Mecanisme de audit și control

Soluții de gestionare a securității datelor și informației

Controale de securitate a informației

Securitatea informațiilor, securitatea cibernetică și protecția vieții private

Principii de lucru

- ✓ISO 27002[1] este conceput pentru organizații de toate tipurile și dimensiunile și trebuie utilizat ca referință pentru determinarea și implementarea controalelor pentru tratarea riscurilor de securitate a informațiilor într-un sistem de management al securității informațiilor (SMSI) bazat pe ISO/IEC 27001;
- ✓poate fi, de asemenea, utilizat ca document de orientare pentru organizațiile care determină și implementează în mod obișnuit controale de securitate a informațiilor;
- ✓în plus, acest document este destinat utilizării în elaborarea de linii directoare de management al securității informațiilor specifice industriei și organizației, ținând cont de mediul (mediile) specifice de risc pentru securitatea informațiilor;
- ✓controalele organizaționale sau specifice mediului, altele decât cele incluse în acest document, pot fi determinate prin evaluarea riscurilor, dacă este necesar;
- ✓un sistem de management al securității informațiilor adecvat și eficient oferă conducerii organizației și altor părți interesate asigurarea că informațiile lor și alte active asociate sunt păstrate în mod rezonabil în siguranță și protejate împotriva amenințărilor și daunelor, permițând astfel organizației să atingă obiectivele de afaceri declarate;
- ✓SMSI necesită sprijin din partea întregului personal din organizație, precum și a altor părți interesate (acționarii, furnizorii) sau consultanță de la experți în domeniu.

Activități de management și procese organizaționale

Controalele de securitate a datelor și informației se realizează prin:

- ➡ implementarea unui set adecvat de politici, reguli, procese, proceduri, structuri organizaționale și funcții software și hardware.
- ➡ implementarea monitorizarea, revizuirea și îmbunătățirea mecanismelor manageriale, în cadrul unui sistem coerent, pentru îndeplinirea obiectivelor specifice de securitate și de afaceri:
  - ➡ ISO 27001 stabilește o viziune coordonată asupra riscurilor organizației pentru securitatea informațiilor, pentru a determina și implementa o suită cuprinzătoare de controale de securitate a datelor și informației;
- ➡ activități de management și procese organizaționale adecvate, deoarece nivelul de securitate al multor sisteme informatice care poate fi atins doar prin măsuri tehnologice este limitat (nu au fost concepute pentru a fi sigur în ceea ce privește SMSI):
  - ➡ identificarea controalelor necesare a fi puse în aplicare necesită o planificare minuțioasă și atenție la detalii în timpul tratării riscurilor.

Cerințe de securitate a datelor și informațiilor

Există trei surse principale de cerințe de securitate a datelor și informațiilor într-o organizație:

(a) evaluarea riscurilor pentru organizație, ținând cont de strategia generală de afaceri și obiectivele organizației:

(1) analiza poate fi facilitată sau susținută printr-o evaluare a riscurilor specifice securității informațiilor.

(2) evaluarea trebuie să aibă ca rezultat determinarea controalelor necesare pentru a se asigura că riscul rezidual pentru organizație îndeplinește criteriile sale de acceptare a riscurilor;

(b) cerințele legale, statutare, de reglementare și contractuale pe care trebuie să le respecte o organizație și părțile sale interesate (parteneri comerciali, furnizori de servicii etc.) și mediul lor socio-cultural;

(c) setul de principii, obiective și cerințe de afaceri pentru toate etapele ciclului de viață al informațiilor pe care o organizație le-a dezvoltat pentru a-și susține operațiunile.

Noțiuni despre controale

Controale de securitate
Un control este definit ca o măsură care modifică sau menține riscul:
- unele dintre controalele modifică riscul (de ex.: respectarea politicii de securitate a informațiilor poate modifica riscul);
- alte controale mențin riscul - o politică de securitate a informațiilor, de exemplu, poate menține riscul;

Mai mult, unele controale descriu aceeași măsură generică în diferite contexte de risc. Standardul ISO 27002 oferă un amestec generic de controale de securitate a informațiilor organizaționale, umane, fizice și tehnologice derivate din cele mai bune practici recunoscute la nivel internațional.

Determinarea controalelor
Determinarea controalelor depinde de:
(a) deciziile organizației în urma unei evaluări a riscurilor, cu un domeniu de aplicare clar definit, care trebuie să se bazeze pe:
(1)criteriile de acceptare a riscurilor,
(2)opțiunile de tratare a riscurilor și
(3)abordarea de gestionare a riscurilor aplicată de organizație.
(b) legislațiile și reglementările naționale și internaționale relevante;
(c) modul în care controalele interacționează între ele pentru a oferi apărare în profunzime;
(d) resursele și investițiile necesare pentru implementarea și operarea unui control față de valoarea afacerii realizată:
(1)ISO/IEC TR 27016 conține îndrumări privind deciziile privind investiția într-un SMSI și consecințele economice ale acestor decizii în contextul cerințelor concurente pentru resurse;
(2)trebui să existe un echilibru între resursele desfășurate pentru implementarea controalelor și impactul potențial pe afaceri care rezultă din incidentele de securitate în absența acestor controale.

Rezultatele unei evaluări a riscurilor trebuie să ajute la:
(1) ghidarea acțiunii adecvate de management,
(2) determinarea priorităților pentru gestionarea riscurilor de securitate a informațiilor și
(3) implementarea controalelor considerate necesare pentru a proteja împotriva acestor riscuri.
ISO/IEC 27005 conține informații despre determinarea controalelor și a altor opțiuni de tratare a riscurilor.

Ciclul de viață al datelor

Elaborarea liniilor directoare specifice organizației

Trebuie să țină seama de:

- nu toate controalele și îndrumările din standard pot fi aplicabile tuturor organizațiilor;
- pot fi solicitate controale și orientări suplimentare care nu sunt incluse pentru a aborda nevoile specifice ale organizației și riscurile care au fost identificate;
- când sunt elaborate documente care conțin orientări sau controale suplimentare, poate fi util să se includă referințe încrucișate la clauze din acest document pentru referințe viitoare.

Considerații privind ciclul de viață

Informația are un ciclu de viață, de la creare până la eliminare. Valoarea și riscurile pentru informații pot varia pe parcursul acestui ciclu de viață:

- de exemplu, dezvăluirea neautorizată sau furtul conturilor financiare ale unei companii nu sunt semnificative după ce au fost publicate, dar integritatea rămâne critică;
- prin urmare, securitatea informațiilor rămâne importantă într-o oarecare măsură la toate etapele.

Sistemele informaționale și alte active relevante pentru securitatea informațiilor:

- au cicluri de viață în care sunt concepute, specificate, proiectate, dezvoltate, testate, implementate, utilizate, întreținute și eventual scoase din funcțiune și eliminate;
- securitatea informațiilor ar trebui luată în considerare în fiecare etapă;
- controalele de securitate pot fi îmbunătățite prin noile proiecte de dezvoltare ale sistemelor și ținând cont de riscurile organizației și lecțiile învățate din incidente.

Standarde internaționale conexe

Alte documente din familia ISO/IEC 27000 oferă sfaturi sau cerințe complementare cu privire la alte aspecte ale procesului general de gestionare a securității informațiilor:

- ISO/IEC 27000 conține o introducere generală atât la SMSI, cât și la familia de documente și oferă un glosar, care definește majoritatea termenilor utilizați în întreaga familie de documente ISO/IEC 27000 și descrie domeniul de aplicare și obiectivele pentru fiecare membru al familiei;
- există standarde specifice sectorului care au controale suplimentare care urmăresc să abordeze domenii specifice:
    - ISO/IEC 27017 pentru servicii cloud,
    - ISO/IEC 27701 pentru confidențialitate,
    - ISO/IEC 27019 pentru energie,
    - ISO/IEC 27011 pentru organizațiile de telecomunicații și
    - ISO 27799 pentru sănătate.

Auditul securității datelor. Rolul controlului

Auditul securității informației:

- are loc atunci când o echipă tehnologică efectuează o revizuire organizațională pentru a se asigura că sunt aplicate procesele și infrastructura corecte și cele mai actualizate;
- include o serie de teste care garantează că securitatea informațiilor îndeplinește toate așteptările și cerințele din cadrul unei organizații;
- în timpul acestui proces, angajații sunt intervievați cu privire la rolurile de securitate și alte detalii relevante [2];
- este o formă de control subordonată consiliului de administrație cu rol de a asigura atingerea obiectivelor companiei, printr-o abordare bazată pe riscuri și axată pe controale [3].

Tipul controlului

Este un atribut pentru vizualizarea controalelor din perspectiva când și cum modifică controlul riscul în ceea ce privește apariția unui incident de securitate a informației.

Valorile atributelor constau în:

- **preventiv -** controlul are ca scop prevenirea apariția unui incident de securitate a informațiilor;
- **detectiv -** controlul se realizează atunci când are loc un incident de securitate a informațiilor;
- **corectiv -** controlul se realizează după ce are loc un incident de securitate a informațiilor.

Scopul controlului intern este de atenuare a riscurilor prin controale adecvate și asigurare rezonabilă că societatea nu este împiedicată în atingerea obiectivelor.

Clasificarea controalelor, conform clauzelor ISO 27002

5. Controale organizaționale

5.1 Politici pentru securitatea informațiilor
5.2 Roluri și responsabilități în materie de securitate a informațiilor
5.3 Separarea sarcinilor
5.4 Responsabilitățile managementului
5.5 Contactul cu autoritățile
5.6 Contactul cu grupuri de interese speciale
5.7 Informații despre amenințări
5.8 Securitatea informației în managementul proiectelor
5.9 Inventarul informațiilor și al altor active asociate
5.10 Utilizarea acceptabilă a informațiilor și a altor active asociate
5.11 Returnarea activelor
5.12 Clasificarea informațiilor
5.13 Etichetarea informațiilor
5.14 Transferul de informații
5.15 Controlul accesului
5.16 Managementul identității
5.17 Informații de autentificare
5.18 Drepturi de acces
5.19 Securitatea informațiilor în relațiile cu furnizorii
5.20 Abordarea securității informațiilor în cadrul acordurilor cu furnizorii
5.21 Gestionarea securității informațiilor în lanțul de aprovizionare în Tehnologia Informațiilor și Comunicațiilor (TIC)
5.22 Monitorizare, revizuire și managementul schimbării serviciilor furnizorilor
5.23 Securitatea informațiilor pentru utilizarea serviciilor cloud
5.24 Planificarea și pregătirea managementului incidentelor de securitate a informațiilor
5.25 Evaluare și decizie privind evenimentele de securitate a informațiilor
5.26 Răspuns la incidente de securitate a informațiilor
5.27 Învățare din incidentele de securitate a informațiilor
5.28 Colectarea probelor
5.29 Securitatea informațiilor în timpul întreruperii
5.30 Pregătirea TIC pentru continuitatea afacerii
5.31 Cerințe legale, statutare, de reglementare și contractuale
5.32 Drepturi de proprietate intelectuală
5.33 Protecția înregistrărilor
5.34 Confidențialitate și protecția persoanelor fizice
5.35 Revizuirea independentă a securității informațiilor
5.36 Respectarea politicilor, regulilor și standardelor pentru securitatea informațiilor
5.37 Proceduri de operare documentate

Clasificarea controalelor, conform clauzelor ISO 27002

6. Controlul persoanelor

6.1 Screening
6.2 Termeni și condiții ale angajare
6.3 Conștientizarea, educația și formarea în domeniul securității informațiilor
6.4 Procesul disciplinar
6.5 Responsabilități după încetarea sau schimbarea locului de muncă
6.6 Acorduri de confidențialitate sau de nedezvăluire
6.7 Lucrul de la distanță
6.8 Raportarea evenimentelor de securitate a informațiilor

7. Controale fizice

7.1 Perimetrele de securitate fizică
7.2 Intrarea fizică
7.3 Securizarea birourilor, încăperilor și facilităților
7.4 Monitorizarea securității fizice
7.5 Protecția împotriva amenințărilor fizice și de mediu
7.6 Lucrul în zone securizate
7.7 Birou clar și ecran clar
7.8 Amplasarea și protecția echipamentelor
7.9 Securitatea activelor în afara sediului
7.10 Suporturi de stocare
7.11 Utilități de sprijin
7.12 Securitatea cablajului
7.13 Întreținerea echipamentului
7.14 Eliminarea sau reutilizarea în siguranță a echipamentelor

Clasificarea controalelor, conform clauzelor ISO 27002

8. Controale tehnologice

8.1 Dispozitive terminale ale utilizatorului
8.2 Drepturi de acces privilegiate
8.3 Restricționarea accesului la informații
4 8.4 Accesul la codul sursă
8.5 Autentificare securizată
8.6 Managementul capacității
8.7 Protecția împotriva programelor malware
8.8 Managementul vulnerabilităților tehnice
8.9 Gestionarea configurației
8.10 Ștergerea informațiilor
8.11 Mascarea datelor
8.12 Prevenirea scurgerilor de date
8.13 Copiere de rezervă a informațiilor
8.14 Redundanța facilităților de procesare a informațiilor
8.15 Înregistrare
8.16 Activități de monitorizare
8.17 Sincronizarea ceasului
8.18 Utilizarea programelor utilitare privilegiate
8.19 Instalarea software-ului pe operațional sisteme
8.20 Securitatea rețelelor
8.21 Securitatea serviciilor de rețea
8.22 Segregarea rețelelor
8.23 Filtrare web
8.24 Utilizarea criptografiei
8.25 Ciclul de viață al dezvoltării securizate
8.26 Cerințe de securitate a aplicației
8.27 Arhitectura sistemului sigur și principiile de inginerie
8.28 Codare securizată
8.29 Testare de securitate în dezvoltare și acceptare
8.30 Dezvoltare externalizată
8.31 Separarea mediilor de dezvoltare, testare și producție
8.32 Gestionarea modificărilor
8.33 Informații de testare
8.34 Protecția sistemelor informaționale în timpul testării de audit

Controlul protecției informațiilor clasificate

Asigurarea protejării informațiilor clasificate în România

Legea nr.182/2002. HG nr.585/2002

Cele două acte normative prevăd că:

(1) Serviciul Român de Informații, prin unitatea sa specializată (ORNISS), are competență generală de exercitare a controlului asupra modului de aplicare a măsurilor de protecție de către instituțiile publice și unitățile deținătoare de informații clasificate [4];

(2) Ministerul Apărării Naționale, Ministerul de Interne, Ministerul de Justiție, Serviciul Român de Informații, Serviciul de Informații Externe, Serviciul de Protecție și Pază și Serviciul de Telecomunicații Speciale stabilesc structuri și măsuri proprii de protecție a informațiilor secrete de stat, conform competențelor în domeniile de activitate și responsabilitate (coordonare și control);

(3) măsurile de protecție a informațiilor clasificate în cadrul Parlamentului, Administrației Prezidențiale, Guvernului și Consiliului Suprem de Apărare a țării se organizează conform legii, iar SRI acordă asistență de specialitate;

(4) activitatea de control în cadrul reprezentanțelor României în străinătate se reglementează și se realizează de către Serviciul de Informații Externe;

(5) Ministerul Apărării Naționale realizează, prin structura specializată, coordonarea activității și controlul măsurilor privitoare la protecția informațiilor secrete de stat pentru:

a. Oficiul Central de Stat pentru Probleme Speciale și Administrația Națională a Rezervelor de Stat;

b. activitatea specifica a atașaților militari din cadrul misiunilor diplomatice ale României și a reprezentanților militari pe lângă organismele internaționale [5].

Scopurile și clasificarea controalelor

Scopurile controlului

(a) evaluarea eficienței măsurilor concrete de protecție adoptate la nivelul deținătorilor de informații clasificate, în conformitate cu:
    (1) legea nr.182/2002;
    (2) prevederile Standardelor de protecție din HG nr.585/2002 și altor norme în materie, precum și
    (3) programele de prevenire a scurgerii de informații clasificate;
(b) identificarea vulnerabilităților existente în sistemul de protecție a informațiilor clasificate, care ar putea conduce la compromiterea acestor informații, în vederea luării măsurilor de prevenire necesare;
(c) luarea măsurilor de remediere a deficiențelor și de perfecționare a cadrului organizatoric și funcțional la nivelul structurii controlate;
(d) constatarea cazurilor de nerespectare a normelor de protecție a informațiilor clasificate și:
    (1) aplicarea sancțiunilor contravenționale sau, după caz,
    (2) sesizarea organelor de urmărire penală, în situația în care fapta constituie infracțiune;
(e) informarea Consiliului Suprem de Apărare a țării și Parlamentului cu privire la modul în care unitățile deținătoare de informații clasificate aplică reglementările în materie (art. 192).

Clasificarea controalelor:

(I) în funcție de obiectivele urmărite, controalele pot fi:
    a) controale de fond: urmăresc verificarea întregului sistem organizatoric, structural și funcțional de protecție a informațiilor clasificate;
    b) controale tematice: vizează anumite domenii ale activității de protecție a informațiilor clasificate;
    c) controale în situații de urgență: au ca scop verificarea unor aspecte punctuale, stabilite ca urmare a identificării unui risc de securitate.

(II) în funcție de modul în care sunt stabilite și organizate, controalele pot fi:
    a) planificate;
    b) inopinate;
    c) determinate de situații de urgență.

Modalitatea de realizare

(1) conducătorii unităților care fac obiectul controlului au obligația să pună la dispoziția echipelor de control toate informațiile solicitate privind modul de aplicare a măsurilor prevăzute de Legea nr.182/2002;

(2) conducătorii unităților deținătoare de informații clasificate au obligația să organizeze anual și ori de câte ori este nevoie controale interne privind gestionarea acestora;

(3) fiecare acțiune de control se încheie printr-un document de constatare, întocmit de echipa/persoana care l-a efectuat.

(4) în cazul în care controlul relevă fapte și disfuncționalități de natură să reprezinte riscuri majore de securitate pentru protecția informațiilor clasificate:

(a) va fi informat, de îndată, Consiliul Suprem de Apărare a țării,

(b) iar instituția controlată va dispune măsuri imediate:

i. remedierea deficiențelor constatate,

ii. va iniția cercetarea administrativă:

(i) după caz, va aplica măsurile sancționatorii, și

(ii) va sesiza organele de urmărire penală, în situația în care rezultă indicii că s-ar fi produs infracțiuni.

Inventarierea și arhivarea

Protecția informațiilor clasificate la agenții economici având ca obiect de activitate inventarierea și arhivarea

Deținători de informații clasificate au apelat la firme specializate pentru inventarierea și arhivarea documentelor clasificate (inclusiv a celor circumscrise HCM nr.19/1972), sub motivația lipsei de personal.

Aspecte problematice:

1. în contracte, nu au fost inserate clauze referitoare la informații clasificate, dacă prestatorii identificau astfel de documente;
2. angajații firmelor contractante nu erau autorizați să acceseze informații din clasa de secretizare supusă inventarierii/arhivării - conducătorii unităților deținătoare au fost neglijenți;
3. nu s-a întreprins măsurile ce se impun pe palierul securității industriale (încheierea anexelor de securitate, obținerea de către firme a autorizațiilor/certificatelor de securitate industrială;
4. externalizarea acestor servicii se poate realiza doar cu respectarea strictă a cadrului normativ în materie, altfel se produc incidente de securitate (contravenții săi infracțiuni).

Studiu de caz

Cu ocazia unui control al SRI la un agent economic, a reieșit că reprezentanții săi legali au încheiat un contract de prestări servicii având ca obiect „administrarea și depozitarea arhivei” cu o firmă specializată.

Firma a preluat documentații, de nivel maxim de secretizare „strict secret”, și le-a transportat cu mijloace proprii la sediul acesteia.

Punerea la dispoziția societății de inventariere a documentelor secrete de stat a întrunit elementele constitutive ale infracțiunii de „neglijență care are drept scop distrugerea, alterarea, pierderea sau sustragerea unui document ce constituie secret de stat, precum și neglijența care a dat prilej unei persoane să afle un asemenea secret, dacă fapta este de natură să aducă atingere intereselor statului” (art.252 Cod penal).

Au fost sesizate organele de urmărire penală competente [6].

Evaluarea protecției informațiilor clasificate

Măsurile aplicate în Uniunea Europeană

Vizitele de evaluare

Conform **Deciziei Consiliului UE nr.2013/488** [7], vizitele de evaluare vizează evaluarea eficienței măsurilor aplicate pentru protecția informațiilor clasificate ale Uniunii Europene (IUEC) și desemnează orice:

(a) inspecție periodică sau vizită de evaluare cu privire la managementul IUEC măsurile de securitate destinate protecției IUEC de la/din:
  (a) serviciile și incintele unde sunt gestionate sau păstrate IUEC (de către autoritățile de securitate competente);
(b) incinta Secretariatului General al Consiliului (SGC) și
(c) organismele, agențiile și entitățile UE care aplică decizia (ambele de către Secretarul General, care este autoritatea de securitate a SGC);
(d) serviciile și incintele aparținând statelor membre (de către Secretarul general, împreună și de comun acord cu ANS interesate);

(b) vizită de evaluare pentru a se stabili eficiența măsurilor de securitate aplicate într-un stat terț sau de către o organizație internațională pentru protecția IUEC furnizate sau schimbate.

Scopurile vizitelor de evaluare:

(a) asigurarea faptului că standardele minime necesare stabilite pentru protecția IUEC sunt respectate;
(b) sublinierea importanței securității și a unui management al riscului de securitate eficient în interiorul entităților inspectate;
(c) recomandarea unor contramăsuri pentru a atenua impactul specific al pierderii confidențialității, integrității sau disponibilității informațiilor clasificate; și
(d) consolidarea programelor de educație continuă și de conștientizare privind securitatea destinate autorităților de securitate.

Desfășurarea vizitelor de evaluare

(1) Programul vizitelor de evaluare se stabilește la sfârșitul anului calendaristic pentru anul următor, de comun acord cu agenția UE, statul membru, statul terț sau organizația internațională interesată;

(2) sunt efectuate pentru a verifica normele, regulamentele și procedurile relevante ale entității vizitate și a se asigura că practicile entității respectă principiile de bază și standardele minime stabilite și în dispozițiile care reglementează schimbul de informații clasificate cu entitatea respectivă;

(3) vizitele de evaluare se desfășoară în două faze:

(a) înaintea vizitei propriu-zise se organizează o reuniune pregătitoare, dacă este necesar, cu entitatea în cauză.

(b) după această reuniune pregătitoare, echipa de evaluare stabilește, împreună cu entitatea în cauză, un program de vizită detaliat care acoperă toate domeniile de securitate. Echipa care efectuează vizita de evaluare ar trebui să aibă acces la toate locațiile în care se gestionează IUEC, în special la registre și la SIC;

(4) vizitele de evaluare la administrațiile naționale ale statelor membre, în statele terțe și în organizațiile internaționale se desfășoară:

(a) în deplină cooperare cu funcționarii entității, statului terț sau organizației internaționale vizitate;

(b) cu asistența experților ANS pe teritoriul căreia este situată agenția sau organismul;

(c) pot fi solicitate asistența și contribuțiile experților ANS, în conformitate cu măsurile detaliate care vor fi convenite de Comitetul de securitate, la organisme, agenții și entități ale UE.

Rapoartele

1. la sfârșitul vizitei de evaluare, entității vizitate i se prezintă principalele concluzii și recomandări;
2. ulterior se redactează un raport privind vizita de evaluare. În cazurile în care s-au propus măsuri de remediere și recomandări, raportul cuprinde suficiente detalii pentru a sprijini concluziile obținute. Raportul este înaintat autorității competente din cadrul entității vizitate.
3. pentru vizitele de evaluare derulate în cadrul administrațiilor naționale ale statelor membre:
   (a) proiectul raportului de evaluare este înaintat ANS interesate, pentru a i se verifica corectitudinea factuală și faptul că nu conține informații cu un nivel de clasificare superior față de RESTREINT UE/EU RESTRICTED; și
   (b) cu excepția cazului în care ANS a statului membru în cauză solicită împiedicarea distribuției generale, rapoartele de evaluare sunt trimise Comitetului de securitate; raportul este clasificat la nivelul RESTREINT UE/EU RESTRICTED.
   (c) sub responsabilitatea autorității de securitate a SGC (Oficiul de securitate) se elaborează un raport periodic care ilustrează principalele concluzii desprinse în urma vizitelor de evaluare desfășurate în statele membre într-o perioadă specificată și care este analizat de Comitetul de securitate.

4. în cazul vizitelor de evaluare în statele terțe și în cadrul organizațiilor internaționale, raportul este distribuit Comitetului de securitate. Raportul este clasificat cel puțin la nivelul RESTREINT UE/EU RESTRICTED.
5. orice măsură de remediere este verificată în cursul unei vizite de monitorizare și raportată Comitetului de securitate.
6. în cazul vizitelor de evaluare la orice organism, agenție și entitate a Uniunii, rapoartele privind vizitele de evaluare sunt distribuite Comitetului de securitate. Proiectul raportului privind vizita de evaluare este înaintat agenției sau organismului vizate, pentru a i se verifica corectitudinea factuală și faptul că nu conține informații cu un nivel de clasificare superior față de RESTREINT UE/EU RESTRICTED.
7. orice măsură de remediere este verificată în cursul unei vizite de monitorizare și raportată Comitetului de securitate.

Lista de control

1. autoritatea de securitate a SGC (Oficiul de securitate) elaborează și actualizează o listă de control, cuprinzând aspectele care urmează să fie verificate în cursul unei vizite de evaluare. Lista de control respectivă este înaintată Comitetului de securitate;
2. informațiile necesare pentru completarea listei de control sunt obținute în special în timpul vizitei de la personalul de conducere responsabil cu securitatea al entității inspectate. Odată completată cu răspunsurile detaliate, lista de control este clasificată în acord cu entitatea inspectată. Aceasta nu face parte din raportul de inspecție.

Note bibliografice

[1] *ISO/IEC 27002/2022 (E) - Information security, cybersecurity and privacy protection — Information security controls*

[2] *https://ro.theastrologypage.com/information-security-audit (accesat la: 12 martie 2024)*

[3] *https://news24.ro/care-este-diferenta-dintre-controlul-intern-si-auditul-intern/ (accesat la: 12 martie 2024)*

[4] *Legea nr. 182/2002 privind protecția informațiilor clasificate, disponibilă la: https://legislatie.just.ro/Public/DetaliiDocument/35209; (accesat la: 20 martie 2024)*

[5] *Hotărârea Guvernului nr. 585 din 13 iunie 2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România, în: Monitorul Oficial cu numărul 485 din data de 5 iulie 2002, disponibilă la: https://legislatie.just.ro/Public/DetaliiDocument/37319 (accesat la: 23 martie 2024)*

[6] *https://www.sri.ro/fisiere/protectia-inf-cls-ghid.pdf (accesat la: 25.03.2024)*

[7] *Decizia Consiliului Uniunii Europene din 23 septembrie 2013 privind normele de securitate pentru protecția informațiilor UE clasificate (2013/488/UE), disponibilă la: https://eur-lex.europa.eu/legal-content/ro/ALL/?uri=CELEX:32013D0488 (accesat la: 15 martie 2024)*