVISER, București**	**Membru al comitetului de lectură**
dl.	**Florin**	**VREJOIU**	**ARIES - Asociația Română pentru Industria Electronică și Software, București**	

Versiunea română a prezentului standard a fost elaborată de către dl. Alexandru ANDRIESCU și dl. Horațiu Bandoiu (PROVISION, București).

Un standard român nu conține neapărat totalitatea prevederilor necesare pentru contractare. Utilizatorii standardului sunt răspunzători de aplicarea corectă a acestuia.

Este important ca utilizatorii standardelor române să se asigure că sunt în posesia ultimei ediții și a tuturor modificărilor.

Informațiile referitoare la standardele române sunt publicate în *Catalogul Standardelor Române* și în *Buletinul Standardizării.*