ISO/IEC 27001:2022 — Securitatea informației, securitatea cibernetică și protecția vieții private – Sisteme de management al securității informației – Cerințe

În data de 25 octombrie 2022, ISO a publicat noua versiune a standardului ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Principalele modificări ale ISO/IEC 27001:2022

ISO/IEC 27001:2022 nu este o ediție complet revizuită. Principalele sale modificări includ, dar nu se limitează la:

1) Modificarea anexei A care a preluat mijloacele de control din ISO/IEC 27002:2022;
2) Notele clauzei 6.1.3 c) sunt revizuite editorial, inclusiv ștergerea obiectivelor aferente mijloacelor de control și utilizarea termenului de "mijloc de control a securității informațiilor" pentru a înlocui termenul "mijloc de control ";
3) Reformularea clauzei 6.1.3 d) pentru a elimina ambiguitatea potențială.
4) Adăugarea unui nou punct 4.2 c) pentru a determina cerințele părților interesate abordate într-un SMSI;
5) Adăugarea unei nou subclauze 6.3-Planificarea modificărilor, care precizează ca modificările aduse SMSI, trebuie efectuează de către organizație într-o manieră planificată;
6) Menținerea coerenței verbului utilizat în legătură cu informațiile documentate, de exemplu, utilizarea " informațiilor documentate trebuie să fie disponibilă ca dovadă a XXX" din clauzele 9.1, 9.2.2, 9.3.3 și 10.2;
7) Utilizarea expresiei "procese, produse sau servicii furnizate din exterior" pentru a înlocui "procesele externalizate" din clauza 8.1 și ștergerea termenului "externalizare";
8) Denumirea și reordonarea subclauzelor din clauzele 9.2-Audit intern (Divizarea 9.2 în 9.2.1 Generalități / 9.2.2 Programul de audit) si 9.3-Analiza efectuata de management Divizarea 9.3 în 9.3.1 Generalități / 9.3.2 Intrări ale AEM / 9.3.3 Ieșiri ale AEM);
9) Schimbarea ordinii celor două subclauze din clauza 10-Îmbunătățire;
10) Actualizarea ediției documentelor enumerate în Bibliografie, cum ar fi ISO/IEC 27002 și ISO 31000;
11) Unele abateri din ISO/IEC 27001:2013 de la structura de nivel înalt, textul de bază identic, termenii comuni și definițiile de bază ale standardelor pentru sisteme de management sunt revizuite pentru a menține conformitatea cu structura armonizată prevăzută in Anexa SL, de exemplu, clauza 6.2 d).

Nota 1: Primele două elemente provin din ISO/IEC 27001:2013/AMD1:2022, ultimul element fiind din ISO/IEC 27001:2013/COR 2:2015, al treilea este din ISO/IEC 27001:2013/COR 2:2015 , iar celelalte modificări rezultă din structura armonizată prevăzută de Anexa SL.

Nota 2: Comparativ cu ediția veche, numărul de mijloace de control din ISO/IEC 27002:2022 scade de la 114 mijloace de control în 14 grupe la 93 de mijloace de control în 4 grupe (11 mijloace de control sunt noi, 24 de mijloace de control sunt îmbinate din mijloacele de control existente și 58 de mijloace de control sunt actualizate).

În plus, structura mijloacelor de control este revizuită, s-au introdus "atribute" și "scop" pentru fiecare mijloc de control și nu se mai utilizează "obiectiv" pentru un grup de mijloace de control

Nota 3: ISO/IEC 27001:2013/COR 1:2014 este legată de anexa A și suprapusă cu ISO/IEC 27001:2013/AMD1:2022.

Impactul real al modificărilor din ISO/IEC 27001:2022 include, dar nu se limitează la introducerea unei noi anexe A și a clauzei 6.3-Planificarea modificărilor, deoarece:

1) ISO/IEC 27001:2013/COR 2:2015 a fost deja publicat și implementat;
2) Anexa A este normativă.
3) Structura armonizată conform Anexei SL este considerată o revizuire minoră pentru structura de nivel înalt, textul de bază identic, termenii comuni și definițiile de bază ale standardelor pentru sisteme de management, majoritatea modificărilor făcute sunt considerate editoriale.

În concluzie, impactul ISO/IEC 27001:2022 asupra organizațiilor care au implementat ISMS nu va fi semnificativ, dar va fi necesară reeditarea Declarațiilor de aplicabilitate, pentru a răspunde noilor cerințe.

Restructurarea mijloacelor de control

Există 93 de mijloace de control în versiunea std 2022, în timp ce în versiunea std 2013 au fost 114.

11 mijloace de control sunt noi, 24 provin din combinarea a 57 mijloace control existente și 58 mijloace de control sunt actualizate (23 au numele schimbat șii 35 au rămas aceleași, doar li s-a schimbat numărul).

Un singur mijloc de control 18.2.3 *Technical compliance review* a fost împărțit în două: *5.36 Conformance with policies, rules and standards for information security* si *8.8 Management of technical vulnerabilities*.

Nu s-a renunțat la niciun mijloc de control din cele precizate in ediția din 2013.

Mijloacele de control sunt regrupate în 4 categorii, în loc de 14 categorii care erau în versiunea 2013.

1. Mijloace de control organizaționale - un grup mare de 37 de mijloace de mijloc de control care nu se încadrează perfect în temele rămase si care au legătură mai degrabă cu activități organizaționale;
2. Mijloace de control aferente persoanelor - 8 mijloace de mijloc de control care implică sau au legătură cu resursele umane, de exemplu comportamente, activități, roluri și responsabilități ale persoanelor, termeni și condiții de angajare etc.;
3. Mijloace control fizice - 14 mijloace de control aferente mediului fizic, securității activelor tangibile
4. Mijloace de control tehnologice - 34 de mijloace de control care implică sau se referă la soluții tehnologice, în special IT

Mijloace de control nou introduse

11 noi mijloace de control sunt introduse pentru a reflecta evoluția tehnologiilor și practicilor industriale.

Extinderea utilizării tehnologiei și protecției datelor	Includerea mijloacelor de control aferente datelor sensibile	Recunoașterea rolului esențial al tehnologiei în reziliența afacerilor	Alte mijloace de control noi
5.7 Informații privind amenințările	8.10 Ștergerea informațiilor	5.30 Pregătirea IT&C pentru continuitatea afacerii	7.4 Supravegherea securității fizice
5.23 Securitatea informației pentru utilizarea serviciilor cloud	8.11 Mascarea datelor		8.9 Managementul configurației
8.12 Prevenirea scurgerii de date			8.16 Activități de supraveghere
			8.23 Filtrare web
			8.28 Codare securizată

ISO/IEC 27001:2022 — Securitatea informației, securitatea cibernetică și protecția vieții private – Sisteme de management al securității informației – Cerințe

Corespondența dintre mijloacele de control din ISO/IEC 27001:2022 și mijloacele de control din ISO/IEC 27002:2013

Identificator al mijlocului de control ISO/IEC 27001:2022	Identificator al mijlocului de control ISO/IEC 27001:2013	Nume mijloc de control
Mijloace de control organizaționale		
5.1	05.1.1, 05.1.2	Politici de securitate a informației
5.2	06.1.1	Roluri și responsabilități privind securitatea informației
5.3	06.1.2	Separarea sarcinilor
5.4	07.2.1	Responsabilitățile managementului
5.5	06.1.3	Contact cu autoritățile
5.6	06.1.4	Contact cu grupuri speciale de interese
5.7	Nou	Informații privind amenințările
5.8	06.1.5, 14.1.1	Securitatea informației în managementul de proiect
5.9	08.1.1, 08.1.2	Inventarul informațiilor și al altor active asociate
5.10	08.1.3, 08.2.3	Utilizarea acceptabilă a informațiilor și a altor active asociate
5.11	08.1.4	Restituirea activelor
5.12	08.2.1	Clasificarea informației
5.13	08.2.2	Etichetarea informației
5.14	13.2.1, 13.2.2, 13.2.3	Transferul informațiilor
5.15	09.1.1, 09.1.2	Controlul accesului
5.16	09.2.1	Managementul identității
5.17	09.2.4, 09.3.1, 09.4.3	Autentificarea informației
5.18	09.2.2, 09.2.5, 09.2.6	Drepturi de acces
5.19	15.1.1	Securitatea informației în relațiile cu furnizorii
5.20	15.1.2	Abordarea securității informației în cadrul acordurilor cu furnizorii
5.21	15.1.3	Managementul securității informației în lanțul de aprovizionare TIC
5.22	15.2.1, 15.2.2	Monitorizarea, analizarea și managementul schimbării serviciilor furnizorilor
5.23	Nou	Securitatea informației pentru utilizarea serviciilor cloud
5.24	16.1.1	Planificarea și pregătirea managementului incidentelor de securitate a informației
5.25	16.1.4	Evaluare și decizie cu privire la evenimentele de securitate a informației
5.26	16.1.5	Răspuns la incidentele de securitate a informației
5.27	16.1.6	Învățare din incidentele de securitate a informației
5.28	16.1.7	Colectarea dovezilor
5.29	17.1.1, 17.1.2, 17.1.3	Securitatea informației în timpul întreruperii

Identificator al mijlocului de control ISO/IEC 27001:2022	Identificator al mijlocului de control ISO/IEC 27001:2013	Nume mijloc de control
5.30	Nou	Pregătirea IT&C pentru continuitatea afacerii
5.31	18.1.1, 18.1.5	Cerințe legale, statutare, de reglementare și contractuale
5.32	18.1.2	Drepturi de proprietate intelectuală
5.33	18.1.3	Protecția înregistrărilor
5.34	18.1.4	Confidențialitatea și protecția PII (datelor cu caracter personal)
5.35	18.2.1	Revizuirea (Analizarea) independentă a securității informației
5.36	18.2.2, 18.2.3	Conformarea cu politicile, regulile și standardele pentru securitatea informației
5.37	12.1.1	Proceduri operaționale documentate
Mijloace de control aferente persoanelor		
6.1	07.1.1	Verificare
6.2	07.1.2	Termeni și condiții de angajare
6.3	07.2.2	Conștientizarea, educare și instruire cu privire la securitatea informației
6.4	07.2.3	Proces disciplinar
6.5	07.3.1	Responsabilități după încetarea sau schimbarea contractului de muncă
6.6	13.2.4	Acorduri de confidențialitate și nedezvăluire
6.7	06.2.2	Lucrul de la distanță
6.8	16.1.2, 16.1.3	Raportarea evenimentelor de securitate a informației
Mijloace de control fizice		
7.1	11.1.1	Perimetre de securitate fizică
7.2	11.1.2, 11.1.6	Intrarea fizică
7.3	11.1.3	Securizarea birourilor, încăperilor și echipamentelor
7.4	Nou	Supravegherea securității fizice
7.5	11.1.4	Protecția împotriva amenințărilor fizice și de mediu
7.6	11.1.5	Lucrul în zone securizate
7.7	11.2.9	Birou curat și ecran curat
7.8	11.2.1	Amplasarea și protecția echipamentelor
7.9	11.2.6	Securitatea activelor în afara sediului
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Suporturi de stocare
7.11	11.2.2	Utilități suport
7.12	11.2.3	Securitatea cablajului
7.13	11.2.4	Mentenanța echipamentelor
7.14	11.2.7	Eliminarea sau reutilizarea securizata echipamentelor

Identificator al mijlocului de control ISO/IEC 27001:2022	Identificator al mijlocului de control ISO/IEC 27001:2013	Nume mijloc de control
Mijloace de control tehnologice		
8.1	06.2.1, 11.2.8	Dispozitive terminale ale utilizatorului
8.2	09.2.3	Drepturi de acces privilegiat
8.3	09.4.1	Restricționarea accesului la informații
8.4	09.4.5	Acces la codul sursă
8.5	09.4.2	Autentificare securizată
8.6	12.1.3	Managementul capacității
8.7	12.2.1	Protecție împotriva malware
8.8	12.6.1, 18.2.3	Managementul vulnerabilităților tehnice
8.9	Nou	Managementul configurației
8.10	Nou	Ștergerea informațiilor
8.11	Nou	Mascarea datelor
8.12	Nou	Prevenirea scurgerii de date
8.13	12.3.1	Copie de siguranță a (backup) informației
8.14	17.2.1	Redundanța mijloacelor de prelucrare a informației
8.15	12.4.1, 12.4.2, 12.4.3	Înregistrare Logging
8.16	Nou	Activități de supraveghere
8.17	12.4.4	Sincronizarea ceasului
8.18	09.4.4	Utilizarea programelor utilitare privilegiate
8.19	12.5.1, 12.6.2	Instalarea software-ului pe sisteme operaționale
8.20	13.1.1	Securitatea rețelelor
8.21	13.1.2	Securitatea serviciilor de rețea
8.22	13.1.3	Separarea rețelelor
8.23	Nou	Filtrare web
8.24	10.1.1, 10.1.2	Utilizarea criptării
8.25	14.2.1	Ciclul de viață al dezvoltării securizate
8.26	14.1.2, 14.1.3	Cerințe de securitate a aplicației
8.27	14.2.5	Arhitectura sistemului securizat și principiile de inginerie
8.28	Nou	Codare securizată
8.29	14.2.8, 14.2.9	Testarea securității în dezvoltare și acceptare
8.30	14.2.7	Dezvoltare externalizată
8.31	12.1.4, 14.2.6	Separarea mediilor de dezvoltare, testare și operare
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Managementul modificărilor
8.33	14.3.1	Informație de testare
8.34	12.7.1	Protejarea sistemelor informaționale în timpul testării de audit

ISO 27002:2022 a introdus „atribute” și „scop” pentru fiecare mijloc de control și nu mai folosește „obiectiv” pentru un grup de mijloace de control .

Exista 5 seturi de "atribute":

1 Tipul de mijloc de control : Mijloacele de control sunt privite din perspectiva momentului și a modului în care mijlocul de control ul influențează rezultatul riscului în timpul unui incident de securitate a informațiilor. Aceste valori ale atributelor constau în:

a) Preventiv - mijlocul de control acționează preventiv înainte de apariția unei amenințări;

b) Detectiv - mijlocul de control acționează atunci când apare o amenințare;

c) Corectiv - mijlocul de control acționează după apariția unei amenințări.

Acest atribut poate ușura sarcina atunci când vine vorba de a face aceste determinări pe cont propriu și se poate utiliza, de asemenea, dacă se dorește să se verifice echilibrul mijloacelor de control stabilite. De exemplu, se poate utiliza pentru a verifica dacă s-au introdus mijloace de control adecvate pentru a detecta evenimentele de securitate a informațiilor, nu doar cele pentru a preveni incidentele de securitate a informațiilor.

2 Proprietăți de securitate a informațiilor: Mijloacele de control sunt privite din perspectiva cărei caracteristici a informației respectivul mijloc de control urmează să contribuie la protejare. Valorile atributelor constau în:

a) Confidențialitate

b) Integritate

c) Disponibilitate.

Acest atribut poate fi foarte util în timpul procesului de evaluare a riscurilor, deoarece luarea în considerare a atenuării riscurilor asociate cu confidențialitatea / integritatea / disponibilitatea este una dintre cerințele clauzei 6.1.2 din ISO 27001.

3 **Concepte de securitate cibernetică**: Mijloacele de control sunt privite din perspectiva asocierii mijloacelor de mijloc de la conceptele de securitate cibernetică definite în cadrul de securitate cibernetică descris în standardul ISO/IEC TS 27110. Aceste valori ale atributelor constau în:

a) Identificare

b) Protejare

c) Detectare

d) Răspuns

e) Recuperare.

Dacă se stabilește atât un cadru SMSI, cât și un cadru de securitate cibernetică, atunci acest atribut poate ajuta. Acesta poate prezenta relevanța dintre mijloacele de control SMSI descrise în standardul ISO 27001 și cele cinci concepte ale cadrului de securitate cibernetică descrise în ISO/IEC TS 27110.

4 Capacități operaționale: Mijloacele de control sunt privite din perspectiva unui practician asupra capabilităților cu privire la securitatea informațiilor. Să presupunem că dacă se dorește să se atribuie un risc sau un mijloc de control asociat departamentelor responsabile, se poate face acest lucru pe baza acestor valori ale atributelor (de Guvernanță, Management active, Protecție informație, Securitate resursă umană, Securitate fizică, Securitate sistem și rețea, Securitate aplicație, Configurare securizată, Management identitate și acces, Management amenințare și vulnerabilitate, Continuitate, Securitate relații furnizor, Legal (cerințe legale) și conformare, Management eveniment securitate informație și Asigurarea securității informație.

Se pot utiliza aceste subclasificări mai detaliate ale fiecărui mijloc de control pentru delimitarea sau atribuirea proprietarului riscului/mijlocului de control.

5 <u>Domenii de securitate:</u> Mijloacele de control sunt privite din perspectiva a patru domenii de securitate a informației:

a) „Guvernanță și ecosistem” care include „Guvernanța securității sistemului informațional & Managementul riscurilor” și „Managementul securității cibernetice a ecosistemului” (inclusiv părțile interesate interne și externe);
b) „Protecție” care include „Arhitectura de securitate IT”, „Administrarea securității IT”, „Identitate și managementul accesului”, „Mentenanța securității IT” și „Securitate fizică și de mediu”;
c) „Apărare” care include „Detectare” și „Managementul incidentelor privind securitatea informației”;
d) „Reziliență” care include „Continuitatea operațiilor” și „Managementul crizelor”.

Valorile atributelor constau în Guvernanță_și_Ecosistem, Protecție, Apărare și Reziliență

Atributele prezentate în acest document au fost alese deoarece sunt considerate suficient de generice pentru a fi utilizate de diferite tipuri de organizații. Organizațiile pot să aleagă să ignore unul sau mai multe dintre atributele prezentate în acest document. De asemenea, pot să creeze propriile atribute (cu valorile atributelor corespondente) pentru a-și crea propriile vederi organizaționale

Odată cu introducerea atributelor în standardul ISO 27002:2022, organizațiile pot utiliza procesul de analiza a propriului SMSI pentru a implementa atributele. Beneficiul atributelor, este posibilitatea de a crea diferite vizualizări sau clasificări ale mijloacelor de mijloc de control.

De exemplu, se pot vizualiza mijloacele de control din perspectiva tipurilor mijloacelor de control (Mijloace de control preventive, detective sau corective) sau se poate face acest lucru pe baza diferitelor proprietăți de securitate a informației (confidențialitate, integritate, disponibilitate) sau pe baza diferitelor capacități operaționale (guvernanță, identitate și gestionarea accesului, cerințe legale și conformare) etc.

Comentarii asupra mijloacelor de control noi

5.7 Informații privind amenințările

Tip de mijloc de control	Proprietăți ale securității informației	Concepte de securitate cibernetică	Capabilități operaționale	Domenii de securitate
#Preventiv #Detectiv #Crectiv	#Confidențialitate #Integritate #Disponibilitate	#Identificare #Detectare #Răspuns	#Management amenințări și vulnerabilități	#Apărare #Reziliență

Mijloc de control

Informațiile referitoare la amenințările privind securitatea informației trebuie să fie colectate și analizate pentru a rezulta informații referitoare la amenințări.

Scop

Să prevadă conștientizarea cu privire la mediul de amenințare a organizației, astfel încât să se poată lua măsurile de atenuare adecvate.

Observație:

Acest mijloc de control impune organizațiilor să colecteze și să analizeze informații despre amenințări și să le atenueze în mod corespunzător. Tipurile de informații ar putea include date despre atacuri specifice, metodele pe care le folosesc atacatorii și tipurile de atacuri. Informațiile ar trebui colectate intern și din surse externe, cum ar fi rapoartele furnizorilor, organismele guvernamentale și anunțurile din industrie.

5.23 Securitatea informației pentru utilizarea serviciilor cloud

Tip de mijloc de control	Proprietăți ale securității informației	Concepte de securitate cibernetică	Capabilități operaționale	Domenii de securitate
#Preventiv	#Confidențialitate #Integritate #Disponibilitate	#Protecție	#Securitate relații furnizor	#Guvernanță și Ecosistem #Protecție

Mijloc de control

Procesele de achiziție, utilizare, management și ieșire din serviciile cloud trebuie să fie stabilite în conformitate cu cerințele de securitate a informației ale organizației.

Scop

Să specifice și să gestioneze securitatea informației pentru utilizarea serviciilor cloud.

Observație:

Este necesar ca cerințele de securitate pentru serviciile cloud să fie stabilite pentru protecția informațiilor din cloud. În acest mijloc de control ar trebui să fie incluse politici privind achiziția, utilizarea, managementul și încetarea utilizării serviciilor cloud.

5.30 Pregătirea IT&C pentru continuitatea afacerii

Tip de mijloc de control	Proprietăți ale securității informației	Concepte de securitate cibernetică	Capabilități operaționale	Domenii de securitate
#Corectiv	#Disponibilitate	#Răspuns	#Continuitate	#Reziliență

Mijloc de control

Pregătirea IT&C trebuie să fie planificată, implementată, menținută și testată pe baza obiectivelor de continuitate a activității și a cerințelor de continuitate TIC.

Scop

Să asigure disponibilitatea informațiilor organizației și a altor active asociate în timpul întreruperii.

Observație:

Acest mijloc de control cere ca oamenii, procesele și sistemele să fie pregătite în caz de perturbări, astfel încât informațiile și activele esențiale să fie disponibile atunci când este necesar.

7.4 Supravegherea securității fizice

Tip de mijloc de control	Proprietăți ale curității informației	Concepte de curitate cibernetică	Capabilități operaționale	Domenii de securitate
#Preventiv #Detectiv	#Confidențialitate #Integritate #Disponibilitate	#Protejare #Detectare	#Securitate_fizică	#Protecție #Apărare

Mijloc de control

Clădirile trebuie să fie supravegheate continuu având în vedere accesul fizic neautorizat.

Scop

Să detecteze și să descurajeze accesul fizic neautorizat.

Observație:

Zonele sensibile trebuie monitorizate pentru a se asigura că numai personalul autorizat le poate accesa. Aceasta ar putea include birouri, facilități de producție, depozite și alte spații fizice cheie.

8.9 Managementul configurației

Tip de mijloc de control	Proprietăți ale securității informației	Concepte de securitate cibernetică	Capabilități operaționale	Domenii de securitate
#Preventiv	#Confidențialitate #Integritate #Disponibilitate	#Protejare	#Configurare securizare	#Protecție

Mijloc de control

Configurațiile, inclusiv configurațiile de securitate, ale hardware-ului, software-ului, serviciilor și rețelelor trebuie să fie stabilite, documentate, implementate, supravegheate și revizuite.

Scop

Să asigure că hardware-ul, software-ul, serviciile și rețelele să funcționeze corect cu setările de securitate necesare și ca configurația să nu fie modificată de modificări neautorizate sau incorecte.

Observație:

Se cere sa existe un management al configurației tuturor echipamentelor, pentru toate tehnologiile si sistemele existenta.

8.10 Ștergerea informațiilor

Tip de mijloc de control	Proprietăți ale securității informației	Concepte de securitate cibernetică	Capabilități operaționale	Domenii de securitate
#Preventiv	#Confidențialitate	#Protejare	#Protecție informație #Cerinte legale și conformare	#Protecție

Mijloc de control

Informațiile stocate în sistemele informaționale, pe dispozitive sau pe orice alt suport de stocare trebuie să fie șterse atunci când nu mai sunt necesare.

Scop

Să prevină expunerea inutilă a informațiilor sensibile și să respecte cerințele legale, statutare, de reglementare și contractuale pentru ștergerea informațiilor.

Observație:

Este abordata ștergerea datelor atunci când nu mai sunt necesare sau când timpii de stocare depășesc perioadele de păstrare documentate. Intenția este de a mijloc de control a potențialul de scurgere a datelor sensibile și de a respecta orice cerințe relevante privind confidențialitatea și alte cerințe. Ștergerile ar putea include date în sisteme IT, suporturi amovibile sau servicii cloud.

8.11 Mascarea datelor

Tip de mijloc de control	Proprietăți ale securității informației	Concepte de securitate cibernetică	Capabilități operaționale	Domenii de securitate
#Preventiv	#Confidențialitate	#Protejare	#Protecție informație	#Protecție

Mijloc de control

Mascarea datelor trebuie să fie utilizată în conformitate cu politica organizației privind controlul accesului și alte politici pe subiecte specifice și cu cerințele de afaceri, ținând cont de legislația aplicabilă.

Scop

Să se limiteze expunerea datelor sensibile, inclusiv a datelor cu caracter personal și să se respecte cerințele legale, statutare, de reglementare și contractuale.

Observație:

Acest mijloc de control necesită ca mascarea datelor să fie utilizată în combinație cu mijloace de control ale accesului adecvate pentru a reduce probabilitatea expunerii la informații sensibile. Acest mijloc de control se concentrează în special pe datele cu caracter personal, deoarece acest lucru este puternic reglementat prin intermediul reglementărilor privind confidențialitatea, dar si altor și altor forme de date sensibile, relevante pentru organizație.

8.12 Prevenirea scurgerii de date

Tip de mijloc de control	Proprietăți ale securității informației	Concepte de securitate cibernetică	Capabilități operaționale	Domenii de securitate
#Preventiv	#Confidențialitate	#Protejare #Detectare	#Protecție informație	#Protecție #Apărare

Mijloc de control

Măsurile de prevenire a scurgerii datelor trebuie să se aplice sistemelor, rețelelor și oricăror alte dispozitive care prelucrează, stochează sau transmit informații sensibile.

Scop

Să detecteze și să prevină dezvăluirea și extragerea neautorizată a informațiilor de persoane sau sisteme.

Observație:

Acest mijloc de control necesită aplicarea prevenirii scurgerilor de date prin măsuri adecvate pentru a evita divulgarea neautorizată a informațiilor sensibile. Măsurile de prevenire a scurgerii datelor ar trebui să se aplice sistemelor, rețelelor și oricăror alte dispozitive care prelucrează, stochează sau transmit informații sensibile Aceasta acoperă, de asemenea, includerea măsurilor de detectare a incidentelor în timp util.

8.16 Activități de supraveghere

Tip de mijloc de control	Proprietăți ale securității informației	Concepte de securitate cibernetică	Capabilități operaționale	Domenii de securitate
#Detectiv #Corectiv	#Confidențialitatea #Integritate #Disponibilitate	#Detectare #Răspuns	#Management eveniment securitate informație	#Apărare

Mijloc de control

Rețelele, sistemele și aplicațiile trebuie monitorizate pentru comportamentul anormal și trebuie luate masuri adecvate pentru a evalua potențialele incidente privind securitatea informației.

Obiectiv

Să detecteze comportamentul anormal și potențialele incidente privind securitatea informației.

Observație:

Acest mijloc de control necesită managementul și monitorizarea rețelelor, sistemelor și aplicațiilor pentru comportamentul anormal și se recomandă luarea de măsuri adecvate pentru a evalua potențialele incidente privind securitatea informației.

8.23 Filtrare web

Tip de mijloc de control	Proprietăți ale securității informației	Concepte de securitate cibernetică	Capabilități operaționale	Domenii de securitate
#Preventiv	#Confidențialitate #Integritate #Disponibilitate	#Protejare	#Securitate sistem și rețea	#Protecție

Mijloc de control

Trebuie sa se aplice un management al accesului la site-uri web externe pentru a reduce expunerea la un conținut rău intenționat.

Obiectiv

Să protejeze sistemele de a nu fi compromise de programe malware și să prevină accesul la resurse web neautorizate.

Observație:

Acest mijloc de control presupune managementul accesului la site-uri web externe pentru a reduce expunerea la un conținut rău intenționat.

8.28 Codare securizată

Tip de mijloc de control	Proprietăți ale securității informației	Concepte de securitate cibernetică	Capabilități operaționale	Domenii de securitate
#Preventiv	#Confidențialitate #Integritate #Disponibilitate	#Protejare	#Securitate aplicație #Securitate sistem și rețea	#Protecție

Mijloc de control

Trebuie aplicate principiile de codare securizată a dezvoltării software.

Scop

Să asigure că software-ul este scris securizat, reducând astfel numărul potențialelor vulnerabilități de securitate a informațiilor din software.

Observație:

Se recomandă aplicarea principiilor de codare securizată dezvoltării software, astfel incat să se asigure că software-ul este scris securizat, reducând astfel numărul potențialelor vulnerabilități de securitate a informațiilor din software.

ISO/IEC 27001:2022 — Securitatea informației, securitatea cibernetică și protecția vieții private – Sisteme de management al securității informației – Cerințe

Calendarul tranziției a fost stabilit in documentul IAF MD 26:2022 după cum urmează:

Perioada de tranziție este de 3ani, adică se va finaliza la 31.10.2025.

Activitate	Termen
Organismul de acreditare (OA)	
OA va fi gata să evalueze ISO/IECIEC 27001: 2022 nu mai târziu de	6 luni de la ultima zi a lunii de publicare a ISO/IEC 27001:2022 (adică 30 aprilie 2023)
Evaluarea inițială de către OC conform ISO/IEC 27001:2022 va începe cel târziu	6 luni de la ultima zi a lunii de publicare a ISO/IEC 27001:2022 (adică 30 aprilie 2023)
Tranzițiile acreditarilor OC in vigoare vor fi finalizate de OA in	12 luni de la ultima zi a lunii de publicare a ISO/IEC 27001:2022 (adică 31 octombrie 2023)
Organismul de certificare acreditat (OC)	
Certificările inițiale ale SMSI de către OC conform ISO/IEC 27001: 2022 vor începe cel târziu la	12 luni de la ultima zi a lunii de publicare a ISO/IEC 27001:2022 (adică 31 octombrie 2023)
Tranziția certificărilor SMSI ale clienților certificați de CO vor fi finalizate in maxim	36 de luni de la ultima zi a lunii de publicare a ISO/IEC 27001:2022 (adică 31 octombrie 2025)

Auditul SMSI pentru efectuarea tranziției

OC poate efectua auditul de tranziție împreună cu auditul de supraveghere, auditul de recertificare sau printr-un audit separat.

Auditul de tranziție trebuie sa nu realizeze doar prin analiza documentelor, în special pentru analiza masurilor de control.

Auditul de tranziție trebuie să includă, fără însă să se limiteze la următoarele:

- analiza GAP a modificărilor din ISO/IEC 27001:2022, precum și necesitatea modificării SMSI al clientului;
- actualizarea declarației de aplicabilitate (SoA);
- dacă este cazul, actualizarea planului de tratare al riscurilor;
- implementarea și eficacitatea mijloacelor de controalelor aferente securității informațiilor noi sau modificate alese de clienți.

OC poate efectua o parte a auditului de tranziție de la distanță dacă se asigură că obiectivele auditului de tranziție sunt îndeplinite.

Va fi necesar un timp suplimentar pentru tranziția certificărilor SMSI astfel:

- Minim 0,5 zile auditor pentru auditul de tranziție atunci când este efectuat împreună cu un audit de recertificare
- Minim 1,0 zile auditor pentru auditul de tranziție atunci când acesta este efectuat împreună cu un audit de supraveghere sau ca un audit separat.

Dr. ing. Cristian RONCEA

26.10.2022