STANDARD MOLDOVEAN

SM SR ISO/CEI 27001:2016

ICS 35.040

Adoptat la 10.02.2016

Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Cerinţe

Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

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

Prezentul standard este identic cu standardul român
SR ISO/CEI 27001:2013

Prezentul standard înlocuieşte standardul SM ISO/CEI 27001:2014
care este anulat

INSTITUTUL NAŢIONAL DE STANDARDIZARE (INS)

Republica Moldova, mun. Chişinău, str. E. Coca, 28
Tel.: 22 905 303, fax: 22 905 333
www.standard.md

ICS 35.040

SR ISO/CEI 27001

Standard Român

Noiembrie 2013

Titlu

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

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

Technologies de l'information. Techniques de sécurité. Systèmes de management de la sécurité de l'information. Exigences

Aprobare

Aprobat de Directorul General al ASRO la 29 noiembrie 2013

Standardul internațional ISO/CEI 27001:2013 are statutul unui standard român

Înlocuieşte SR ISO/CEI 27001:2006

Data publicării versiunii române: 20 noiembrie 2015

Corespondență

Acest standard este identic cu standardul internațional ISO/CEI 27001:2013

ASOCIAȚIA DE STANDARDIZARE DIN ROMÂNIA

✉ Str. Mendeleev nr. 21-25, cod 010362, Bucureşti , 💻 www.asro.ro

Preambul național

Acest standard reprezintă versiunea română a textului în limba engleză al standardului internațional ISO/CEI 27001:2013.

Acest standard include modificările precizate în erata ISO/CEI 27001:2013/Cor.1:2014.

Versiunea română a fost recunoscută de ISO şi CEI ca având aceeaşi valabilitate cu versiunea oficială.

Standardul ISO/CEI 27001:2013 a fost adoptat ca standard român la data de 29 noiembrie 2013, prin publicarea unei file de confirmare.

Acest standard înlocuieşte SR ISO/CEI 27001:2006.

Corespondența dintre standardele internaționale la care se face referire şi standardele române este următoarea:

ISO/CEI 27000:2014	IDT	SR ISO/CEI 27000:2015 Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Privire de ansamblu şi vocabular

Pentru aplicarea acestui standard se utilizează standardele internaționale la care se face referire (respectiv standardele române identice cu acestea).

Simbolurile gradelor de echivalență (IDT - identic, MOD - modificat, NEQ - neechivalent), conform SR 10000-8.

Prezentul standard intră în patrimoniul ASRO/CT 208, Tehnici de securitate în informatică.

Versiunea română

Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe

Cuprins

Preambul

ISO (Organizația Internațională pentru Standardizare) şi CEI (Comisia Electrotehnică Internațională) constituie sistemul specializat pentru standardizare internațională. Organismele naționale care sunt membre ale ISO sau CEI participă la dezvoltarea standardelor internaționale în cadrul comitetelor tehnice stabilite de respectiva organizație pentru a se ocupa cu domeniile specifice de activitate tehnică. Comitetele tehnice ISO şi CEI colaborează în domenii de interes reciproc. Alte organizații internaționale, guvernamentale şi neguvernamentale, în colaborare cu ISO şi CEI, iau de asemenea parte la activitate. În domeniul tehnologiei informației, ISO şi CEI au stabilit un comitet tehnic comun ISO/CEI JTC 1.

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

Sarcina principală a comitetului tehnic comun este aceea de a elabora standarde internaționale. Proiectele standardelor internaționale adoptate de comitetul tehnic comun sunt transmise în vederea votării la organismele naționale. Publicarea ca standard internațional necesită aprobarea de către cel puțin 75% din organismele naționale participante la vot.

Se atrage atenția asupra posibilității ca unele dintre elementele acestui document să intre sub incidența unor drepturi de proprietate intelectuală. ISO şi CEI nu vor putea fi făcute responsabile pentru identificarea unuia sau a tuturor acestor drepturi de proprietate intelectuală.

ISO/CEI 27001 a fost elaborat de Comitetul Tehnic Comun ISO/CEI JTC 1, *Tehnologia Informației,* Subcomitetul SC 27, *Tehnici de Securitate TI.*

Această a doua ediție anulează şi înlocuieşte prima ediție (ISO/CEI 27001:2005), care a fost revizuită din punct de vedere tehnic.

0 Introducere

0.1 Generalități

Acest standard internațional a fost elaborat pentru a furniza cerințe pentru stabilirea, implementarea, întreținerea şi îmbunătățirea continuă a unui sistem de management al securității informației. Adoptarea unui sistem de management al securității informației este o decizie strategică pentru o organizație. Stabilirea şi implementarea unui sistem de management al securității informației într-o organizație este influențată de nevoile şi obiectivele acesteia, cerințele de securitate, procesele organizaționale utilizate, precum şi de mărimea şi structura organizației. Este de aşteptat ca toți aceşti factori de influență să se schimbe în timp.

Sistemul de management al securității informației păstrează confidențialitatea, integritatea şi disponibilitatea informațiilor, prin aplicarea unui proces de management al riscului şi conferă încredere părților interesate că riscurile sunt gestionate corespunzător.

Este important ca sistemul de management al securității informației să fie parte integrantă din şi integrat cu procesele şi structura globală de management ale organizației şi ca securitatea informației să fie luată în considerare în proiectarea proceselor, sistemelor informaționale şi mijloacelor de control. Este de aşteptat ca implementarea unui sistem de management al securității informației să fie dimensionată în conformitate cu nevoile organizației.

Acest standard internațional poate fi utilizat de părți interne sau externe pentru evaluarea abilității organizației de a satisface propriile cerințe de securitate a informației.

Ordinea în care aceste cerințe sunt specificate în prezentul standard internațional nu reflectă importanța lor şi nici nu implică ordinea în care ele trebuie implementate. Articolele din listă sunt enumerate doar pentru referință.

ISO/CEI 27000 prezintă o privire de ansamblu şi vocabularul sistemelor de management al securității informației, cu referire la familia de standarde a sistemului de management al securității informației (inclusiv ISO/CEI 27003[2], ISO/CEI 27004[3] şi ISO/CEI 27005[4]), cu termenii şi definițiile aferente.

0.2 Compatibilitatea cu alte standarde referitoare la sisteme de management

Acest standard internațional aplică structura de nivel înalt, titluri identice pentru paragrafe, text identic, termeni comuni şi definiții de bază specificate în anexa SL a Directivelor ISO/CEI, partea 1, Supliment ISO consolidat şi de aceea menține compatibilitatea cu alte standarde referitoare la sisteme de management care au adoptat anexa SL.

Această abordare comună specificată în anexa SL va fi utilă pentru acele organizații care aleg să funcționeze cu un singur sistem de management, pentru a satisface cerințele a două sau mai multe standarde referitoare la sisteme de management.

1 Domeniu de aplicare

Acest standard internațional specifică cerințele pentru stabilirea, implementarea, întreținerea, şi îmbunătățirea continuă a unui sistem de management al securității informației în contextul organizației. De asemenea, prezentul standard internațional include cerințele pentru evaluarea şi tratarea riscurilor de securitate a informației potrivit nevoilor organizației. Cerințele specificate în prezentul standard internațional sunt generice şi sunt destinate a fi aplicate tuturor organizațiilor, indiferent de tip, mărime sau natură. Excluderea oricăror cerințe specificate în articolele de la 4 până la 10 nu este acceptabilă, atunci când o organizație pretinde conformitatea cu prezentul standard internațional

2 Referințe normative

Următoarele documente, în întregime sau parțial, sunt referințe normative în acest document şi sunt indispensabile pentru aplicarea acestuia. Pentru referințele datate, se aplică doar ediția citată. Pentru referințe nedatate, se aplică ultima ediție a documentului la care se face referire (inclusiv eventualele amendamente).

ISO/IEC 27000, Information technology - Security techniques - Information security management systems - Overview and vocabulary

3 Termeni şi definiții

Pentru scopurile acestui document, se aplică termenii şi definițiile specificate în ISO/CEI 27000.

4 Contextul organizației

4.1 Înțelegerea organizației şi contextului ei

Organizația trebuie să determine problemele externe şi interne care sunt relevante pentru scopul său şi care afectează abilitatea sa de a obține rezultatele prevăzute pentru sistemul său de management al securității informației.

NOTĂ - Determinarea acestor probleme se referă la stabilirea contextului extern şi intern al organizației, conform paragrafului 5.3 din ISO 31000:2009[5].

4.2 Înțelegerea nevoilor şi aşteptărilor părților interesate

Organizația trebuie să determine:

a) părțile interesate care sunt relevante pentru sistemul de management al securității informației;

b) cerințele acestor părți interesate, referitoare la securitatea informației.

NOTĂ - Cerințele părților interesate pot include cerințe legale sau de reglementare şi obligații contractuale.

4.3 Determinarea domeniului de aplicare a sistemului de management al securității informației

Organizația trebuie să determine limitele şi aplicabilitatea sistemului de management al securității informației pentru a stabili domeniul său de aplicare.

Pentru determinarea acestui domeniu de aplicare, organizația trebuie să ia în considerare:

a) problemele externe şi interne la care se face referire în 4.1;

b) cerințele menționate în 4.2;

c) interfețele şi dependențele între activitățile desfăşurate de organizație şi cele care sunt desfăşurate de alte organizații.

Domeniul de aplicare trebuie să fie disponibil ca informație documentată.

4.4 Sistem de management al securității informației

Organizația trebuie să stabilească, să implementeze, să întrețină şi să îmbunătățească în mod continuu un sistem de management al securității informației, în conformitate cu cerințele prezentului standard internațional.

5 Conducere

5.1 Conducere şi angajament

Managementul superior trebuie să demonstreze abilități de conducere şi angajament cu privire la sistemul de management al securității informației prin:

a) asigurarea faptului că politica referitoare la securitatea informației şi obiectivele de securitate a informației sunt stabilite şi sunt compatibile cu direcțiile strategice ale organizației;

b) asigurarea integrării cerințelor pentru sistemul de management al securității informației în procesele organizației;

c) asigurarea faptului că resursele necesare pentru sistemul de management al securității informației sunt disponibile;

d) comunicarea importanței unui management eficace al securității informației şi a conformării cu cerințele unui sistem de management al securității informației;

e) asigurarea faptului că sistemul de management al securității informației obține rezultatele prevăzute;

f) direcționarea şi sprijinirea persoanelor pentru a contribui la eficacitatea sistemului de management al securității informației;

g) promovarea îmbunătățirii continue;

h) sprijinirea altor roluri relevante ale managementului pentru a demonstra abilitățile lor de conducere, aşa cum se aplică în ariile lor de responsabilitate.

5.2 Politică

Managementul superior trebuie să stabilească o politică referitoare la securitatea informației, care:

a) este adecvată scopului organizației;

b) include obiective de securitate a informației (a se vedea 6.2) sau furnizează un cadru de lucru pentru stabilirea obiectivelor de securitate a informației;

c) include un angajament de îndeplinire a cerințelor aplicabile referitoare la securitatea informației;

d) include un angajament pentru îmbunătățirea continuă a sistemului de management al securității informației.

Politica referitoare la securitatea informației trebuie:

e) să fie disponibilă ca informație documentată;

f) să fie comunicată în cadrul organizației;

g) să fie disponibilă părților interesate, după cum este necesar.

5.3 Roluri organizaționale, responsabilități şi autoritate

Managementul superior trebuie să se asigure că responsabilitățile şi autoritatea pentru rolurile relevante pentru securitatea informației sunt atribuite şi comunicate.

Managementul superior trebuie să atribuie responsabilități şi autoritate pentru:

a) asigurarea faptului că sistemul de management al securității informației este conform cu cerințele prezentului standard internațional;

b) raportarea performanței sistemului de management al securității informației către managementul superior.

NOTĂ – De asemenea, managementul superior poate să atribuie responsabilități şi autoritate pentru raportarea performanței sistemului de management al securității informației în cadrul organizației.

6 Planificare

6.1 Acțiuni referitoare la riscuri şi oportunități

6.1.1 Generalități

Atunci când planifică sistemul de management al securității informației, organizația trebuie să ia în considerare aspectele la care se face referire în 4.1 şi cerințele la care se face referire în 4.2 şi să determine riscurile şi oportunitățile care trebuie abordate pentru:

a) a asigura că sistemul de management al securității informației poate obține rezultatele prevăzute;

b) a preveni sau a reduce efectele nedorite;

c) a obține o îmbunătățire continuă.

Organizația trebuie să planifice:

d) acțiuni pentru a aborda aceste riscuri şi oportunități;

e) modul în care:

   1) să integreze şi să implementeze acțiunile în cadrul sistemului său de management al securității informației;

   2) să evalueze eficacitatea acestor acțiuni.

6.1.2 Evaluare a riscului de securitate a informației

Organizația trebuie să definească şi să aplice un proces de evaluare a riscului de securitate a informației, care:

a) stabileşte şi menține criteriile de risc de securitate a informației, care includ:

   1) criteriile de acceptare a riscului;

   2) criteriile pentru realizarea evaluării riscului de securitate a informației.

b) asigură că evaluarea repetată a riscului de securitate a informației produce rezultate consistente, valide şi comparabile;

c) identifică riscurile de securitate a informației:

   1) aplică procesul de evaluare a riscurilor de securitate a informației pentru identificarea riscurilor asociate cu pierderea confidențialității, integrității şi disponibilității informației în cadrul domeniului de aplicare a sistemului de management al securității informației;

   2) identifică proprietarii riscurilor.

d) analizează riscurile de securitate a informației:

   1) evaluează consecințele potențiale care ar rezulta dacă riscul identificat în 6.1.2 c) 1) ar surveni;

   2) evaluează plauzibilitatea reală de apariție a riscului identificat în 6.1.2 c) 1);

   3) determină nivelurile riscului.

e) estimează riscurile de securitate a informației:

   1) compară rezultatele analizei de risc cu criteriile de risc stabilite în 6.1.2 a);

   2) stabileşte prioritățile riscurilor analizate în vederea tratării riscului.

Organizația trebuie să rețină informație documentată despre procesul de evaluare a riscurilor de securitate a informației.

6.1.3 Tratarea riscurilor de securitate a informației

Organizația trebuie să definească şi să aplice un proces de tratare a riscurilor de securitate a informației, pentru:

a) alegerea opțiunile adecvate de tratare a riscurilor de securitate a informației, luând în considerare rezultatele evaluării riscului;

b) determinarea tuturor mijloacele de control necesare pentru implementarea opțiunile alese pentru tratarea riscului de securitate a informației;

   NOTĂ - Organizațiile pot să proiecteze mijloace de control după cum este necesar sau să le identifice din orice sursă.

c) compararea mijloacele de control alese în 6.1.3 b) de mai sus cu cele din anexa A şi verificarea faptului că niciun mijloc de control necesar nu a fost omis;

   NOTA 1 - Anexa A conține o listă cuprinzătoare a obiectivelor şi mijloacelor de control. Utilizatorii prezentului standard internațional sunt îndrumați către anexa A pentru a se asigura că nu este trecut cu vederea niciun mijloc de control necesar.

   NOTA 2 - Obiectivele de control sunt incluse implicit în mijloacele de control alese. Obiectivele şi mijloacele de control enumerate în anexa A nu sunt exhaustive şi pot fi necesare obiective şi mijloace de control suplimentare.

d) elaborarea unei Declarații de aplicabilitate, care conține mijloacele de control necesare (a se vedea 6.1.3 b) şi c)), justificarea pentru includerea lor, indiferent dacă ele sunt implementate sau nu, precum şi justificarea pentru excluderea mijloacelor de control din anexa A;

e) formularea unui plan de tratare a riscurilor de securitate a informației;

f) obținerea din partea proprietarilor riscului a aprobării planului de tratare a riscurilor de securitate a informației şi a acceptării riscurilor reziduale ale securității informației.

Organizația trebuie să rețină informație documentată despre procesul de tratare a riscurilor de securitate a informației.

NOTĂ - Procesele de evaluare şi tratare a riscurilor de securitate a informației din prezentul standard internațional se aliniază principiilor şi liniilor directoare generice furnizate în ISO 31000[5].

6.2 Obiectivele de securitate a informației şi planificarea obținerii lor

Organizația trebuie să stabilească obiective de securitate a informației pentru funcții şi niveluri relevante.

Obiectivele de securitate a informației trebuie:

a) să fie consistente în raport cu politica de securitate a informației;

b) să fie măsurabile (dacă se poate);

c) să ia în considerare cerințele aplicabile de securitate a informației şi rezultatele evaluării şi tratării riscului;

d) să fie comunicate;

e) să fie actualizate după cum este necesar.

Organizația trebuie să rețină informație documentată despre obiectivele de securitate a informației.

Atunci când se planifică modul de atingere al obiectivelor de securitate a informației, organizația trebuie să determine:

f) ce se va face;

g) ce resurse vor fi necesare;

h) cine va fi responsabil

i) când se va finaliza;

j) cum vor fi evaluate rezultatele.

7 Suport

7.1 Resurse

Organizația trebuie să stabilească şi să furnizeze resursele necesare pentru stabilirea, implementarea, întreținerea şi îmbunătățirea continuă a sistemului de management al securității informației.

7.2 Competență

Organizația trebuie:

a) să determine competența(ele) necesară(e) a(le) persoanei(lor) care lucrează sub controlul său şi care afectează performanța securității informației;

b) să asigure că aceste persoane sunt competente, pe baza educației, instruirii sau experienței adecvate;

c) să ia măsuri, acolo unde este aplicabil, pentru a obține competența necesară şi să evalueze eficacitatea măsurilor luate;

d) să rețină informație documentată adecvată, ca dovadă a competenței.

NOTĂ - Acțiunile aplicabile pot include, de exemplu: furnizarea de instruire, îndrumarea sau realocarea angajaților actuali; sau angajarea sau contractarea unor persoane competente.

7.3 Conştientizare

Persoanele care lucrează sub controlul organizației trebuie să fie conştiente asupra:

a) politicii referitoare la securitatea informației;

b) contribuției lor la eficacitatea sistemului de management al securității informației, inclusiv beneficiile unui sistem îmbunătățit de management al securității informației;

c) implicațiilor neconformării cu cerințele sistemului de management al securității informației.

7.4 Comunicare

Organizația trebuie să determine nevoia de comunicare internă şi externă relevantă pentru sistemul de management al securității informației, incluzând:

a) despre ce să se comunice;

b) când să se comunice;

c) cu cine să se comunice;

d) cine trebuie să comunice;

e) procesul prin care trebuie efectuată comunicarea.

7.5 Informație documentată

7.5.1 Generalități

Sistemul de management al securității informației al organizației trebuie să includă:

a) informație documentată cerută de prezentul standard internațional;

b) informație documentată determinată de organizație ca fiind necesară pentru eficacitatea sistemului de management al securității informației.

NOTĂ - Amploarea informației documentate pentru un sistem de management al securității informației poate diferi de la o organizație la alta datorită:

1) mărimii organizației şi tipurilor sale de activități, procese, produse şi servicii;
2) complexității proceselor şi interacțiuni lor;
3) competenței personalului.

7.5.2 Creare şi actualizare

Atunci când se creează şi se actualizează informație documentată, organizația trebuie să asigure în mod corespunzător:

a) identificarea şi descrierea (de exemplu, un titlu, dată, autor sau număr de referință);

b) formatul (de exemplu, limbă, versiune software, grafică) şi suportul (de exemplu, hârtie, electronic);

c) revizuirea şi aprobarea, pentru potrivire şi adecvare.

7.5.3 Controlul informației documentate

Informația documentată cerută de sistemul de management al securității informației şi de prezentul standard internațional trebuie controlată pentru a se asigura că:

a) este disponibilă şi potrivită utilizării, acolo şi atunci când este nevoie de ea;

b) este protejată în mod adecvat (de exemplu, împotriva pierderii confidențialității, utilizării improprii sau pierderii integrității).

Pentru controlul informației documentate, organizația trebuie să abordeze următoarele activități, după cum este aplicabil:

c) distribuție, acces, regăsire şi utilizare;

d) depozitare şi păstrare, inclusiv păstrarea lizibilității;

e) control al modificărilor (de exemplu, controlul versiunilor);

f) retenție şi eliminare.

Informația documentată de origine externă, determinată de către organizație a fi necesară pentru planificarea şi funcționarea sistemului de management al securității informației, trebuie să fie identificată după cum este cazul şi controlată.

NOTĂ - Accesul implică o decizie referitoare la permisiunea doar de a vizualiza informația documentată sau permisiunea şi autoritatea de a vizualiza şi modifica informația documentată etc.

8 Funcționare

8.1 Planificare operațională şi control operațional

Organizația trebuie să planifice, să implementeze şi să controleze procesele necesare pentru a îndeplinii cerințele securității informației, precum şi să implementeze acțiunile determinate conform 6.1. De asemenea, organizația trebuie să implementeze planuri pentru a atinge obiectivele de securitate a informației determinate conform 6.2.

Organizația trebuie să păstreze informație documentată, în măsura în care este necesar pentru a avea convingerea că procesele s-au desfăşurat aşa cum a fost planificat.

Organizația trebuie să controleze schimbările planificate şi să revadă consecințele schimbărilor neprevăzute, luând măsuri pentru diminuarea oricăror efecte adverse, după cum este necesar.

Organizația trebuie să asigure faptul că procesele externalizate sunt determinate şi controlate.

8.2 Evaluarea riscurilor de securitate a informației

Organizația trebuie să efectueze evaluarea riscurilor de securitate a informației la intervalele planificate sau atunci când se propun sau se întâmplă schimbări semnificative, luând în considerare criteriile stabilite conform 6.1.2 a).

Organizația trebuie să rețină informație documentată pentru rezultatele evaluării riscurilor de securitate a informației.

8.3 Tratarea riscurilor de securitate a informației

Organizația trebuie să implementeze planul de tratare a riscurilor de securitate a informației.

Organizația trebuie să rețină informație documentată pentru rezultatele tratării riscurilor de securitate a informației.

9 Evaluarea performanței

9.1 Supraveghere, măsurare, analiză şi evaluare

Organizația trebuie să evalueze performanța securității informației şi eficacitatea sistemului de management al securității informației.

Organizația trebuie să determine:

a) ce anume necesită supraveghere şi măsurare, inclusiv procese şi mijloace de control pentru securitatea informației;

b) metodele pentru supraveghere, măsurare, analiză şi evaluare, după cum este aplicabil, pentru a asigura rezultate valide;

NOTĂ - Se recomandă ca metodele alese să producă rezultate comparabile şi reproductibile pentru a fi considerate valide.

c) când trebuie efectuată supravegherea şi măsurarea;

d) cine trebuie să supravegheze şi să măsoare;

e) când trebuie analizate şi evaluate rezultatele supravegherii şi măsurării;

f) cine trebuie să analizeze şi să evalueze aceste rezultate.

Organizația trebuie să rețină informație documentată corespunzătoare, ca dovadă a rezultatelor supravegherii şi măsurării.

9.2 Audit intern

Organizația trebuie să efectueze audituri interne la intervale planificate, pentru a furniza informații dacă sistemul de management al securității informației:

a) este în conformitate cu:

1) cerințele proprii ale organizației referitoare la sistemul său de management al securității informației;

2) cerințele prezentului standard internațional.

b) este implementat şi întreținut efectiv.

Organizația trebuie:

c) să planifice, să stabilească, să implementeze şi să întrețină un program de audit, inclusiv frecvența, metodele, responsabilitățile, cerințele de planificare şi raportare. Programul de audit trebuie să ia în considerare importanța proceselor avute în vedere şi rezultatele auditurilor anterioare;

d) să definească criteriile de audit şi domeniul de aplicare al fiecărui audit;

e) să aleagă auditorii şi să efectueze auditurile astfel încât să se asigure obiectivitatea şi imparțialitatea procesului de audit;

f) să asigure că rezultatele auditurilor sunt raportate managementului relevant;

g) să rețină informație documentată ca dovadă a programului de audit şi a rezultatelor auditului.

9.3 Revizuire de către management

Managementul superior trebuie să revizuiască sistemul de management al securității informației al organizației la intervale planificate, pentru a asigura potrivirea, adecvarea şi eficacitatea sa continuă.

Revizuirea de către management trebuie să includă luarea în considerare a:

a) stării acțiunilor din revizuirile anterioare de către management;

b) schimbărilor aspectelor externe şi interne care sunt relevante pentru sistemul de management al securității informației;

c) reacțiilor asupra performanței securității informației, incluzând tendințe în

   1) neconformități şi acțiuni corective;

   2) supraveghere şi rezultatele măsurărilor;

   3) rezultatele auditurilor;

   4) atingerea obiectivelor de securitate a informației;

d) reacțiilor din partea părților interesate;

e) rezultatelor evaluării riscului şi starea planului de tratare a riscului;

f) oportunităților pentru îmbunătățire continuă.

Rezultatele revizuirii de către management trebuie să includă decizii referitoare la oportunitățile de îmbunătățire continuă şi orice necesități de schimbare a sistemului de management al securității informației.

Organizația trebuie să rețină informație documentată, ca dovadă a rezultatelor revizuirilor de către management.

10 Îmbunătățire

10.1 Neconformitate şi acțiune corectivă

Atunci când survine o neconformitate, organizația trebuie:

a) să reacționeze la neconformitate şi, după cum este aplicabil:

   1) să ia măsuri pentru controlul şi corectarea ei;

   2) să facă față consecințelor;

b) să evalueze necesitatea de a acționa în vederea eliminării cauzelor neconformității, astfel încât ea să nu reapară sau să nu apară în altă parte, prin:

   1) revizuirea neconformității;

   2) determinarea cauzelor neconformității;

   3) determinarea existenței neconformităților similare sau care ar putea apare;

c) să implementeze orice acțiune necesară;

d) să revizuiască eficacitatea oricărei acțiuni corective întreprinse;

e) să facă modificări în sistemul de management al securității informației, dacă este necesar.

Acțiunile corective trebuie să fie adecvate efectelor neconformităților întâmpinate.

Organizația trebuie să rețină informație documentată, ca dovadă a:

f) naturii neconformităților şi a oricăror acțiuni luate în consecință;

g) rezultatelor oricăror acțiuni corective.

10.2 Îmbunătățire continuă

Organizația trebuie să îmbunătățească în mod continuu potrivirea, adecvarea şi eficacitatea sistemului de management al securității informației.

Anexa A
(normativă)

Obiective şi mijloace de control de referință

Obiectivele şi mijloacele de control enumerate în tabelul A.1 sunt derivate direct din cele enumerate în ISO/ISO/CEI 27002:2013[1] articolele 5 până la 18 şi trebuie utilizate în contextul paragrafului 6.1.3.

Tabelul A.1 – Obiective şi mijloace de control

A.5 Politica de securitate a informației		
A.5.1 Direcția managerială pentru securitatea informației		
Obiectiv: Să asigure orientarea generală de către management şi sprijinul pentru securitatea informației în conformitate cu cerințele afacerii, legislația şi reglementările aplicabile.		
A.5.1.1	Politici de securitate a informației	*Mijloc de control* Un set de politici de securitate a informației trebuie să fie definit, aprobat de către management, publicat şi comunicat tuturor angajaților şi terților părți relevante.
A.5.1.2	Revizuirea politicii de securitate a informației	*Mijloc de control* Politicile de securitate a informației trebuie să fie revizuite la intervale planificate sau atunci când apar schimbări semnificative, pentru a se asigura permanenta lor adecvare, compatibilitate şi eficiență.
A.6 Organizarea securității informației		
A.6.1 Organizarea internă		
Obiectiv: Să stabilească un cadru de management, pentru a iniția şi controla implementarea şi funcționarea securității informației în organizație.		
A.6.1.1	Roluri şi responsabilități privind securitatea informației	*Mijloc de control* Trebuie definite şi atribuite toate responsabilitățile privind securitatea informației.
A.6.1.2	Separarea sarcinilor	*Mijloc de control* Sarcinile şi domeniile de responsabilitate aflate în conflict trebuie să fie separate pentru a reduce posibilitatea modificării neautorizate sau neintenționate sau utilizarea greşită a resurselor organizației.
A.6.1.3	Contactul cu autoritățile	*Mijloc de control* Trebuie menținute contacte corespunzătoare cu autoritățile relevante.
A.6.1.4	Contactul cu grupuri speciale de interese	*Mijloc de control* Trebuie menținute contacte corespunzătoare cu grupuri speciale de interese sau alte forumuri specializate şi asociații profesionale în domeniul securității.
A.6.1.5	Securitatea informației în managementul proiectelor	*Mijloc de control* Securitatea informației trebuie să fie luată în considerare în managementul proiectelor, indiferent de tipul proiectului.

A.6.2 Dispozitive mobile şi lucrul la distanță		
Obiectiv: Să asigure securitatea lucrului la distanță şi a utilizării dispozitivelor mobile.		
A.6.2.1	Politică referitoare la dispozitivele mobile	*Mijloc de control* Trebuie adoptată o politică şi măsurile de securitate aferente pentru managementul riscului generat prin utilizarea dispozitivelor mobile.
A.6.2.2	Lucru la distanță	*Mijloc de control* Trebuie adoptată o politică şi măsurile de securitate aferente pentru a proteja informația accesată, prelucrată şi stocată în locații de lucru la distanță.
A.7 Securitatea resurselor umane		
A.7.1 Înaintea angajării		
Obiectiv: Să se asigure că angajații şi contractanții înțeleg responsabilitățile care le revin şi sunt corespunzători pentru rolurile pentru care sunt luați în considerare.		
A.7.1.1	Verificare	*Mijloc de control* Pentru toți candidații pentru angajare trebuie să se efectueze verificări de fond în conformitate cu legile aplicabile, cu reglementările şi cu regulile de etică; aceste verificări trebuie să fie proporționale cu cerințele afacerii, cu clasificarea informației la care urmează să aibă acces şi cu riscurile percepute.
A.7.1.2	Cerințe şi condiții de angajare	*Mijloc de control* Acordurile contractuale cu angajații şi contractanții trebuie să precizeze responsabilitățile lor şi ale organizației pentru securitatea informației.
A.7.2 În timpul perioadei de angajare		
Obiectiv: Să se asigure faptul că toți angajații şi contractanții sunt conştienți de responsabilitățile lor referitoare la securitatea informației şi le îndeplinesc.		
A.7.2.1	Responsabilitățile managementului	*Mijloc de control* Managementul trebuie să ceară angajaților să aplice regulile de securitate a informației, în conformitate cu politicile şi procedurile stabilite de organizație.
A.7.2.2	Conştientizare, educație şi instruire referitoare la securitatea informației	*Mijloc de control* Toți angajații organizației şi, acolo unde este relevant, contractanții trebuie să primească educație de conştientizare şi instruire corespunzătoare, precum şi informări regulate în ceea ce priveşte actualizarea politicilor şi procedurilor organizaționale, relevante pentru funcția lor.
A.7.2.3	Procesul disciplinar	*Mijloc de control* Trebuie să existe un proces disciplinar formal şi comunicat împotriva angajaților care produc o încălcare a regulilor de securitate a informației.
A.7.3 Încetarea şi schimbarea contractului de munca		
Obiectiv: Să protejeze interesele organizației în timpul procesului de schimbare sau de terminare a contractului de muncă.		
A.7.3.1	Terminarea sau schimbarea responsabilităților din contractul de muncă	*Mijloc de control* Responsabilitățile şi sarcinile referitoare la securitatea informației care rămân în vigoare după terminarea sau schimbarea contractului de muncă trebuie să fie definite, comunicate angajatului sau contractantului şi puse în aplicare.

A.8 Managementul resurselor		
A.8.1 Responsabilitatea pentru resurse		
Obiectiv: Să identifice resursele organizaționale şi să definească responsabilități de protecție corespunzătoare.		
A.8.1.1	Inventarul resurselor	*Mijloc de control* Informațiile, alte resurse asociate informațiilor şi mijloacele pentru prelucrarea informației trebuie să fie identificate şi trebuie întocmit şi menținut un inventar al acestor resurse.
A.8.1.2	Proprietatea asupra resurselor	*Mijloc de control* Resursele menținute în inventar trebuie să aibă proprietar.
A.8.1.3	Utilizarea în mod acceptabil a resurselor	*Mijloc de control* Regulile pentru utilizarea în mod acceptabil a informației şi resurselor asociate sistemelor de prelucrare a informației trebuie să fie identificate, documentate şi implementate.
A.8.1.4	Restituirea resurselor	*Mijloc de control* Toți angajații şi utilizatorii de terță parte trebuie să restituie toate resursele organizaționale aflate în posesia lor, la terminarea contractului de muncă, a contractului sau a acordului.
A.8.2 Clasificarea informației		
Obiectiv: Să asigure faptul ca informația beneficiază de un nivel de protecție în concordanță cu importanța ei pentru organizație.		
A.8.2.1	Clasificarea informației	*Mijloc de control* Informațiile trebuie să fie clasificate în funcție de cerințele legale, valoare, nivel critic şi susceptibilitatea de a fi dezvăluite neautorizat sau de a fi modificate.
A.8.2.2	Etichetarea informației	*Mijloc de control* Un set corespunzător de proceduri pentru etichetarea informației trebuie să fie dezvoltat şi implementat, în conformitate cu schema de clasificare adoptată de către organizație.
A.8.2.3	Manipularea resurselor	*Mijloc de control* Proceduri pentru manipularea resurselor trebuie să fie dezvoltate şi implementate, în conformitate cu schema de clasificare adoptată de către organizație.
A.8.3 Manipularea suporturilor		
Obiectiv: Să prevină dezvăluirea neautorizată, modificarea, eliminarea sau distrugerea informațiilor stocate pe suporturi.		
A.8.3.1	Managementul suporturilor amovibile	*Mijloc de control* Trebuie implementate proceduri pentru managementul suporturilor amovibile, în conformitate cu schema de clasificare adoptată de către organizație.
A.8.3.2	Eliminarea suporturilor	*Mijloc de control* Suporturile trebuie eliminate în mod sigur, atunci când nu mai sunt utilizate, utilizând proceduri formale.
A.8.3.3	Transferul suporturilor fizice	*Mijloc de control* Suporturile care conțin informații trebuie protejate în timpul transportului împotriva accesului neautorizat, utilizării greşite sau coruperii.

A.9 Controlul accesului		
A.9.1 Cerințe de afaceri pentru controlul accesului		
Obiectiv: Să limiteze accesul la informații şi la mijloacele de prelucrare a informațiilor.		
A.9.1.1	Politica de control al accesului	*Mijloc de control* Trebuie stabilită, documentată şi revizuită o politică de control al accesului, pe baza cerințelor de afaceri şi de securitate a informațiilor.
A.9.1.2	Acces la rețele şi servicii de rețea	*Mijloc de control* Utilizatorilor trebuie să li se furnizeze doar accesul la rețea şi la serviciile de rețea pentru care au fost autorizați în mod specific să le utilizeze.
A.9.2 Managementul accesului utilizatorului		
Obiectiv: Să asigure accesul autorizat al utilizatorului şi să prevină accesul neautorizat la sisteme şi servicii.		
A.9.2.1	Înregistrarea şi anularea înregistrării utilizatorului	*Mijloc de control* Trebuie implementat un proces formal de înregistrare şi anulare a înregistrării utilizatorului, pentru a permite atribuirea de drepturi de acces.
A.9.2.2	Furnizarea accesului utilizatorului	*Mijloc de control* Trebuie implementat un proces formal de furnizare a accesului utilizatorului, pentru atribuirea şi revocarea drepturilor de acces, pentru toate tipurile de utilizatori şi pentru toate sistemele şi serviciile.
A.9.2.3	Managementul drepturilor de acces privilegiat	*Mijloc de control* Atribuirea şi utilizarea drepturilor de acces privilegiat trebuie restricționate şi controlate.
A.9.2.4	Managementul informației secrete de autentificare a utilizatorului	*Mijloc de control* Atribuirea informației secrete de autentificare trebuie controlată printr-un proces formal de management.
A.9.2.5	Revizuirea drepturilor de acces ale utilizatorului	*Mijloc de control* Proprietarii resurselor trebuie să revizuiască drepturile de acces ale utilizatorilor la intervale regulate.
A.9.2.6	Retragerea sau adaptarea drepturilor de acces	*Mijloc de control* Drepturile de acces ale tuturor angajaților şi ale utilizatorilor de terță parte la informație şi la mijloacele de prelucrare a informației trebuie retrase după terminarea contractului de muncă, a contractului sau acordului, sau adaptate în funcție de schimbare.
A.9.3 Responsabilitățile utilizatorului		
Obiectiv: Să responsabilizeze utilizatorii în vederea protejării informației lor de autentificare		
A.9.3.1	Utilizarea informației secrete de autentificare	*Mijloc de control* Utilizatorilor trebuie să li se solicite să urmeze practicile organizației în ceea ce priveşte utilizarea informației secrete de autentificare.
A.9.4 Controlul accesului la sisteme şi aplicații		
Obiectiv: Să prevină accesul neautorizat la sisteme şi aplicații.		
A.9.4.1	Restricționarea accesului la informație	*Mijloc de control* Accesul la informație şi la funcțiile sistemului de aplicații trebuie să fie restricționat în conformitate cu prevederile politicii de control al accesului.

A.9.4.2	Proceduri securizate de conectare	*Mijloc de control* Acolo unde este cerut de politica de control al accesului, accesul la sisteme şi aplicații trebuie să fie controlat de o procedură securizată de conectare.
A.9.4.3	Sistem de management al parolelor	*Mijloc de control* Sistemele de management al parolelor trebuie să fie interactive şi să asigure parole de calitate.
A.9.4.4	Utilizarea programelor utilitare privilegiate	*Mijloc de control* Utilizarea programelor utilitare care pot fi capabile să evite mijloacele de control ale sistemelor şi aplicațiilor trebuie să fie restricționată şi controlată îndeaproape.
A.9.4.5	Controlul accesului la codul sursă al programelor	*Mijloc de control* Accesul la codul sursă al programelor trebuie să fie restricționat.
A.10 Criptografie		
A.10.1 Mijloace de control referitoare la criptografie		
Obiectiv: Să asigure utilizarea corespunzătoare şi eficientă a criptografiei în vederea protejării confidențialității, autenticității şi/sau integrității informației.		
A.10.1.1	Politica de utilizare a mijloacelor de control referitoare la criptografie	*Mijloc de control* Trebuie dezvoltată şi implementată o politică în ceea ce priveşte utilizarea mijloacelor de control referitoare la criptografie pentru protecția informației.
A.10.1.2	Managementul cheilor criptografice	*Mijloc de control* Trebuie dezvoltată şi implementată o politică în ceea ce priveşte utilizarea, protecția şi durata de viață a cheilor criptografice, de-a lungul întregului lor ciclu de viață.
A.11 Securitatea fizică şi a mediului de lucru		
A.11.1 Zone de securitate		
Obiectiv: Să prevină accesul fizic neautorizat, distrugerile şi interferarea cu informațiile şi mijloacele de prelucrare a informației organizației.		
A.11.1.1	Perimetrul fizic de securitate	*Mijloc de control* Trebuie definite şi utilizate perimetre de securitate pentru a proteja zonele care conțin fie informații senzitive sau critice, fie mijloace pentru prelucrarea informației
A.11.1.2	Controlul accesului fizic	*Mijloc de control* Zonele de securitate trebuie protejate prin mijloace de control al intrării adecvate, pentru a se asigura că accesul este permis doar personalului autorizat.
A.11.1.3	Securizarea birourilor, încăperilor şi facilităților	*Mijloc de control* Trebuie elaborate şi aplicate măsuri de securitate fizică pentru birouri, încăperi şi facilități.
A.11.1.4	Protejarea împotriva amenințărilor externe şi de mediu	*Mijloc de control* Trebuie elaborate şi aplicate măsuri de protecție fizică împotriva dezastrelor naturale, atacurilor malițioase sau accidentelor.
A.11.1.5	Desfăşurarea activității în zone de securitate	*Mijloc de control* Trebuie elaborate şi aplicate proceduri pentru desfăşurarea activității în zone de securitate

A.11.1.6	Puncte de livrare şi încărcare	*Mijloc de control* Punctele de acces, precum punctele de livrare şi încărcare sau alte puncte pe unde persoanele care nu sunt autorizate pot intra în interior, trebuie controlate şi, dacă este posibil, izolate de sistemele de prelucrare a informației pentru a se evita accesul neautorizat.
A.11.2 Echipamente		
Obiectiv: Să prevină pierderea, avarierea, furtul sau compromiterea resurselor şi întreruperea activităților din cadrul organizației.		
A.11.2.1	Amplasarea şi protejarea echipamentelor	*Mijloc de control* Echipamentele trebuie să fie amplasate şi protejate astfel încât să se reducă riscurile față de amenințările şi pericolele de mediu şi față de posibilitatea de acces neautorizat.
A.11.2.2	Utilitățile suport	*Mijloc de control* Echipamentele trebuie să fie protejate împotriva penelor de curent sau a altor întreruperi cauzate de probleme ale utilităților suport.
A.11.2.3	Securitatea cablării	*Mijloc de control* Cablurile de alimentare cu energie electrică şi de telecomunicații, purtătoare de date sau servicii de suport pentru informație, trebuie protejate față de interceptări, interferențe sau avarii.
A.11.2.4	Întreținerea echipamentelor	*Mijloc de control* Echipamentele trebuie să fie corect întreținute pentru a se asigura disponibilitatea continuă şi integritatea acestora.
A.11.2.5	Scoaterea resurselor	*Mijloc de control* Echipamentele, informațiile sau produsele software nu trebuie scoase în afara spațiului de lucru fără o autorizare prealabilă.
A.11.2.6	Securitatea echipamentului şi a resurselor situate în afara locației	*Mijloc de control* Pentru resursele situate în afara locației trebuie să fie asigurată o securitate corespunzătoare, cu luarea în considerare a riscurile diferite asociate lucrului în afara locației.
A.11.2.7	Eliminarea sau reutilizarea în condiții de securitate	*Mijloc de control* 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 eliminare sau reutilizare.
A.11.2.8	Echipamente nesupravegheate de utilizator	*Mijloc de control* Utilizatorii trebuie să se asigure că echipamentele nesupravegheate au o protecție corespunzătoare.
A.11.2.9	Politică referitoare la biroul şi ecranul curat	*Mijloc de control* Trebuie adoptate o politică referitoare la biroul curat, pentru hârtii şi medii de stocare amovibile şi o politică de ecran curat, pentru mijloacele de prelucrare a informației.
A.12 Securitatea operațiunilor		
A.12.1 Proceduri operaționale şi responsabilități		
Obiectiv: Să asigure operarea corectă şi în condiții de securitate a sistemelor de prelucrare a informației.		
A.12.1.1	Proceduri de operare documentate	*Mijloc de control* Procedurile de operare trebuie să fie documentate, păstrate şi puse la dispoziția tuturor celor care au nevoie de ele.

A.12.1.2	Managementul schimbărilor	*Mijloc de control* Schimbările privind organizația, procesele de afaceri, precum şi mijloacele şi sistemele de prelucrare a informațiilor, care afectează securitatea informației trebuie să fie controlate.
A.12.1.3	Managementul capacității	*Mijloc de control* Utilizarea resurselor trebuie supravegheată şi ajustată şi trebuie făcute prognoze ale cerințelor viitoare de capacitate, pentru a se asigura performanța necesară a sistemului.
A.12.1.4	Separarea mediilor de dezvoltare, testare şi funcționare	*Mijloc de control* Mediile de dezvoltare, testare şi funcționare trebuie să fie separate pentru a reduce riscurile de acces neautorizat sau de schimbare a mediului de funcționare.
A.12.2 Protecție împotriva malware-ului		
Obiectiv: Să asigure că informația şi mijloacele de prelucrare a informației sunt protejate împotriva malware-ului.		
A.12.2.1	Mijloace de control împotriva malware-ului	*Mijloc de control* Mijloacele de control pentru detecție, prevenire şi recuperare pentru protecția împotriva malware-ului trebuie implementate, împreună cu conştientizarea corespunzătoare a utilizatorului.
A.12.3 Copie de siguranță		
Obiectiv: Să protejeze împotriva pierderii datelor.		
A.12.3.1	Copie de siguranță a informației	*Mijloc de control* Copii de siguranță ale informației, software-ului şi imagini ale sistemului trebuie realizate şi testate în mod regulat, în conformitate cu politica de copii de siguranță agreată.
A.12.4 Înregistrare şi supraveghere		
Obiectiv: Înregistrarea evenimentelor şi generarea dovezilor		
A.12.4.1	Înregistrarea evenimentelor	*Mijloc de control* Jurnalele de evenimente care înregistrează activitățile utilizatorului, excepțiile, defectele şi evenimentele de securitate a informației trebuie produse, păstrate şi revizuite în mod regulat.
A.12.4.2	Protecția informațiilor din jurnale	*Mijloc de control* Mijloacele de înregistrare şi informațiile din jurnale trebuie protejate împotriva modificărilor şi accesului neautorizat.
A.12.4.3	Jurnale ale activităților administratorului şi operatorului	*Mijloc de control* Activitățile administratorului de sistem şi ale operatorului de sistem trebuie înregistrate, iar jurnalele trebuie protejate şi revizuite în mod regulat.
A.12.4.6	Sincronizarea ceasului	*Mijloc de control* Ceasurile tuturor sistemelor relevante de prelucrare a informației din cadrul unei organizații sau dintr-un domeniu de securitate trebuie să fie sincronizate în raport cu o singură sursă de referință temporală.
A.12.5 Controlul software-ului operațional		
Obiectiv: Să asigure integritatea sistemelor operaționale		
A.12.5.1	Instalarea de software pe sistemele operaționale	*Mijloc de control* Trebuie implementate proceduri pentru controlul instalării de software pe sistemele operaționale.

A.12.6 Managementul vulnerabilităților tehnice		
Obiectiv: Prevenirea exploatării vulnerabilităților tehnice		
A.12.6.1	Managementul vulnerabilităților tehnice	*Mijloc de control* Trebuie obținute în timp util informații despre vulnerabilitățile sistemelor informaționale utilizate, trebuie evaluată expunerea organizației la asemenea vulnerabilități şi trebuie luate măsuri adecvate pentru tratarea riscului asociat.
A.12.6.2	Restricții la instalarea de software	*Mijloc de control* Trebuie stabilite şi implementate reguli referitoare la instalarea software-ului de către utilizatori.
A.12.7 Considerații privind auditul sistemelor informaționale		
Obiectiv: Să minimizeze impactul activităților de audit asupra sistemelor operaționale.		
A.12.7.1	Mijloacele de control al auditului sistemelor informaționale	*Mijloc de control* Cerințele şi activitățile de audit care implică verificări asupra sistemelor operaționale trebuie să fie planificate cu grijă şi trebuie convenite astfel încât să se minimizeze riscul întreruperii proceselor de afaceri.
A.13 Securitatea comunicațiilor		
A.13.1 Managementul securității rețelei		
Obiectiv: Să asigure protecția informațiilor în rețele şi în mijloacele de prelucrare a informației care le susțin.		
A.13.1.1	Mijloace de control al rețelelor	*Mijloc de control* Rețelele trebuie administrate şi controlate în mod adecvat pentru protecția informației în sisteme şi aplicații.
A.13.1.2	Securitatea serviciilor de rețea	*Mijloc de control* Cerințele privind mecanismele de securitate, nivelul serviciilor şi management pentru toate serviciile de rețea trebuie identificate şi incluse în acorduri de servicii de rețea, indiferent dacă aceste servicii sunt oferite intern sau sunt externalizate.
A.13.1.3	Separarea în rețele	*Mijloc de control* Grupurile de servicii de informații, utilizatori şi sisteme informaționale trebuie să fie separate în rețele.
A.13.2 Transferul informației		
Obiectiv: Să mențină securitatea informației transferată în cadrul organizației sau cu orice entitate externă.		
A.13.2.1	Politici şi proceduri pentru transferul informației	*Mijloc de control* Pentru protejarea transferului informației folosind orice tip de dispozitiv de comunicare trebuie implementate politici, proceduri şi mijloace de control formalizate.
A.13.2.2	Acorduri de transfer al informației	*Mijloc de control* Acordurile trebuie să abordeze transferul securizat al informației de afaceri între organizație şi părți externe..
A.13.2.3	Mesagerie electronică	*Mijloc de control* Informația implicată în mesageria electronică trebuie protejată în mod corespunzător.
A.13.2.4	Acorduri de confidențialitate sau de nedezvăluire	*Mijloc de control* Cerințele pentru acorduri de confidențialitate sau nedezvăluire care să reflecte nevoile organizației pentru protecția informației trebuie identificate, revizuite şi documentate în mod regulat.

A.14 Achiziția, dezvoltarea şi mentenanța sistemelor		
A.14.1 Cerințe de securitate pentru sistemele informaționale		
Obiectiv: Să asigure faptul ca securitatea este parte integrantă a sistemelor informaționale pe întregul ciclu de viață. Aceasta include, de asemenea, cerințe pentru sisteme informaționale care furnizează servicii prin rețele publice.		
A.14.1.1	Analiza şi specificarea cerințelor de securitate a informației	*Mijloc de control* Cerințele referitoare la securitatea informației trebuie incluse în cerințele pentru sisteme informaționale noi sau îmbunătățiri ale sistemelor informaționale existente.
A.14.1.2	Securizarea serviciilor aplicațiilor în rețele publice	*Mijloc de control* Informația implicată în serviciile aplicațiilor, transmisă prin rețele publice, trebuie să fie protejată de activități frauduloase, dispute asupra contractelor, precum şi de dezvăluirea şi modificarea frauduloasă.
A.14.1.3	Protejarea tranzacțiilor serviciilor aplicațiilor	*Mijloc de control* Informația implicată în tranzacțiile serviciilor aplicațiilor trebuie să fie protejată împotriva transmiterii incomplete, rutării greşite, alterării neautorizate a mesajelor, dezvăluirii neautorizate, duplicării neautorizate sau reluării mesajelor.
A.14.2 Securitatea în procesele de dezvoltare şi de suport		
Obiectiv: Să asigure faptul că securitatea informației este implementată în cadrul ciclului de viață de dezvoltare a sistemelor informaționale.		
A.14.2.1	Politica de dezvoltare securizată	*Mijloc de control* Trebuie stabilite şi aplicate reguli pentru dezvoltarea software-ului şi sistemelor şi aplicate pentru dezvoltările din cadrul organizației.
A.14.2.2	Proceduri de control al modificării sistemelor	*Mijloc de control* Modificarea sistemelor în cadrul ciclului de viață de dezvoltare trebuie controlată prin utilizarea de proceduri formale pentru controlul schimbării.
A.14.2.3	Revizuirea tehnică a aplicațiilor după modificarea platformelor operaționale	*Mijloc de control* Atunci când apar modificări asupra platformelor operaționale, aplicațiile critice de afaceri trebuie revizuite şi încercate pentru a se asigura că nu există un impact advers asupra operațiunilor sau securității organizaționale.
A.14.2.4	Restricții privind modificările asupra pachetelor software	*Mijloc de control* Modificările asupra pachetelor software trebuie descurajate, limitate la modificările necesare, iar toate schimbările trebuie controlate în mod strict.
A.14.2.5	Principiile ingineriei sistemelor securizate	*Mijloc de control* Principiile ingineriei sistemelor securizate trebuie stabilite, documentate, întreținute şi aplicate tuturor eforturilor de implementare a sistemelor informaționale.
A.14.2.6	Mediul de dezvoltare securizat	*Mijloc de control* Organizațiile trebuie să stabilească şi să protejeze în mod corespunzător medii de dezvoltare securizate pentru eforturile de dezvoltare şi integrare a sistemelor care acoperă întregul ciclu de viață a dezvoltării sistemelor.
A.14.2.7	Dezvoltare externalizată	*Mijloc de control* Organizația trebuie să supervizeze şi să supravegheze activitatea externalizată de dezvoltare a sistemelor.

A.14.2.8	Testarea securității sistemelor	*Mijloc de control* Testarea funcționalității de securitate trebuie efectuată în timpul dezvoltării.
A.14.2.9	Testarea sistemelor în vederea recepției	*Mijloc de control* Programele de testare a sistemelor în vederea recepției şi criteriile referitoare la aceasta trebuie stabilite pentru sisteme informaționale noi, actualizări sau versiuni noi.
A.14.3 Date de testare		
Obiectiv: Să asigure protejarea datelor utilizate pentru testare.		
A.14.3.1	Protejarea datelor de testare	*Mijloc de control* Datele de testare trebuie alese cu grijă, protejate şi controlate.
A.15 Relații cu furnizorii		
A.15.1 Securitatea informației în relațiile cu furnizorii		
Obiectiv: Să asigure protejarea resurselor organizației care sunt accesate de furnizori.		
A.15.1.1	Politica de securitate a informației pentru relațiile cu furnizorii	*Mijloc de control* Cerințele de securitate a informației pentru reducerea riscurilor asociate accesului furnizorilor la resursele organizației trebuie agreate cu furnizorii şi documentate.
A.15.1.2	Abordarea securității în acordurile cu furnizorii	*Mijloc de control* Toate cerințele pentru securitatea informației relevante trebuie stabilite şi agreate cu fiecare furnizor care poate accesa, prelucra, stoca, comunica sau furniza componente pentru infrastructura TI a informației organizației.
A.15.1.3	Lanțul de aprovizionare al tehnologiei informației şi comunicațiilor	*Mijloc de control* Acordurile cu furnizorii trebuie să includă cerințe pentru abordarea riscurilor de securitate a informației asociate cu lanțul de aprovizionare cu servicii şi produse de tehnologia informației şi comunicațiilor.
A.15.2 Managementul livrării serviciilor furnizorilor		
Obiectiv: Să mențină un nivel al securității informației şi livrării serviciilor agreat, aliniat cu acordurile cu furnizorii.		
A.15.2.1	Supravegherea şi revizuirea serviciilor furnizorilor	*Mijloc de control* Organizațiile trebuie să supravegheze, să revizuiască şi să auditeze în mod regulat livrarea serviciilor furnizorilor.
A.15.2.2	Gestionarea schimbărilor serviciilor furnizorilor	*Mijloc de control* Schimbările în livrarea serviciilor de către furnizori, inclusiv întreținerea şi îmbunătățirea politicilor, procedurilor şi mijloacelor de control existente de securitate a informațiilor, trebuie gestionate luând în considerare nivelul critic al informației, sistemelor şi proceselor de afaceri implicate şi reevaluarea riscurilor.
A.16 Managementul incidentelor de securitate a informației		
A.16.1 Managementul incidentelor de securitate a informației şi al îmbunătățirilor		
Obiectiv: Să asigure o abordare consistentă şi eficientă a managementului incidentelor de securitate a informației, inclusiv comunicarea evenimentelor de securitate şi a slăbiciunilor		
A.16.1.1	Responsabilități şi proceduri	*Mijloc de control* Responsabilitățile şi procedurile de management trebuie stabilite pentru a asigura un răspuns rapid, eficient şi sistematic la incidentele de securitate a informației.

A.16.1.2	Raportarea evenimentelor de securitate a informației.	*Mijloc de control* Evenimentele de securitate a informației trebuie raportate prin canale de management corespunzătoare, cât mai curând posibil.
A.16.1.3	Reportarea slăbiciunilor de securitate a informației	*Mijloc de control* Angajaților şi contractanților care utilizează sistemele şi serviciile informaționale ale organizației trebuie să li se ceară să noteze şi să raporteze orice slăbiciune de securitate a informației observată sau suspectată în cadrul sistemelor sau a serviciilor.
A.16.1.4	Evaluarea şi decizia asupra evenimentelor de securitate a informației	*Mijloc de control* Evenimentele de securitate a informației trebuie evaluate şi trebuie să se ia decizia dacă ele trebuie să fie clasificate drept incidente de securitate a informației.
A.16.1.5	Răspunsul la incidente de securitate a informației	*Mijloc de control* Incidentelor de securitate a informației trebuie să li se răspundă în conformitate cu procedurile documentate.
A.16.1.6	Învățarea din incidentele de securitate a informației	*Mijloc de control* Cunoştințele dobândite din analizarea şi rezolvarea incidentelor de securitate a informației trebuie utilizate pentru a reduce plauzibilitatea sau impactul incidentelor viitoare.
A.16.1.7	Colectarea probelor	*Mijloc de control* Organizația trebuie să definească şi să aplice proceduri pentru identificarea, colectarea, achiziția şi păstrarea informațiilor care pot servi drept probe.
A.17 Aspecte ale securității informației pentru managementul continuității afacerii		
A.17.1 Continuitatea securității informației		
Obiectiv: Continuitatea securității informației trebuie inclusă în sistemele organizației pentru managementul continuității afacerii.		
A.17.1.1	Planificarea continuității securității informației	*Mijloc de control* Organizația trebuie să determine cerințele sale referitoare la securitatea informației şi la continuitatea managementului securității informației în situații potrivnice, de exemplu, în timpul unei crize sau a unui dezastru.
A.17.1.2	Implementarea continuității securității informației	*Mijloc de control* Organizația trebuie să stabilească, să documenteze, să implementeze şi să întrețină procese, proceduri şi mijloace de control pentru asigurarea nivelului cerut de continuitate pentru securitatea informației în timpul situațiilor potrivnice.
A.17.1.3	Verificarea, revizuirea şi evaluarea continuității securității informației	*Mijloc de control* Organizația trebuie să verifice la intervale regulate mijloacele de control pentru continuitatea securității informației stabilite şi implementate, pentru a se asigura că ele sunt valide şi eficiente în timpul situațiilor potrivnice.
A.17.2 Redundanțe		
Obiectiv: Să asigure disponibilitatea mijloacelor pentru prelucrarea informațiilor.		
A.17.2.1	Disponibilitatea mijloacelor pentru prelucrarea informațiilor	*Mijloc de control* Mijloacele pentru prelucrarea informației trebuie implementate cu o redundanță suficientă pentru a satisface cerințele de disponibilitate.

A.18 Conformitate		
A.18.1 Conformitatea cu cerințele legale şi contractuale		
Obiectiv: Evitarea încălcării obligațiilor legale, statutare, de reglementare şi contractuale referitoare la securitatea informației şi a oricăror cerințe de securitate.		
A.18.1.1	Identificarea legislației aplicabile şi a cerințelor contractuale	*Mijloc de control* Toate cerințele relevante statutare, de reglementare, contractuale precum şi abordarea organizației în vederea îndeplinirii acestor cerințe trebuie să fie identificate, documentate şi actualizate pentru fiecare sistem informațional şi pentru organizație.
A.18.1.2	Drepturile de proprietate intelectuală	*Mijloc de control* Trebuie implementate proceduri corespunzătoare pentru a asigura conformitatea cu cerințele legislative, de reglementare şi contractuale cu privire la drepturile de proprietate intelectuală şi la utilizarea produselor software proprietare.
A.18.1.3	Protejarea înregistrărilor	*Mijloc de control* Înregistrările trebuie protejate împotriva pierderii, distrugerii, falsificării, accesului neautorizat şi a transmiterii neautorizate a acestora în conformitate cu cerințele legislative, de reglementare, contractuale şi de afaceri.
A.18.1.4	Protecția datelor cu caracter personal şi confidențialitatea informațiilor personale	*Mijloc de control* Protecția datelor cu caracter personal şi confidențialitatea acestora trebuie să fie asigurată aşa cum este specificat în legislație şi reglementări, acolo unde este cazul.
A.18.1.5	Reglementări privind măsurile criptografice	*Mijloc de control* Mijloacele de control criptografice trebuie folosite în conformitate cu toate acordurile, legile şi reglementările aplicabile.
A.18.2 Revizuirea securității informației		
Obiectiv: Să asigure că securitatea informației este implementată şi aplicată în conformitate cu politicile şi procedurile organizaționale.		
A.18.2.1	Revizuirea independentă a securității informației	*Mijloc de control* Abordarea de către organizație a gestionării securității informației şi implementarea acesteia (adică obiective de control, mijloace de control, politici, procese şi proceduri pentru securitatea informației) trebuie revizuite în mod independent la intervale planificate sau când survin schimbări semnificative.
A.18.2.2	Conformitatea cu politicile şi standardele de securitate	*Mijloc de control* Managerii trebuie să revizuiască în mod regulat conformitatea procesării informației şi a procedurilor din aria lor de responsabilitate cu politicile de securitate, standardele şi orice alte cerințe de securitate corespunzătoare.
A.18.2.3	Revizuirea conformității tehnice	*Mijloc de control* Sistemele informaționale trebuie revizuite în mod regulat pentru conformitatea cu politicile şi standardele de securitate ale organizației.

Bibliografie

[1] *ISO/IEC 27002:2013, Information technology - Security Techniques - Code of practice for information security controls*

[2] *ISO/IEC 27003, Information technology - Security techniques - Information security management system implementation guidance*

[3] *ISO/IEC 27004, Information technology - Security techniques - Information security management - Measurement*

[4] *ISO/IEC 27005, Information technology - Security techniques - Information security risk management*

[5] *ISO 31000:2009, Risk management - Principles and guidelines*

[6] *ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 2012*

(Pagină albă)

ASRO – Asociația de Standardizare din România

organismul național de standardizare cu atribuții exclusive privind activitatea de standardizare națională şi reprezentarea României în procesul de standardizare european şi internațional.

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

Utilizatorii standardelor sunt răspunzători pentru interpretarea şi aplicarea corectă a prevederilor standardelor române.

Utilizarea standardelor române nu înlătură obligația respectării prevederilor legale în vigoare.

Informațiile referitoare la standardele române sunt publicate lunar în „Buletinul standardizării".

Lista şi datele bibliografice complete ale tuturor standardelor naționale, europene şi internaționale adoptate în România, în vigoare şi anulate, se regăsesc în aplicația electronică *Infostandard*, care se achiziționează de la ASRO.

ASOCIAȚIA DE STANDARDIZARE DIN ROMÂNIA

www.standardizarea.ro http//magazin.asro.ro http://standardizare.wordpress.com/

Director General: Tel.: +40 21 316 32 96, Fax: +40 21 316 08 70
Standardizare: Tel. +40 21 310 17 29, +40 21 310 16 44, +40 21 312 47 44, Fax: +40 21 310 17 29
Vânzări/Abonamente: Tel. +40 21 316 77 25, Fax + 40 21 317 25 14, +40 21 312 94 88; vanzari@asro.ro
Redacție – Marketing, Drepturi de Autor: Tel. : +40 21 316.99.74; marketing@asro.ro