MANAGEMENTUL OPERAȚIUNILOR DE SECURITATE

GHID ILUSTRAT

pentru consultanții și managerii de securitate care efectuează sau contractează operațiuni de securitate privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor

Ion Iordache

CUPRINS

[1]
INTRODUCERE

Managementul securității este un domeniu de management care se concentrează pe siguranța activelor (resurselor umane și bunurile materiale) dintr-o organizație identificând și evaluând prin diferite acțiuni și metode interconectate (politici, proceduri, orientări și standarde, etc.) vulnerabilitățile și amenințările și pentru a le asigura o funcționare în siguranță reducând riscurile la adresa acestora.

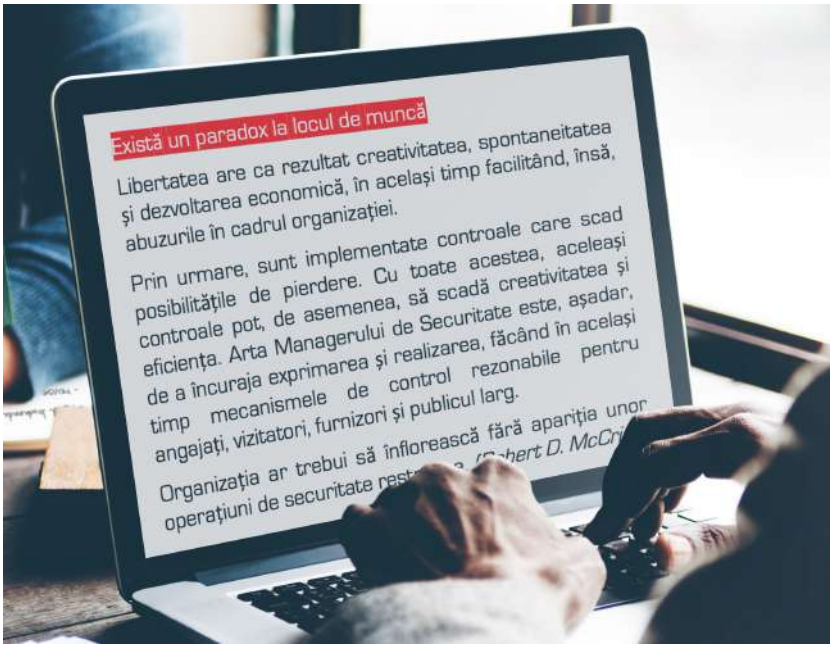
Scopul Managementului Operațiunilor de Securitate este similar cu cel al Managementului Riscurilor, evitarea problemelor sau fenomenelor negative (riscuri și amenințări de securitate), managementul crizelor crizelor și evitarea creării de probleme în activitatea zilnică a organizației.

Managerii de securitate sunt, după cum sugerează și numele, atât specialiști în securitate, cât și manageri de afaceri care, așa cum precizează standardul ocupațional al profesiei "sub conducerea managerului general şi în colaborare cu alţi conducători, organizează activitatea compartimentului de specialitate, avizează recrutarea si formarea personalului din subordine, urmăreşte randamentul şi eficienţa activităților, reprezintă organizaţia în relaţiile cu terţi."

În România, în exercitarea profesiei de manager de securitate sunt aplicabile prevederile cadrului legislativ specific legislaţiei incidentă domeniului sistemelor de securitate private, **"LEGEA nr. 333 din 2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor"** *(republicată și actualizată)* și a **"HOTĂRÂRII nr. 301 din 2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003"** *(actualizată)* dar și a altor legi cum ar fi Legea privind siguranţa naţională a României și/sau Legea privind protecţia informaţiilor clasificate, etc.

Pentru a-și exercita cu maxim de eficiență sarcinile profesionale, managerii de securitate, trebuie să opereze programe de securitate eficiente care se bazează pe politica de securitate a organizației și pe o serie de operațiuni și procese de securitate prin care trebuie atinse obiectivele de protecție eficientă ale organizației.

Acest lucru nu este simplu de realizat deoarece, în foarte multe situații, eforturile de protejare a vieții angajaților și ale bunurilor organizației nu vor primi sprijinul tuturor persoanelor implicate și uneori nici chiar al managementului de nivel înalt.



În acest eBook voi prezenta câteva din aspectele prezentate mai sus cu accent pe cerințele unui **Sistem de Management al Operațiunilor de Securitate (SMOS)** bazate pe standardul international **"ISO 18788: 2015 Sistem de gestionare a operațiunilor de securitate privată"** și pe principalele operațiuni desfășurate de managerul de securitate în cadrul unei organizații pentru a asigura securitatea persoanelor și bunurilor unei organizații.

[2]
IMPORTANȚA UNUI SISTEM DE MANAGEMENT AL OPERAȚIUNILOR DE SECURITATE

Un sistem de management al operațiunilor de securitate oferă un cadru pentru stabilirea, implementarea, operarea, monitorizarea, revizuirea, întreținerea și îmbunătățirea gestionării operațiunilor de securitate.

În general, un sisteme de management încurajează organizațiile să analizeze cerințele organizaționale și ale părților interesate și să definească procesele care contribuie la succesul organizației.

Acesta oferă o bază pentru stabilirea politicilor și obiectivelor, stabilirea procedurilor pentru realizarea rezultatelor dorite, măsurarea și monitorizarea realizării obiectivelor și rezultatelor.

Implementarea unui sistem de management oferă încredere atât organizației, cât și clienților săi, că organizația este capabilă să își gestioneze obligațiile contractuale, de securitate și legale, precum și să respecte drepturile omului.

În mod concret, standardul internațional "ISO 18788: 2015 Sistem de gestionare a operațiunilor de securitate privată" oferă principiile și cerințele pentru un sistem de management a operațiunilor de securitate; un cadru de management al afacerilor și al riscurilor pentru organizațiile care desfășoară sau contractează operațiuni de securitate și activități și funcții conexe, demonstrând în același timp că:

a) are nevoie să demonstreze capacitatea sa de a furniza consecvent activități de securitate fizică în scopul asigurării siguranței și protecției persoanelor împotriva oricăror acte ostile care le pot periclita viața, integritatea fizică sau sănătatea; pentru a-și asigura bunurile și valorile împotriva oricăror acțiuni ilicite care lezează dreptul de proprietate și existența materială a acestora;

b) urmărește responsabilitatea față de lege și demonstrarea angajamentul față de obligațiile legale de protecție a vieții propriilor angajați, clienți, colaboratori sau vizitatori, a bunurilor și valorilor aflate în proprietatea sa;

c) urmărește să crească satisfacția clienților săi prin aplicarea eficace a sistemului, inclusiv a proceselor pentru îmbunătățirea sistemului și asigurarea conformității cu cerințele clienților, cu cerințele legale și reglementările aplicabile.

Avantajele implementării unui sistem de management al operațiunilor de securitate

- ❑ Oferă fiabilitate și stabilește o guvernanță corporativă eficientă.
- ❑ Consolidează credibilitatea și protejază reputația organizației.
- ❑ Asigură calitatea și profesionalismul organizațiilor de securitate private.
- ❑ Demonstrează îmbunătățiri în asigurarea securității atât propriilor angajați cât și clienților organizației.
- ❑ Oferă încredere propriilor angajați, clienților și agențiilor guvernamentale de aplicare a legii.
- ❑ Crește potențialul de succes operațional.

Prin urmare, putem concluziona că implementarea cerințelor unui sistem de management al operațiunilor de securitate vă poate ajuta cu siguranță să stabiliți nivelul dorit de securitate în organizația dvs.

[3]
CONTEXTUL ÎN CARE ÎȘI DESFĂȘOARĂ ACTIVITATEA ORGANIZAȚIA

Atunci când o organizație dorește să implementeze un Sistem de Management al Operațiunilor de Securitate (SMOS) trebuie să determine problemele externe și interne relevante pentru scopul său și care îi afectează capacitatea de a obține rezultatele dorite.

În general, proiectarea și implementarea unui cadru de sistem de management se bazează pe înțelegerea organizației și a contextului său intern și extern de funcționare.

Prin urmare, organizația își definește și documentează contextul intern și extern, inclusiv lanțul de aprovizionare și subcontractanții săi.

Acești factori trebuie luați în considerare la stabilirea, implementarea și menținerea SMOS, organizația trebuind să evalueze factorii interni și externi care pot influența modul în care va gestiona riscurile de securitate.

Context extern:

Organizația trebuie să definească și să documenteze contextul său extern, inclusiv:

- contextul cultural și politic;
- mediul legal, de reglementare, tehnologic, economic, natural și competitiv;
- acordurile contractuale, inclusiv alte organizații din sfera contractului;
- dependențele de infrastructură și interdependențele operaționale;
- relațiile și angajamentele lanțului de aprovizionare și ale contractorilor;
- problemele cheie și tendințele care pot avea impact asupra proceselor și/sau obiectivelor organizației;
- percepțiile, valorile, nevoile și interesele părților interesate externe (inclusiv comunitățile locale din domeniile de activitate);
- forțele operaționale și liniile de autoritate.

La stabilirea contextului său extern, organizația se asigură că obiectivele și preocupările părților interesate externe sunt luate în considerare la elaborarea criteriilor de management a operațiunilor de securitate.

Organizația identifică și documentează întreg lanțul de aprovizionare, în special utilizarea subcontractanților care pot avea un impact asupra riscului și potențialul de a provoca un eveniment nedorit sau perturbator.

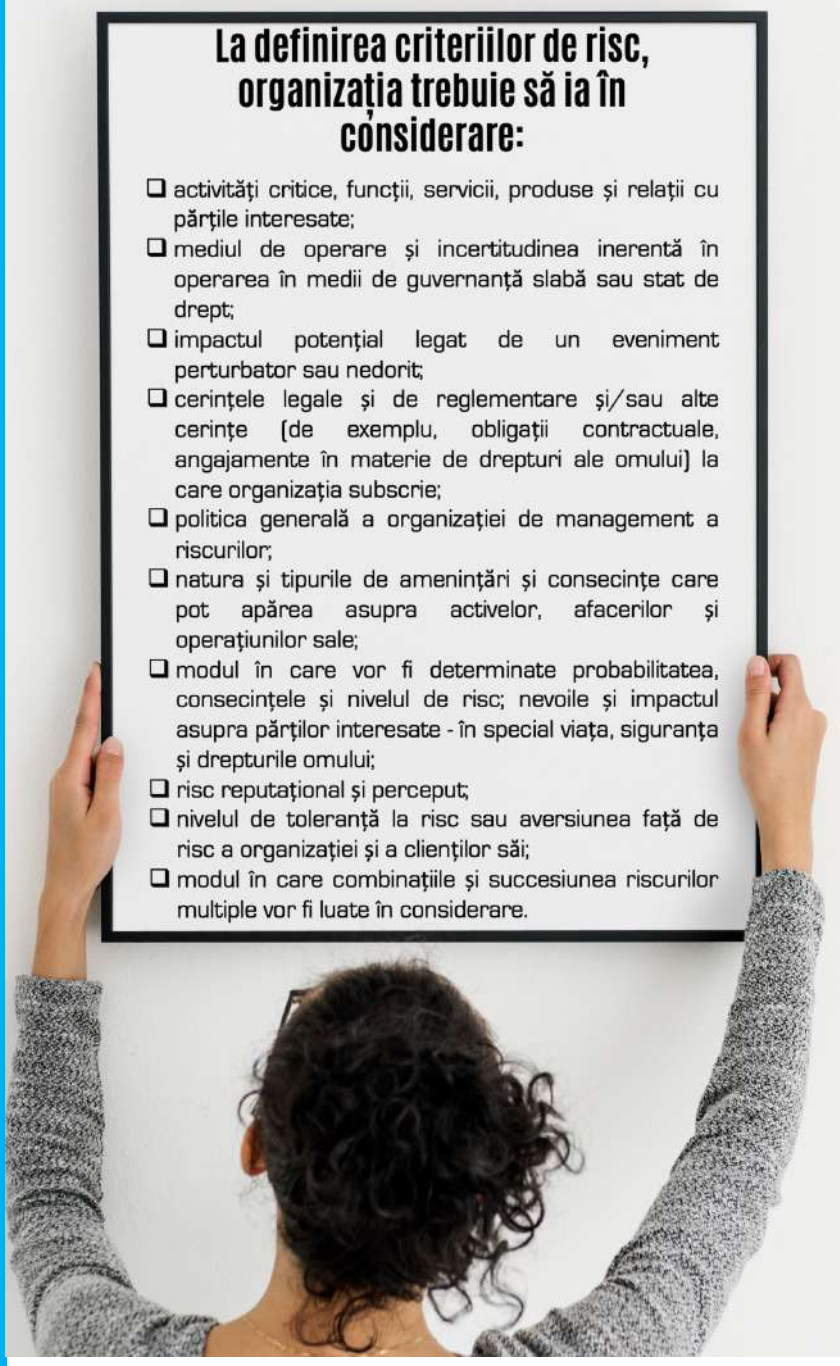
Gestionarea riscului lanțului de aprovizionare trebuie să fie inclusă în programul general de gestionare a operațiunilor de securitate a unei organizații în care au fost identificate riscuri semnificative și există potențialul de a provoca un eveniment nedorit sau perturbator.

[4]
DEFINIREA CRITERIILOR DE RISC ȘI ÎNȚELEGEREA NEVOILOR ȘI AȘTEPTĂRILOR PĂRȚILOR INTERESATE

Organizația trebuie să definească și să documenteze criteriile pentru a evalua semnificația riscului iar criteriile de risc trebuie să reflecte valorile, obiectivele și resursele organizației.

În timp ce criteriile de risc sunt stabilite la începutul procesului de evaluare a riscurilor, acestea sunt dinamice și vor fi continuu monitorizate și revizuite.

Organizația va determina părțile interesate care sunt relevante pentru SMOS și cerințele relevante ale acestor părți interesate.



Top managementul se asigură că interesele părților interesate interne și externe sunt identificate, evaluate și documentate, pentru a atinge obiectivele contractelor sale și a minimiza riscurile iar atunci când identifică nevoile și cerințele părților interesate interne și externe, organizația trebuie să ia în considerare:

- ❑ disponibilitatea pentru risc a părților interesate;
- ❑ obligațiile contractuale specificate de client;
- ❑ cerințe legale, de reglementare și angajamentele voluntare;
- ❑ responsabilitățile privind drepturile omului și impacturile relevante pentru serviciile furnizate;
- ❑ impactul și interacțiunile cu părțile interesate externe (cum ar fi poliția, comunitățile locale, clienții și alți furnizori de securitate);
- ❑ înregistrări și cerințe de documentare pentru furnizarea de servicii de securitate și neconformități.

[5]
MANAGEMENTUL ORGANIZAȚIEI ȘI ANGAJAMENTUL SĂU FAȚĂ DE ASIGURAREA SECURITĂȚII

Fără angajamentul Top managementului (Consiliul de administrație sau directorul general, de exemplu), niciun sistem de management nu poate avea succes.

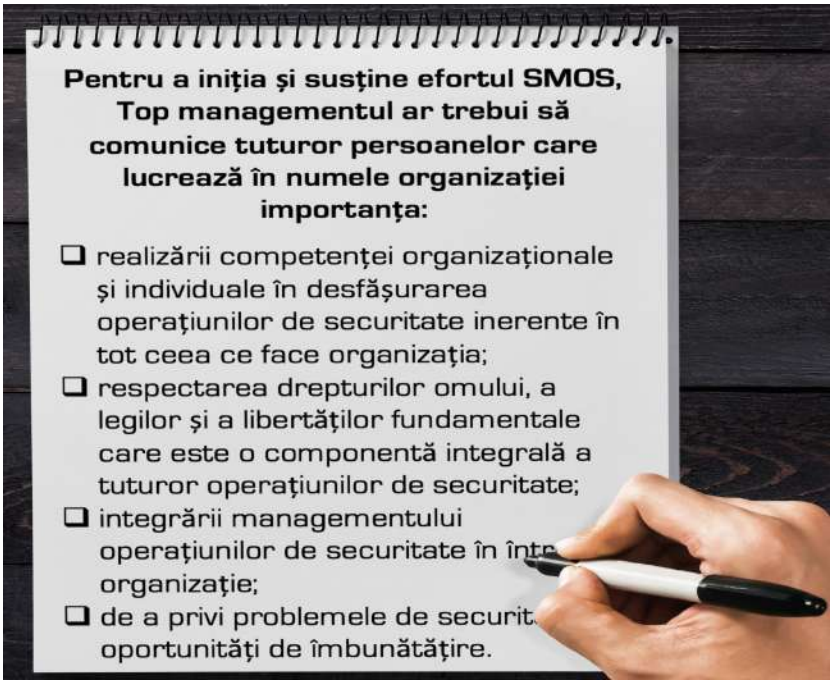
Top managementul ar trebui să demonstreze părților interesate interne și externe un angajament vizibil de a respecta drepturile omului, legile și libertățile fundamentale în furnizarea de operațiuni de securitate.

Este esențial ca managementul de vârf al organizației să furnizeze resursele necesare și să își asume responsabilitatea pentru crearea, întreținerea, testarea și implementarea unui SMOS eficient.

Acest lucru va asigura faptul că conducerea și personalul de la toate nivelurile din cadrul organizației înțeleg că SMOS este o prioritate critică de top management.

Top managementul trebuie să demonstreze leadership și angajament în ceea ce privește dezvoltarea și implementarea unui Sistem de Management al Operațiunilor de Securitate (SMOS) și îmbunătățirea continuă a eficacității sale prin:

- ❑ asigurarea faptului că politica operațiunilor de securitate și obiectivele operațiunilor de securitate sunt stabilite și sunt compatibile cu direcția strategică a organizației;
- ❑ asigurarea integrării cerințelor SMOS în procesele de afaceri ale organizației;
- ❑ asigurarea disponibilității resurselor necesare SMOS pentru stabilirea, implementarea, operarea, monitorizarea, revizuirea, întreținerea și îmbunătățirea SMOS;
- ❑ comunicarea importanței gestionării eficiente a operațiunilor de securitate și a conformării cu cerințele SMOS și responsabilitățile sale legale;
- ❑ asigurarea faptului că SMOS își atinge rezultatul (rezultatele) prevăzut ;
- ❑ îndrumarea și sprijinirea persoanelor pentru a contribui la eficacitatea SMOS;
- ❑ promovarea îmbunătățirii continue;
- ❑ efectuarea la intervale planificate de revizuiri de management ale SMOS.



Managementul trebuie să elaboreze, să documenteze și să publice o declarație de conformitate care să indice angajamentul organizației și conformitatea cu responsabilitatea sa de a respecta drepturile omului și legislația în vigoare.

Declarația de conformitate va fi:

- ❑ documentată și implementată;
- ❑ disponibilă public și comunicată intern și extern tuturor părților interesate relevante;
- ❑ aprobată de Top management.

[6]
POLITICA OPERAȚIUNILOR DE SECURITATE

Politica operațiunilor de securitate este cadrul care stă la baza stabilirii obiectivelor de securitate ale organizației aceasta fiind suficient de clară pentru a putea fi înțeleasă de părțile interesate interne și externe și ar trebui revizuită periodic pentru a reflecta condițiile și informațiile în schimbare.

Domeniul său de aplicare ar trebui să fie clar identificabil și ar trebui să reflecte natura, amploarea și impactul unic al riscurilor activităților, funcțiilor, produselor și serviciilor sale.

Gestionarea riscurilor nu este doar responsabilitatea Top managementului.

Pentru ca un SMOS să fie eficient, acesta trebuie implementat de fiecare persoană care lucrează în numele organizației.

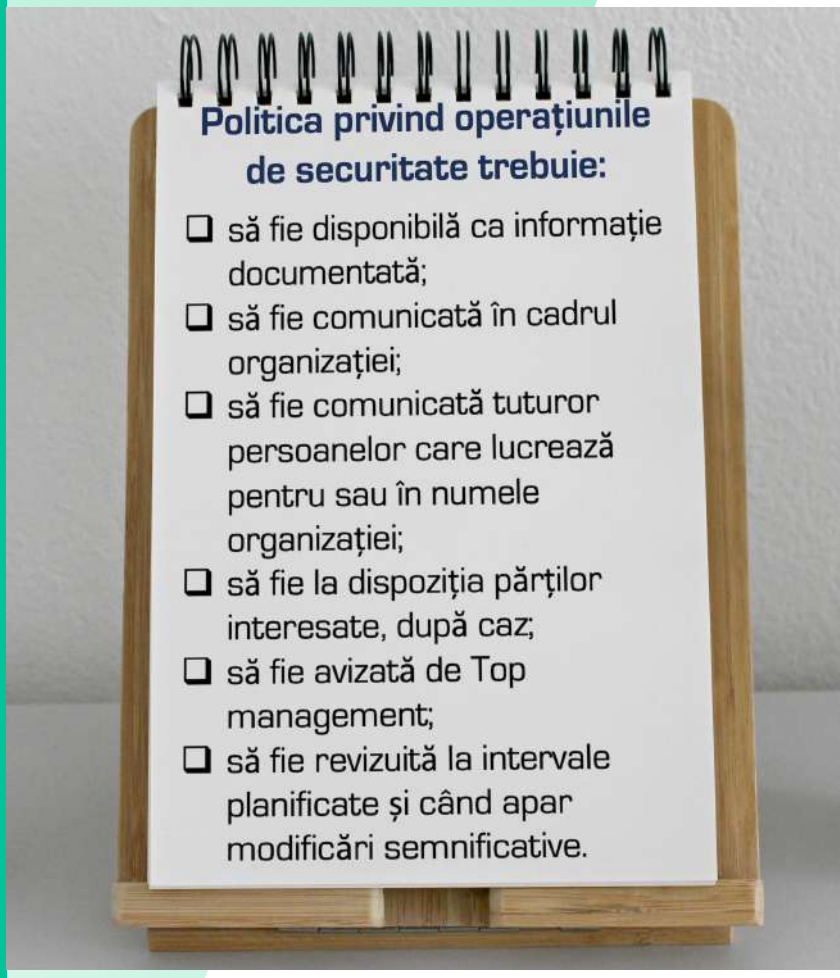
Este o abordare de sus în jos și de jos în sus.

Protecția drepturilor omului și gestionarea riscurilor trebuie să devină o parte integrantă a culturii organizației.

Prin urmare, toți factorii de decizie și asumare a riscurilor ar trebui să fie administratori de riscuri.

Top managementul va stabili o politică privind operațiunile de securitate care:

- ❑ este adecvată scopului organizației;
- ❑ oferă un cadru pentru stabilirea obiectivelor operațiunilor de securitate;
- ❑ include angajamentul de a îndeplini cerințele legale și alte cerințe aplicabile, inclusiv angajamentele voluntare la care organizația subscrie;
- ❑ include un angajament pentru îmbunătățirea continuă a SMOS;
- ❑ se angajează să respecte drepturile omului;
- ❑ oferă angajamentul de a evita, preveni și reduce probabilitatea și consecințele unor evenimente perturbatoare sau nedorite.



Sistemul de management este implementat de oameni din cadrul organizației. **Una sau mai multe persoane calificate ar trebui numite și împuternicite să implementeze, să testeze sau să exercite și să mențină SMOS.**

Top managementul ar trebui să efectueze propriile revizuiri periodice și audituri ale SMOS.

O echipă de planificare a managementului operațiunilor de securitate, incluzând lideri superiori din toate funcțiile organizaționale majore și grupurile de sprijin, poate fi numită pentru a asigura acceptarea pe scară largă a SMOS.

POLITICA OPERAȚIUNILOR DE SECURITATE

(Exemplu)

Cod:	iQS 21.2.1
Versiune/data:	0.2
Creat de:	Ion Iordache - Manager de Securitate
Aprobat de:	Popescu Vasile - Manager General

[7]
ABORDAREA RISCURILOR ȘI OPORTUNITĂȚILOR

Atunci când planifică un Sistem de Management al Operațiunilor de Securitate (SMOS), organizația trebuie să ia în considerare contextul intern și extern în care acționează și să stabilească riscurile și oportunitățile care trebuie abordate asigurându-se că se pot preveni sau reduce efectele nedorite și că se pot obține îmbunătățiri continue.

Organizația trebuie să stabilească, să pună în aplicare și să mențină un proces formal și documentat de evaluare a riscurilor pentru operațiunile sale de securitate, inclusiv pentru partenerii săi relevanți din lanțul de aprovizionare și din activitățile de subcontractare.

Procesul de evaluare a riscurilor include:

- ❑ **identificarea riscurilor** - identificarea și evaluarea amenințărilor, vulnerabilităților, consecințelor și riscurilor legate de viaţa, integritatea fizică și/sau sănătatea persoanelor, bunurilor şi valorilor; identificarea riscurilor strategice, tactice și operaționale datorate evenimentelor intenționate, neintenționate și naturale care pot avea consecințe directe sau indirecte asupra activităților, activelor, operațiunilor, funcțiilor organizației și părțile interesate afectate, precum și capacitatea sa de a respecta principiile și drepturilor omului;
- ❑ **analiza riscurilor** - analizarea în mod sistematic a riscului (probabilitatea și analiza consecințelor, inclusiv analiza riscurilor privind drepturile omului) pentru a determina acele riscuri care au un impact semnificativ asupra activităților, funcțiilor, serviciilor, produselor, lanțului de aprovizionare, subcontractanților, relațiilor cu părțile interesate, populațiilor locale și mediului;
- ❑ **evaluarea riscurilor** - evaluarea în mod sistematic și stabilirea priorităților în ceea ce privește controalele și tratamentele riscurilor și costurile aferente acestora pentru a determina cum să aduceți riscul într-un nivel acceptabil, în concordanță cu criteriile de risc.

Organizația trebuie să:

- ❑ documenteze și să păstreze aceste informații actualizate și sigure;
- ❑ revizuiască periodic dacă domeniul de aplicare al SMOS, politica, criteriile de risc și evaluarea riscurilor este încă adecvată având în vedere contextul intern și extern al organizației;
- ❑ reevalueze riscurile în contextul modificărilor din cadrul organizației sau aduse organizației de mediul de operare, proceduri, funcții, servicii, parteneriate și lanțurile de aprovizionare;
- ❑ evalueze beneficiile și costurile directe și indirecte ale opțiunilor de management al riscurilor și de sporire a fiabilității și rezilienței;
- ❑ evalueze eficacitatea efectivă a opțiunilor de tratament ale riscurilor după incidente și după exerciții;
- ❑ se asigure că riscurile și impacturile prioritare sunt luate în considerare la stabilirea, implementarea și operarea SMOS;
- ❑ monitorizeze și să evalueze eficacitatea controalelor de risc și a tratamentelor aplicate riscurilor.

DETALII	OBSERVATII	RECOMANDARI
Perimetre (garduri, balustrade, granite de proprietate etc.)		
Admiterea accesului (controlul intrarilor si iesirilor)		
Amenajarea terenului (natural/artificial)		
Parcari		
Iuminatul exterior		
SSV		
Magazii, depozite, dependinte		
Semnalizari/anunturi de securitate		
Spatii de servicii (alimentare carburant, generatoare de curent, spatiu depozitare deseuri etc.)		
Altele		

6. PROCEDURI SI CONTROALE DE SECURITATE - LISTA DE INTREBARI

A. RECRUTAREA PERSONALULUI, SELECTIA, ANGAJAREA, CONCEDIEREA		DA/NU
1	Exista un formular de aplicatie standardizat pentru aplicare?	
2	Referintele sunt verificate?	
3	Se solicita un CV? Daca DA, acesta este verificat?	
4	Exista un contract de munca?	
5	Se verifica competentele solicitantului?	
6	Sunt descrise in detaliu conditiile de angajare?	
7	Se prezinta aplicantului structura fisei postului?	
8	Exista proceduri clare de concediere?	
9	Exista masuri de protectie fata de personalul concediat?	

B. CONTROLUL SI SECURITATEA NUMERARULUI		DA/NU
1	Casele de marcat sunt asigurate corespunzator si monitorizate individual?	
2	Personalul caselor de marcat este instruit corespunzator in operatiunile de manipulare a numerarului?	
3	Casele de bani/seifurile sunt prinse in podea si asigurate corespunzator?	
4	Numararea banilor se face in conditii de siguranta si respectand proceduri specifice?	
5	Exista proceduri de securitate pentru tranzactiile electronice?	
6	Exista masuri si metode de verificare a numerarului?	
7	Se emit facturi/chitante/bonuri fiscale pentru toate marfurile vandute?	
8	Colectarea numerarului si transportul acestuia se face in conditii de siguranta?	
9	Daca exista ATM-uri, acestea sunt asigurate corespunzator?	

C. SECURITATEA SI CONTROLUL VALORILOR		DA/NU
1	Este utilizat principiul "just-in-time" in aprovizionare?	
2	Exista personal special desemnat pentru aprovizionare si/sau livrare?	
3	Toate livrarile sunt inregistrate la "iesire"?	
4	Zonele de depozitare/livrare sunt asigurate corespunzator?	
5	Exista spatii sigure pentru depozitarea/vizualizarea bunurilor de mare valoare?	
6	Este controlat accesul personalului la zonele de depozitare/livrare?	
7	Se fac verificari periodice ale stocului de marfa?	
8	Exista o marcare de securitate pentru marfurile din depozit?	
9	Exista un control asupra deseurilor?	
10	Exista substante/medicamente ce necesita control special?	
11	Daca exista substante/medicamente ce necesita control special sunt asigurate conform legislatiei?	
12	Personalul ce manipuleaza valori este doar cel special desemnat si instruit pentru aceste operatiuni?	

C. PROCEDURI DE SECURITATE - GENERALE		DA/NU
1	Incuietorile de securitate utilizate sunt sigure pentru personal?	
2	Personalul de securitate are acces la toate cheile/codurile de acces?	
3	Exista o politica de securitate?	
4	Exista proceduri de lucru cu personalul in situatia furturilor interne?	

[8]
LEGISLAȚIA SPECIFICĂ ȘI ALTE CERINȚE

Organizația ar trebui să identifice și să înțeleagă cerințele legale, de reglementare și contractuale care afectează atingerea obiectivelor sale de securitate.

Acestea pot include cerințe legale naționale și internaționale. Identificarea și înțelegerea acestor cerințe ajută la asigurarea conformității legale, previne litigiile, îmbunătățesc imaginea organizației și sporesc capacitatea sa de a oferi servicii de protecție responsabile clienților să interni și externi.

Organizația trebuie să documenteze aceste informații și să le actualizeze comunicând informațiile relevante cu privire la cerințele legale și de altă natură persoanelor care lucrează în numele său și altor părți terțe relevante, inclusiv subcontractanților.

NOTĂ: în sensul standardului internațional **"ISO 18788: 2015 Sistem de gestionare a operațiunilor de securitate privată"**, legile naționale le pot include pe cele din țara organizației, din țările personalului acesteia, țara operațiunilor și țara clientului.

Organizația ar trebui să stabilească, să pună în aplicare și să încorporeze în procesele sale, măsuri pentru identificarea, respectarea și evaluarea cerințelor legale și voluntare aplicabile, inclusiv (dar nu limitat la):

a) cerințele legale, de reglementare și de altă natură aplicabile și relevante la nivel local, național și internațional legate de activitățile și operațiunile sale de securitate și ale oricăror subcontractanți sau asocieri;
b) dreptul internațional umanitar relevant și drepturile omului, inclusiv, dar fără a se limita la, interzicerea torturii sau a altor tratamente crude, inumane sau degradante; conștientizarea și interzicerea exploatării și abuzului sexual sau a violenței bazate pe gen, recunoașterea și prevenirea traficului de persoane și a sclaviei;
c) legislația și codurile aplicabile internaționale și naționale privind ocuparea forței de muncă și de mediu;
d) măsuri internaționale și naționale împotriva mitei, corupției și infracțiunilor similare;
e) procese de conformitate cu legislația locală, națională și internațională în ceea ce privește achiziționarea, acordarea licențelor și transbordarea armelor de foc (de exemplu) pentru a fi utilizate în operațiunile sale de securitate;
f) orice coduri sau convenții voluntare la care organizația subscrie. Acestea pot include, de exemplu, Principiile directoare ale ONU privind afacerile și drepturile omului (UNGP)

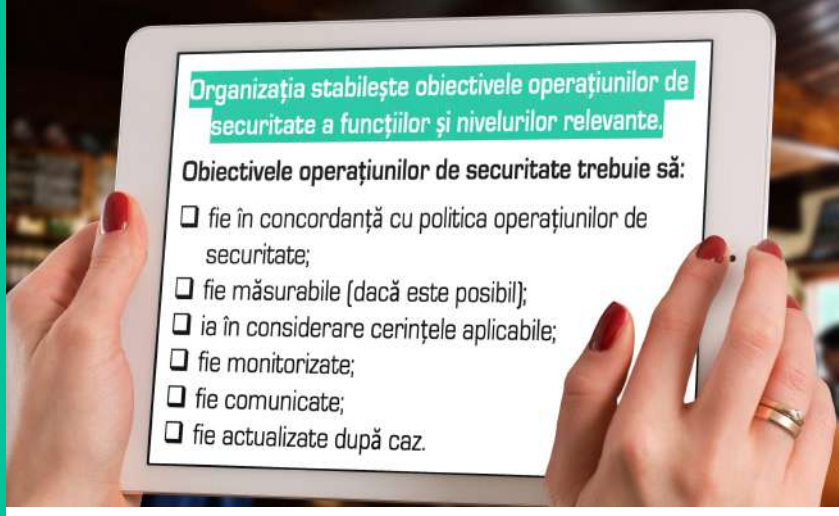
Exemple de alte cerințe pe care organizația, dacă este cazul, ar trebui să le îndeplinească:

- ❑ obligații comerciale și alte obligații contractuale;
- ❑ acorduri cu clienții;
- ❑ principii voluntare sau coduri de practică;
- ❑ informații de identitate, confidențialitate și cerințe de confidențialitate.

În România legislaţia incidentă domeniului sistemelor de securitate private este fromată din următoare documente:

- ❑ **LEGEA nr. 333 din 8 iulie 2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor** (actualizată la data de 1 decembrie 2015)
- ❑ **HOTĂRÂREA nr. 301 din 11 aprilie 2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003** privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor (actualizată până la data de 29 ianuarie 2016*)
- ❑ **INSTRUCŢIUNILE nr. 9 din 1 februarie 2013 privind efectuarea analizelor de risc la securitatea fizică** a unităţilor ce fac obiectul Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor.

[9]
OBIECTIVELE OPERAȚIUNILOR DE SECURITATE ȘI PLANIFICAREA ACESTORA



Prin stabilirea obiectivelor operațiunilor de securitate, organizația poate pune în planuri de acțiune politica sa de securitate, cu precizarea că aceste obiective și ținte ar trebui să fie specifice și măsurabile pentru a urmări progresul și a stabili modul în care Sistemul de Management al Operațiunilor de Securitate (SMOS) este performant.

"Obiectivele" SMOS sunt considerente prioritare, cum ar fi de exemplu, eliminarea furturilor interne. „Țintele" operațiunilor de securitate sunt valori specifice pentru măsurarea performanței pe baza indicatorilor cheie de performanță ia acestea, împreună cu obiectivele ar trebui să fie adecvate pentru organizație, pe baza evaluării riscurilor fiind necesară revizuirea lor periodică.

La stabilirea și revizuirea obiectivelor și țintelor sale, o organizație trebuie să ia în considerare cerințele sale financiare, operaționale și de afaceri, cerințele legale, de reglementare și de altă natură, impactul asupra drepturilor omului, riscurile semnificative, opțiunile sale tehnologice și opiniile părților interesate.

Organizația păstrează informații documentate cu privire la obiectivele operațiunilor de securitate.

Atunci când planifică modul de realizare a obiectivelor operațiunilor de securitate, organizația trebuie să stabilească:

- ❑ ce se va face;
- ❑ ce resurse vor fi necesare;
- ❑ cine va fi responsabil;
- ❑ când vor fi finalizate;
- ❑ modul în care vor fi evaluate rezultatele.

Obiectivele trebuie să fie derivate din și în concordanță cu politica operațiunilor de securitate și evaluarea riscurilor, inclusiv angajamentele pentru:

- ❑ minimizarea riscului prin reducerea probabilității și a consecințelor;
- ❑ respectarea legilor naționale și internaționale;
- ❑ cerințele financiare, operaționale și de afaceri (inclusiv angajamentele privind subcontractorii și lanțul de aprovizionare);
- ❑ îmbunătățirea continuă.

Obiectivele asociate cu indicatorii cheie de performanță trebuie să fie măsurabili calitativ și/sau cantitativ.

Obiectivele vor fi derivate din și în concordanță cu obiectivele operațiunilor de securitate și vor fi:

- ❑ la un nivel adecvat de detaliu;
- ❑ proporțional cu evaluarea riscului;
- ❑ specifice, măsurabile, realizabile, relevante și bazate pe timp (acolo unde este posibil);
- ❑ comunicate tuturor angajaților și terților, inclusiv subcontractanților și partenerilor din lanțul de aprovizionare, cu intenția ca aceste persoane să fie conștientizate de obligațiile lor individuale;
- ❑ revizuite periodic pentru a se asigura că acestea rămân relevante și coerente cu obiectivele operațiunilor de securitate și modificate în consecință.

[10]
PROGRAMUL DE SECURITATE

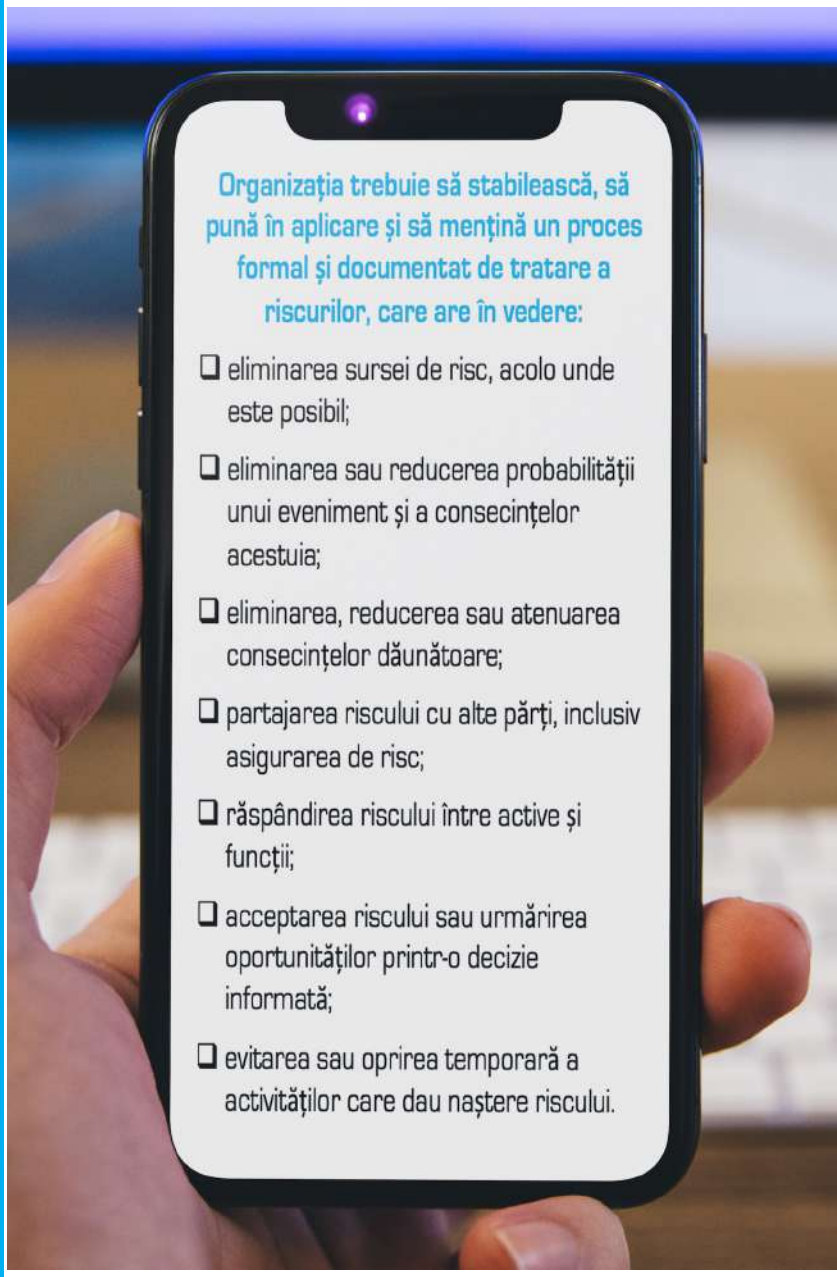
Organizația trebuie să stabilească, să pună în aplicare și să mențină programe pentru realizarea operațiunilor sale de securitate și a obiectivelor de tratare a riscurilor.

Programele vor fi optimizate și prioritizate pentru a controla și trata riscurile asociate operațiunilor sale, subcontractanților și lanțului de aprovizionare.

Un program de securitate este un document care descrie politica de securitate, strategiile, obiectivele, programele și procesele de securitate ale organizației oferind o imagine detaliată a riscurilor și a planurilor de atenuare a acestora.

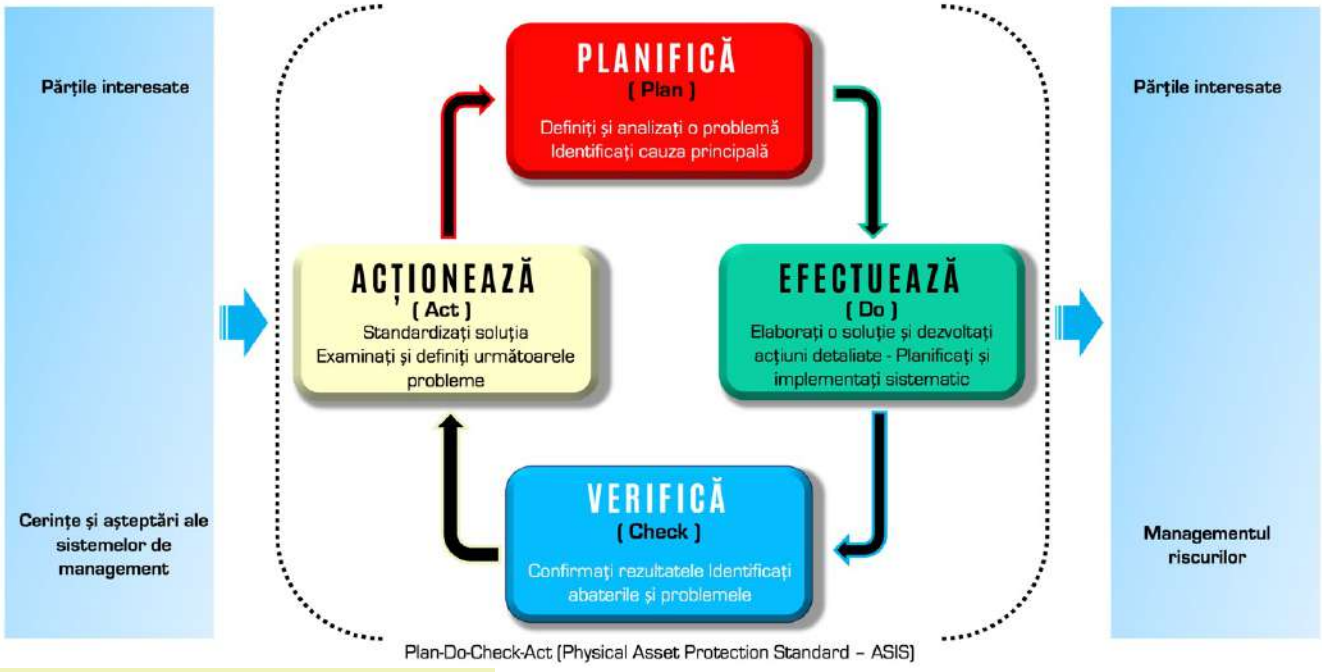
Top managementul trebuie să:

- ❑ evalueze beneficiile și costurile opțiunilor de eliminare, reducere sau menținere a riscului;
- ❑ evalueze programele sale de operațiuni de securitate pentru a determina dacă aceste măsuri au introdus noi riscuri;
- ❑ revizuiască periodic tratamentul riscurilor pentru a reflecta modificările aduse mediului extern, inclusiv cerințele legale, de reglementare și alte cerințe, precum și modificările aduse politicii organizației, facilităților, sistemului (sistemelor) de gestionare a informațiilor, activităților, funcțiilor, produselor, serviciilor și lanțului de aprovizionare.



[11]
PROGRAMUL DE SECURITATE ABORDAREA PE BAZĂ DE PROCES

Abordarea pe bază de proces prin asigurarea unor măsuri preventive dezvoltate în cadrul unui Program de Securitate bazat pe modelul Planifică - Efectuează - Verifică - Acționează (Plan-Do-Check-Act (PDCA) aplicabil, de altfel, tuturor proceselor **Sistemului de Management al Operațiunilor de Securitate (SMOS)** în ansamblul său) urmărește asigurarea unui nivel acceptabil de protecție a vieții persoanelor și activelor unei organizații.



Plan-Do-Check-Act (Physical Asset Protection Standard – ASIS)

Ciclul PDCA pentru îmbunătățirea continuă aplicat Programului de Securitate

PLANIFICĂ (Plan) (Stabilește Programul de Securitate)	Stabilește politica, obiectivele, procesele și procedurile Programului de Securitate și ale proceselor sale și resursele necesare obținerii rezultatelor în concordanță cu cerințele clientului și cu politicile organizației, identifică și tratează riscurile și oportunitățile.
EFECTUEAZĂ (Do) (Implementează și operează Programul de Securitate)	Implementează și operează ceea ce s-a planificat, politica, controalele, procesele și procedurile Programului de Securitate.
VERIFICĂ (Check) (Monitorizează și revizuiește Programul de Securitate)	Monitorizează, evaluează, măsoară și (atunci cand este cazul) revizuiește procesele și serviciile rezultate, față de politici, obiective, cerințe și activități planificate; raporteaza rezultatele managementului organizației.
ACȚIONEAZĂ (Act) (Menține și îmbunătățește Programul de Securitate)	Întreprinde actiuni pentru îmbunatatirea performantelor, dupa cum este necesar prin luarea de măsuri preventive și corective, pe baza rezultatelor auditului intern al Programului de Securitate și al revizuirii managementului, pentru a realiza îmbunătățirea continuă a Programului de Securitate.

[12]
SISTEMUL DE MANAGEMENT AL OPERAȚIUNILOR DE SECURITATE
- RESURSE -

Resursele necesare pentru un Sistem de Management al Operațiunilor de Securitate (SMOS) ar trebui identificate și includ resursele umane și abilitățile (competențele) specializate, echipamentele, infrastructura internă, tehnologia, idate, informații și resurse financiare.

Top managementul trebuie să stabilească și să furnizeze resursele necesare pentru înființarea, implementarea, întreținerea și îmbunătățirea continuă a SMOS și trebuie să ia în considerare: resursele interne, capacitățile, limitările existente și posibilele suplimentări; ce servicii și bunuri urmează să fie furnizate extern.

Cerințe structurale

Organizația trebuie să fie o entitate juridică sau o parte definită a unei entități juridice. Acesta trebuie să aibă o structură de management clar definită, care să demonstreze controlul și responsabilitatea la fiecare nivel al organizației (inclusiv filialele sale din sfera de aplicare).

Organizația trebuie să-și documenteze structura organizatorică, indicând atribuțiile, responsabilitățile și autoritățile conducerii; să definească și să documenteze dacă organizația este o parte definită a unei alte persoane juridice și relația cu alte părți ale aceleiași persoane juridice; să definească orice acord comun sau parteneriat în cadrul SMOS.

Asigurări

Organizația trebuie să demonstreze că are asigurare pentru acoperirea riscurilor și a datoriilor asociate care decurg din operațiunile și activitățile sale, în conformitate cu evaluarea riscurilor sale.

Atunci când externalizează sau subcontractează servicii, operațiuni sau funcții, organizația trebuie să asigure o acoperire de asigurare pentru activitățile subcontractate, după caz.

Externalizarea și subcontractarea

Organizația trebuie să aibă un acord documentat care să acopere acorduri subcontractate sau externalizate, inclusiv:

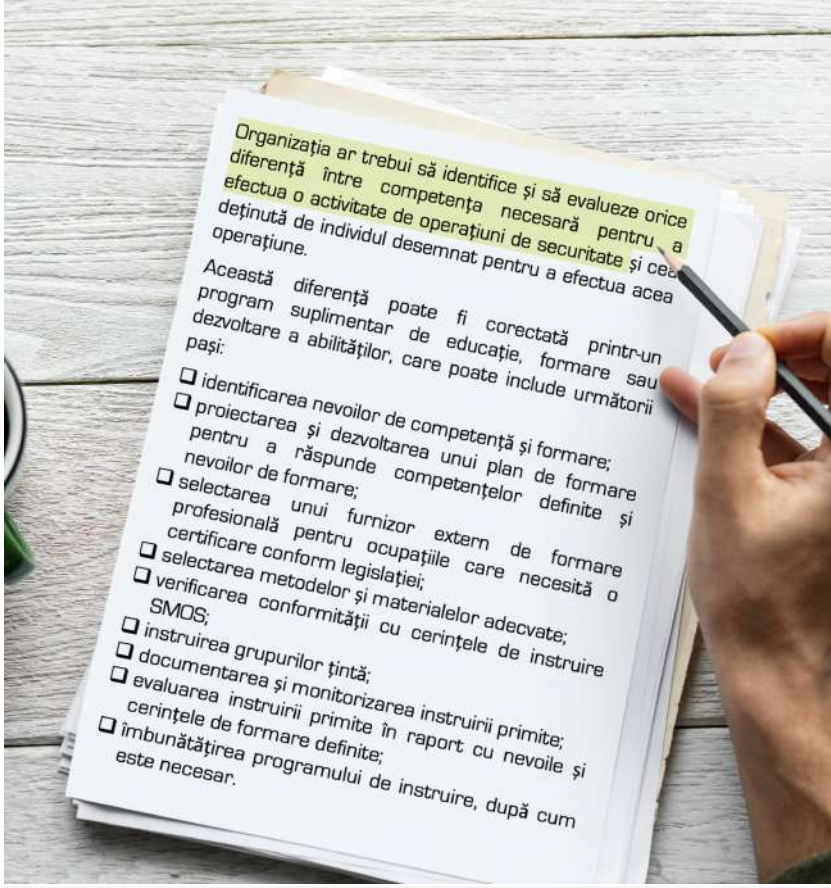
- ❑ angajamentul subcontractanților de a respecta aceleași angajamente și obligații legale, etice și legate de drepturile omului, deținute de organizație;
- ❑ procesul de raportare a riscurilor, precum și apariția și răspunsul la evenimente nedorite și perturbatoare;
- ❑ acorduri de confidențialitate și conflicte de interese;
- ❑ definirea și documentarea clară a serviciilor care urmează să fie furnizate;
- ❑ sfera și limitele de comandă și control;
- ❑ definirea relației de sprijin dintre contractant și subcontractant;
- ❑ conformitatea cu prevederile aplicabile ale standardului internațional **"ISO 18788: 2015 Sistem de gestionare a operațiunilor de securitate privată".**

[13]
SISTEMUL DE MANAGEMENT AL OPERAȚIUNILOR DE SECURITATE
- COMPETENȚE -

Este responsabilitatea organizației ca toate persoanele care lucrează în numele său să fie suficient instruite și în mod continuu în îndeplinirea funcțiilor lor; să respecte legile locale, naționale și internaționale.

Organizația trebui să determine competența necesară a persoanei (persoanelor) care lucrează sub controlul său care afectează managementul operațiunilor sale de securitate; se asigură că aceste persoane sunt competente pe baza educației, formării sau experienței corespunzătoare; dacă este cazul, întreprinde acțiuni pentru a dobândi competențele necesare și pentru a evalua eficacitatea acțiunilor întreprinse; păstrează informațiile documentate corespunzătoare ca dovadă a competenței.

Obiectivele de formare definite ar trebui să se bazeze pe evaluarea riscurilor și să faciliteze uniformitatea și standardizarea cerințelor de formare.



Identificarea competențelor

Organizația trebuie să stabilească, să implementeze și să mențină proceduri pentru a se asigura că persoanele care îndeplinesc sarcini de securitate în numele său demonstrează un nivel adecvat de competență în fiecare dintre următoarele domenii:

- ❑ îndeplinirea funcțiilor lor de securitate;
- ❑ evaluarea riscurilor;
- ❑ gestionarea riscurilor identificate în evaluarea riscurilor și a potențialelor efecte asupra drepturilor omului asociate muncii lor;
- ❑ legile locale și internaționale aplicabile, inclusiv drepturile penale, drepturile omului și legile umanitare internaționale.

Pregătirea și evaluarea competențelor

Organizația trebuie să ofere instruire bazată pe competențe și să stabilească un mijloc de măsurare a gradelor de competență sau a nivelurilor de competență.

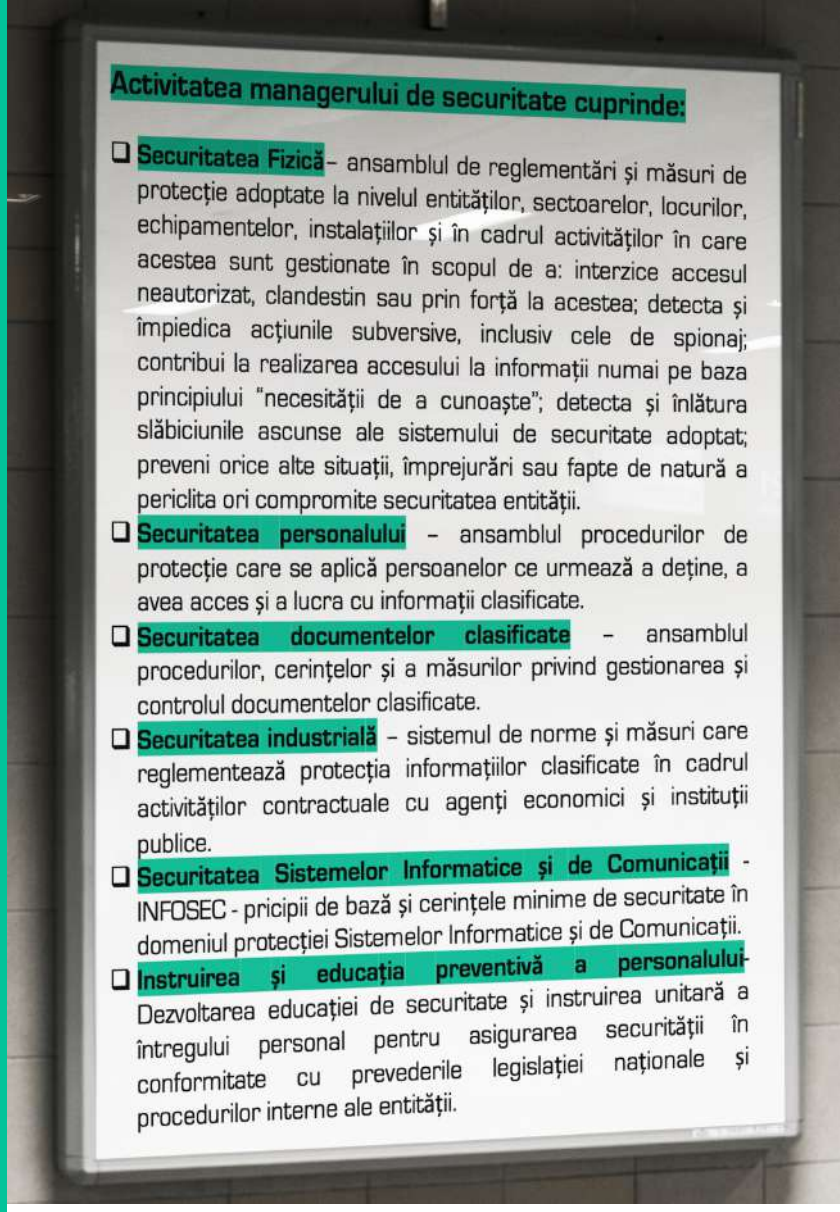
Persoanele care lucrează în numele organizației trebuie să fie instruite pentru a demonstra nivelul de competență necesar.

[14]
MANAGERUL DE SECURITATE
- PROFESIA -

Conform standardului ocupațional "managerul de securitate, sub conducerea managerului general și în colaborare cu alți conducători , organizează activitatea compartimentului de specialitate, avizează recrutarea si formarea personalului din subordine, urmăreşte randamentul şi eficienţa activităților, reprezintă organizaţia în relaţiile cu terţi."

Activitatea managerului de securitate este o activitate obiectivă care asigură echipei de conducere informațiile necesare şi cunoştinţele suficiente despre cadrul de desfăşurare al procesului de management al securității, astfel încât obiectivele entității să fie îndeplinite.

Pregătirea profesională pentru a deveni "Manager de securitate" se efectuează de furnizori de formare profesională autorizați conform legii pe baza Standardului Ocupațional și a Programei Cadru avizată de Inspectoratul General al Poliţiei Române - Direcţia de Ordine Publică.



În România, ocupația de Manager de Securitate ˝Cod COR 121306 se află pe ˝Lista profesiilor și ocupațiilor pentru care există cerințe speciale la organizarea pregătirii profesionale˝ iar cursul de formare profesională este organizat în baza Standardului Ocupațional și a Programei-Cadru avizată de Inspectoratul General al Poliției Române (I.G.P.R.)

[15]
PLANIFICAREA ȘI CONTROLUL OPERAȚIONAL

O organizație ar trebui să evalueze acele operațiuni care sunt asociate cu riscurile semnificative identificate și ar trebui să se asigure că acestea sunt conduse într-un mod care va controla sau reduce probabilitatea și consecințele negative asociate acestora pentru a îndeplini cerințele politicii sale de securitate. Aceasta ar trebui să includă toate părțile operațiunilor sale, inclusiv subcontractantul, lanțul de aprovizionare și activitățile de întreținere.

Este nevoie de utilizarea unor proceduri documentate pentru a controla situațiile în care absența acestora ar putea duce la abateri de la politica de management al operațiunilor de securitate.

Pentru a minimiza probabilitatea unui eveniment nedorit sau perturbator, aceste proceduri ar trebui să includă controale administrative, operaționale și tehnologice. În cazul în care aranjamentele existente sunt revizuite sau sunt introduse noi aranjamente care ar putea avea un impact asupra operațiunilor și activităților, organizația ar trebui să ia în considerare reducerea la minimum a amenințărilor și riscurilor asociate înainte de implementarea lor.

Organizația se asigură că procesele externalizate sunt controlate.

Organizația trebuie să planifice, să implementeze și să controleze procesele necesare pentru a îndeplini cerințele și pentru a pune în aplicare acțiunile de abordare a riscurilor și oportunităților prin:

- ❑ stabilirea criteriilor pentru procese;
- ❑ implementarea controlului proceselor în conformitate cu criteriile;
- ❑ păstrarea informațiilor documentate pentru a avea încredere că procesele au fost desfășurate conform planificării.

Organizația identifică activitățile asociate cu riscurile semnificative identificate și în concordanță cu politica sa de management, a operațiunilor de securitate, evaluarea riscurilor și a obiectivelor, pentru a se asigura că acestea sunt desfășurate în condiții specificate, ceea ce îi va permite să:

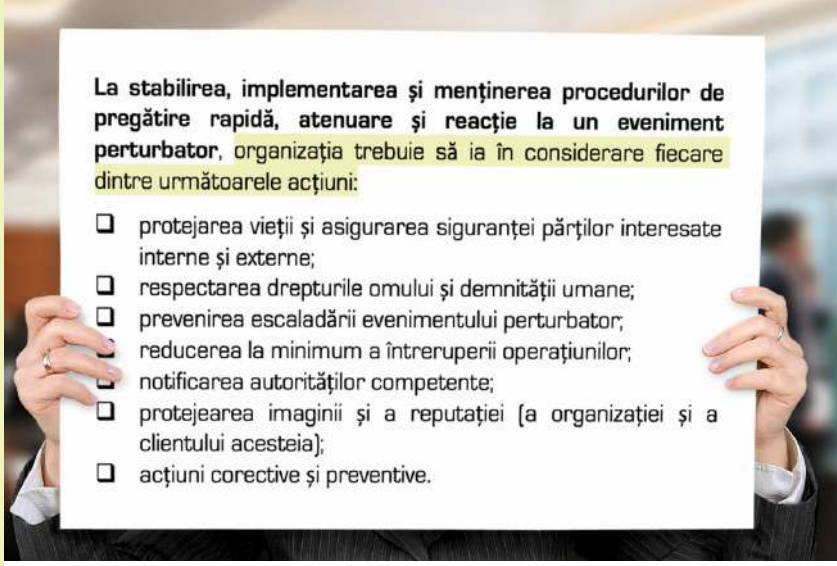
- ❑ respecte cerințele legale și alte cerințe de reglementare, inclusiv permisele și licențierea operațiunilor sale;
- ❑ îndeplinească misiunea protejând în același timp reputația clientului;
- ❑ respecte legile naționale și internaționale, inclusiv legile internaționale umanitare și drepturile omului;
- ❑ asigure securitatea, bunăstarea și drepturile persoanelor care lucrează în numele organizației;
- ❑ respecte drepturile comunităților locale;
- ❑ implementeze controale de management al riscurilor pentru a minimiza probabilitatea și consecințele unui eveniment perturbator sau nedorit;
- ❑ atingă obiectivele operațiunilor de securitate.

[16]
MANAGEMENTUL INCIDENTELOR DE SECURITATE

Organizația trebuie să stabilească, să implementeze și să mențină proceduri pentru identificarea evenimentelor nedorite și perturbatoare care pot avea impact asupra organizației, activităților sale, serviciilor, părților interesate, drepturilor omului și mediului.

Procedurile trebuie să documenteze modul în care organizația va preveni în mod proactiv, va atenua și va răspunde la evenimente.

Reclamațiile care presupun posibile infracțiuni, încălcări ale drepturilor omului sau pericole iminente pentru indivizi vor fi tratate imediat de către organizație și alte autorități, după caz



Monitorizarea incidentelor, raportarea și investigațiile

Organizația trebuie să stabilească, să pună în aplicare și să mențină proceduri de raportare a monitorizării incidentelor, investigații, aranjamente disciplinare și remediere.

Incidentele se raportează și se investighează cu următoarele măsuri luate, inclusiv:

- ❑ documentația incidentului;
- ❑ notificarea autorităților competente;
- ❑ măsurile luate pentru investigarea incidentului;
- ❑ identificarea cauzelor de bază;
- ❑ acțiuni corective și preventive întreprinse;
- ❑ orice despăgubire și despăgubire acordată părților afectate.

Proceduri interne și externe de rezolvare a reclamațiilor

Organizația va stabili proceduri pentru documentarea și soluționarea reclamațiilor primite de la părțile interesate interne și externe (inclusiv clienții și alte părți afectate).

Criteriile de eficacitate pentru procedurile de reclamație trebuie stabilite și documentate. Organizația va investiga acuzațiile în mod rapid și imparțial, cu respectarea cuvenită a confidențialității și a restricțiilor impuse de legislația în vigoare.

Organizația trebuie să stabilească și să documenteze procedurile pentru:

- ❑ primirea și soluționarea reclamațiilor;
- ❑ stabilirea etapelor ierarhice pentru procesul de rezoluție;
- ❑ investigarea reclamațiilor, inclusiv proceduri pentru;
  1. cooperarea cu mecanismele oficiale de investigații externe;
  2. prevenirea intimidării martorilor sau zădărnicirea colectării probelor;
  3. protejearea persoanele de represalii care depun o reclamație cu bună-credință.
- ❑ identificarea cauzelor de bază;
- ❑ măsuri corective și preventive întreprinse, inclusiv măsuri disciplinare proporționale cu orice infracțiune;
- ❑ comunicări cu autoritățile competente.

[17]
MONITORIZARE, MĂSURARE, ANALIZĂ ȘI EVALUARE

Organizația trebuie să evalueze performanța operațiunilor de securitate și eficacitatea Sistemului de Management al Operațiunilor de Securitate (SMOS).

Organizația evaluează planurile, procedurile și capacitățile de gestionare a operațiunilor de securitate prin evaluări periodice, teste, rapoarte postincidente, lecții învățate, evaluări ale performanței și exerciții.

Modificările semnificative ale acestor factori trebuie reflectate imediat în proceduri.

Organizația ține evidența rezultatelor evaluărilor periodice și păstrează informațiile documentate corespunzătoare ca dovadă a rezultatelor.

Organizația trebuie să stabilească, să implementeze și să mențină măsurători și proceduri de performanță pentru a monitoriza și măsura, în mod regulat, acele caracteristici ale operațiunilor sale care au un impact semnificativ asupra performanței sale (inclusiv parteneriatele, subcontractele și relațiile din lanțul de aprovizionare).

Procedurile trebuie să includă documentarea informațiilor pentru a monitoriza performanța, controalele operaționale aplicabile și conformitatea cu obiectivele și țintele de gestionare a operațiunilor de securitate ale organizației.

Organizația trebuie să evalueze și să documenteze performanța sistemelor care îi protejează activele (umane și fizice), precum și a sistemelor sale de comunicații și informații.

Exerciții și teste

Organizația va utiliza exerciții și alte mijloace pentru a testa adecvarea și eficacitatea planurilor, proceselor și procedurilor sale SMOS, inclusiv relațiile cu părțile interesate și interdependențele subcontractanților.

Exercițiile scenariilor operaționale și de gestionare a incidentelor trebuie să abordeze problemele identificate în evaluarea riscurilor, precum și să testeze stresul procedurile de gestionare a riscurilor pentru a identifica potențiale probleme sau puncte slabe.

Exercițiile vor fi efectuate în mod regulat (cel puțin anual) sau în urma unor modificări semnificative ale misiunii și/sau structurii organizației sau în urma modificărilor semnificative ale mediului extern.

După fiecare exercițiu se va scrie un raport oficial.

Raportul va evalua adecvarea și eficacitatea planurilor, proceselor și procedurilor SMOS ale organizației, inclusiv neconformitățile și va propune acțiuni corective și preventive.

[18]
AUDITUL INTERN ȘI REVIZUIREA MANAGEMENTULUI

Este esențial să se efectueze audituri interne ale Sistemului de Management al Operațiunilor de Securitate (SMOS) pentru a se asigura căacesta își atinge obiectivele, că se conformează aranjamentelor planificate, că a fost implementat și întreținut în mod corespunzător și pentru a identifica oportunități de îmbunătățire.

Auditurile interne ale SMOS ar trebui să fie efectuate la intervale planificate pentru a determina și furniza informații către Top management cu privire la adecvarea și eficacitatea sa, precum și pentru a oferi o bază pentru stabilirea obiectivelor pentru îmbunătățirea continuă a performanței acestuia.

Top managementul va revizui SMOS, la intervale planificate, pentru a asigura adecvarea și eficacitatea continuă a acestuia.

Această revizuire include evaluarea oportunităților de îmbunătățire și a necesității modificărilor SMOS, inclusiv a politicii și obiectivelor sale.

Rezultatele analizelor trebuie să fie clar documentate și să se păstreze înregistrări.

Organizația trebuie să stabilească, să pună în aplicare și să mențină un program de audit al Sistemului de Management al Operațiunilor de Securitate (SMOS) și să efectueze audituri interne la intervale planificate pentru a furniza informații dacă SMOS:

a. este conform cu:
   - cerințele proprii ale organizației pentru SMOS;
   - obligațiile legale, de reglementare, de drepturile omului și contractuale relevante;
   - cerințele standardului internațional *"ISO 18788: 2015 Sistem de gestionare a operațiunilor de securitate privată"*;
b. este implementat și întreținut în mod eficient și corect;
c. funcționează conform așteptărilor;
d. a fost eficient în realizarea politicii, obiectivelor și obiectivelor SMOS ale organizației.

Organizația trebuie să:

a. planifice, stabilească, implementeze și să mențină un program (programe) de audit, inclusiv frecvența, metodele, responsabilitățile, cerințele de planificare și raportare, care trebuie să ia în considerare starea și importanța proceselor și domeniilor în cauză și a rezultatelor auditurilor anterioare;
b. definească criteriile de audit, frecvența domeniului de aplicare, metodele, responsabilitățile, cerințele de planificare și raportarea pentru fiecare audit;
c. selecteze auditori și să efectueze audituri pentru a asigura obiectivitatea și imparțialitatea procesului de audit (de exemplu, auditorii nu ar trebui să își auditeze propria activitate);
d. se asigure că rezultatele auditurilor sunt raportate managementului relevant pentru zona care face obiectul auditului;
e. păstreze informații documentate ca dovezi ale implementării programului de audit și ale rezultatelor auditului.

Managementul responsabil de zona care face obiectul auditului se asigură că se iau măsuri fără întârzieri nejustificate pentru a elimina neconformitățile detectate și cauzele acestora.

Activitățile de urmărire includ verificarea acțiunilor întreprinse și raportarea rezultatelor verificării.

[19]
NECONFORMITĂȚI ȘI ACȚIUNI CORECTIVE

Organizația ar trebui să stabilească proceduri eficiente pentru a se asigura că neîndeplinirea unei cerințe, incidentele și punctele slabe asociate cu Sistemul de Management al Operațiunilor de Securitate (planurile și procedurile sale) sunt identificate și comunicate în timp util pentru a preveni apariția ulterioară a situației de neconformitate.

Procedurile ar trebui să permită detectarea, analizarea și eliminarea continuă a cauzelor reale și potențiale ale neconformităților.

Ar trebui efectuată o investigație a cauzei (cauzelor) rădăcină a oricărei neconformități identificate pentru a dezvolta un plan de acțiuni corective pentru abordarea imediată a problemei; pentru a atenua orice consecințe și pentru a face modificările necesare de corectare a situației cu scopul restabilirii operațiunilor normale de securitate.

Natura și momentul acțiunilor ar trebui să fie adecvate dimensiunii și naturii neconformității și consecințelor sale potențiale.

Organizația ar trebui să ia măsuri pentru a elimina cauza neconformităților asociate cu implementarea și funcționarea SMOS pentru a preveni reapariția acestora.

Procedurile documentate pentru acțiunile corective ar trebui să definească cerințe pentru:

- ❑ identificarea oricăror neconformități;
- ❑ determinarea cauzelor neconformităților;
- ❑ evaluarea necesității acțiunilor pentru a se asigura că neconformitățile nu se repetă;
- ❑ determinarea și implementarea acțiunii corective necesare;
- ❑ înregistrarea rezultatelor acțiunilor întreprinse;
- ❑ revizuirea acțiunilor corective luate și a rezultatelor acelei acțiuni.

Organizația trebuie să stabilească, să pună în aplicare și să mențină proceduri pentru tratarea neconformităților și pentru luarea de măsuri corective și preventive; procedurile trebuie să definească cerințele pentru identificarea și corectarea neconformităților și luarea de măsuri pentru a atenua consecințele acestora.

Atunci când apare o neconformitate, organizația trebuie să:

a. reacționeze la neconformitate și, după caz:
   - acționează pentru a o controla și a o corecta;
   - se ocupe de consecințe;
b. evalueze necesitatea acțiunii pentru a preveni neconformitățile și a elimina cauzele neconformității, pentru ca aceasta să nu se repete sau să apară în altă parte, prin:
   - revizuirea neconformității;
   - determinarea cauzelor profunde ale neconformității;
   - determinarea dacă există neconformități similare sau ar putea să apară;
c. investigheze neconformitățile, determinând cauzele acestora și luând măsuri pentru a evita reapariția acestora;
d. implementeze orice acțiune adecvată necesară și concepută pentru a evita apariția acestora;
e. revizuiască eficacitatea oricărei acțiuni corective și preventive întreprinse;
f. înregistreze rezultatele acțiunilor corective și preventive întreprinse;
g. să facă modificări la SMOS, dacă este necesar.

Acțiunile corective trebuie să fie adecvate efectelor neconformităților întâlnite.

Organizația păstrează informații documentate ca dovadă a:

- natura neconformităților și orice acțiuni ulterioare întreprinse;
- rezultatele oricărei acțiuni corective.

[20]
ANALIZA GAP

O organizație ar trebui să cunoască poziția sa actuală în ceea ce privește managementul riscurilor de securitate potențiale prin intermediul unei analize a decalajelor existente (analiza GAP).

O analiză GAP permite organizației să își compare performanța reală cu performanța potențială necesară pentru a-și îndeplini obiectivele de securitate.

Analiza ar trebui să ia în considerare riscurile organizației (inclusiv impacturile potențiale) ca bază pentru stabilirea unui Sistem de Management al Operațiunilor de Securitate (SMOS).

În toate cazurile, trebuie avute în vedere operațiunile și funcțiile din cadrul organizației, relațiile acesteia cu părțile interesate relevante și condițiile potențial perturbatoare și de urgență.

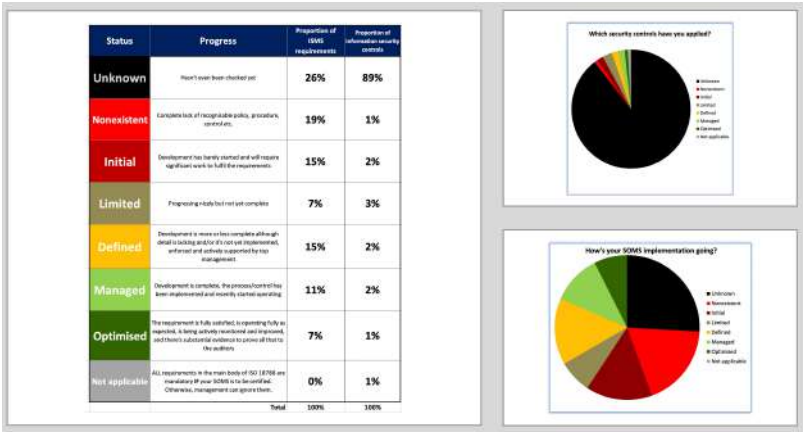
Instrumentele și metodele pentru efectuarea unei analize GAP pot include liste de verificare, efectuarea de interviuri, inspecție și măsurare directă sau rezultate ale auditurilor anterioare sau ale altor revizuiri, în funcție de natura activităților.

Analiza GAP ar trebui să acopere cinci domenii cheie:

1. **identificarea riscurilor**, inclusiv a celor asociate condițiilor de operare, situațiilor de urgență, accidentelor și evenimentelor potențiale nedorite și perturbatoare;
2. **analiza riscurilor** privind drepturile omului pentru a determina gravitatea impactului operațiunilor de securitate ale organizației și pentru a identifica oportunități de îmbunătățire;
3. **identificarea cerințelor legale** aplicabile și a altor cerințe la care organizația subscrie;
4. **evaluarea practicilor și procedurilor** existente de gestionare a riscurilor;
5. **evaluarea situațiilor de urgență** și a accidentelor anterioare, precum și a măsurilor anterioare luate pentru a preveni și a răspunde la evenimente nedorite și perturbatoare.

ANALIZA GAP
Sistem de Management al Operațiunilor de Securitate

Clause	ISO 18788 requirement	Status	Notes
4	**Context of the organisation**		
4,1	**Organisational context**		
4.1	Determine the aims of your organisation's SOMS and any issues that might affect its effectiveness	Initial	
4,2	**Interested parties**		
4.2 (a)	Identify interested parties including applicable laws, regulations, contracts etc.	Defined	
4.2 (b)	Determine those parties' security relevant requirements and obligations	Optimised	
4,3	**SOMS scope**		
4.3	Determine and document the scope of your SOMS	Managed	
4,4	**Security operations management system (SOMS)**		
4.4	Establish, implement, maintain and continually improve your SOMS according to the standard	Limited	
5	**Leadership**		
5,1	**Leadership and commitment**		
5.1	Top management must demonstrate leadership and commitment to the SOMS	Defined	
5,2	**Policy**		
5.2	Document the security policy	Nonexistent	
5,3	**Organisational roles, responsibilities and authorities**		
5.3	Assign and communicate security roles and responsibilities	Unknown	
6	**Planning**		
6,1	**Actions to address risks and opportunities**		
6.1.1	Design/plan the SOMS to satisfy the requirements, addressing risks and opportunities	Nonexistent	
6.1.2	Define and apply a security risk assessment process	Managed	
6.1.3	Document and apply a security risk treatment process	Initial	
6,2	**Security objectives and plans**		
6.2	Establish and document the security objectives and plans	Initial	



[21]
CONSULTANȚĂ GDPR

Vă pot ajuta să respectați și să implementați cerințele Regulamentului General privind Protecția Datelor (GDPR) cu o metodologie simplă în patru pași pe care am denumit-o "iQS GDPR Approach".

Fiecare pas este alcătuit dintr-o serie de activități de sprijin.

Cerința principală este ca fiecare etapă să fie finalizată într-o secvență iterativă cu scopul de a îndeplini obiectivul principal: executarea cu succes a fiecărei operațiuni.

Această metodologie este integrată într-un plan general.

Serviciile mele pot fi angajate pentru întregul pachet "iQS GDPR Approach" situație în care vom aborda planul general complet sau doar pentru unul sau mai mulți pași din planul general.

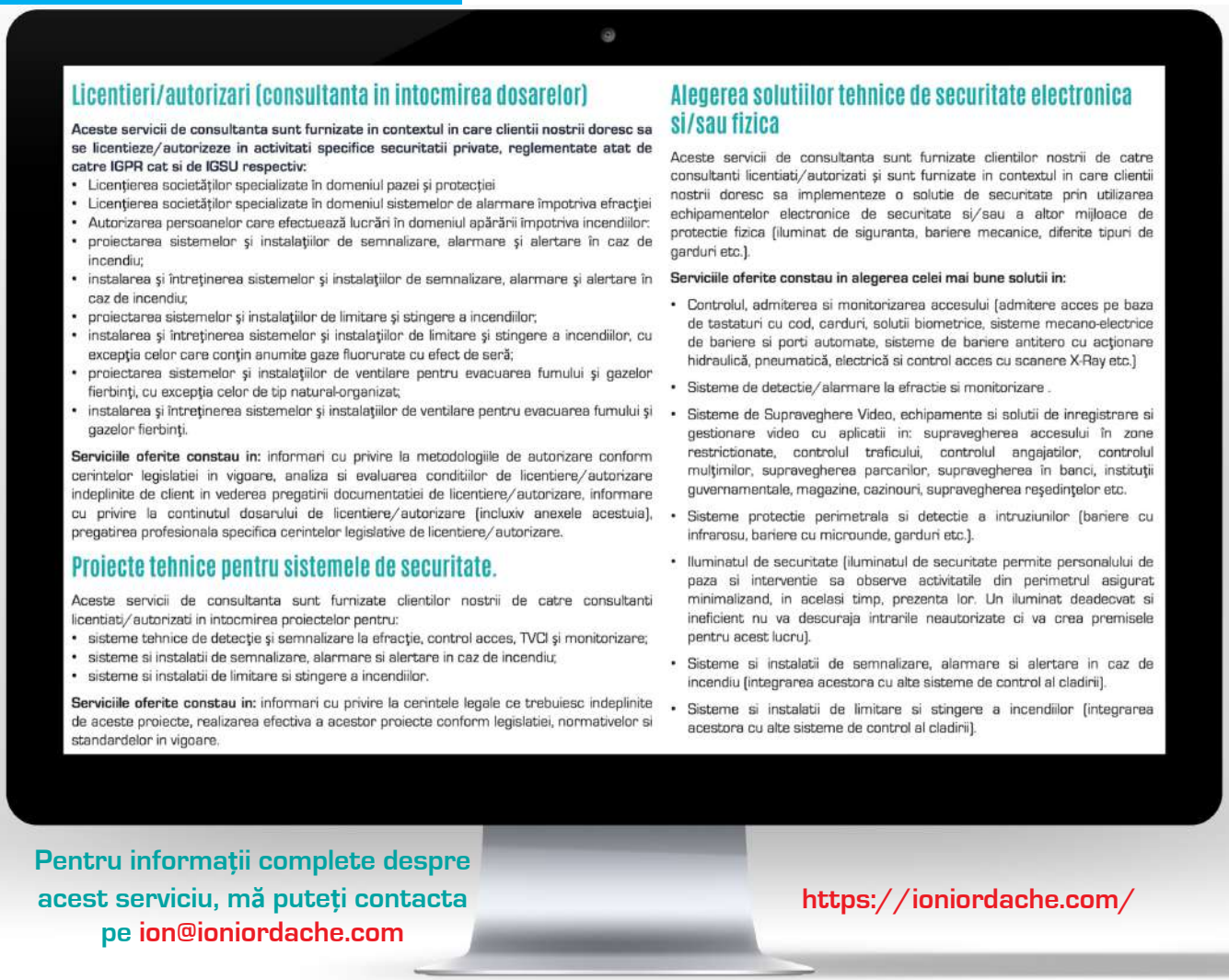
Pentru informații complete despre acest serviciu, mă puteți contacta pe ion@ioniordache.com

https://ioniordache.com/

[22]
CONSULTANȚĂ SECURITATE

iQuality Services

Metodologia de consultanță de securitate "Security Management Solutions" (SMS) propusa de **iQuality Services** este o alternativa la modelul traditional de management al securitatii ce ofera o serie de soluții la problemele companiilor de securitate.



Pentru informații complete despre acest serviciu, mă puteți contacta pe ion@ioniordache.com

https://ioniordache.com/

Managementul proiectelor de securitate fizică

Aceste servicii de consultanta sunt furnizate in contextul in care clientii nostrii accepta si inteleg importanta managementului de securitate fizică pe care le desfasoara si doresc sa faca acest lucru utilizand o metodologie moderna de management al proiectelor.

Serviciile oferite constau in consultanta si sprijin direct in urmatoarele grupe de procese:

1. initiere;
2. planificare;
3. executie;
4. monitorizare si control;
5. incheierea.

[23]
FORMARE PROFESIONALĂ GDPR

RQM CERT, furnizor de formare profesionala organizează în România atât cursuri acreditate de **Autoritatea Națională pentru Calificări (ANC)** în baza Standardelor Ocupaționale și a Programelor Cadru cât și cursuri ca provider pentru **PECB** („PECB Group Inc.") care este un organism internațional de educație și certificare în conformitate cu ISO/IEC 17024 pentru programele de certificare a personalului.

https://rqmcert.com

Responsabil cu protecția datelor cu caracter personal

(Cod COR: 242231)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educaţiei.

Cursul este recomandat persoanelor desemnate de organizațiile din sectorul public și/sau privat ca Responsabil cu Protectia Datelor cu Caracter Personal (DPO) conform cerințelor GDPR.

https://rqmcert.com

GDPR - Foundation

Certificat de absolvire eliberat de **PECB**.

Curs de formare introductiv care vă permite să înțelegeți conceptele de bază și cerințele GDPR.

- Înțelegeți conceptele de bază și componentele protecției datelor.
- Înțelegeți principiile, provocările, problemele de protecție a datelor și importanța unui responsabil cu protecția datelor, a unui operator și a unui procesator.
- Înțelegeți conceptele, abordările, metodele și tehnicile pentru protecția eficientă a datelor.

https://rqmcert.com

PECB | Data Protection Officer

GDPR - Certified Data Protection Officer

Certificat de absolvire eliberat de **PECB**.

Cursul de formare vă permite să dobândiți cunoștințele și abilitățile necesare și să dezvoltați competența de a îndeplini rolul Responsabilului cu Protecția Datelor într-o implementare a programului de conformitate cu GDPR.

După ce ați trecut cu succes examenul, puteți solicita acreditarea ca

PECB Certified Data Protection Officer.

[24]
FORMARE PROFESIONALĂ SECURITATE

În România, ocupațiile din domeniile sistemelor de securitate private și apărării împotriva incendiilor se află pe ˝Lista profesiilor și ocupațiilor pentru care există cerințe speciale la organizarea pregătirii profesionale˝ iar cursurile de formare profesională sunt organizate de către **RQM CERT**, furnizor de formare profesionala acredita de **Autoritatea Națională pentru Calificări (ANC)** în baza Standardelor Ocupaționale și a Programelor Cadru avizate de către **Inspectoratul General al Poliției Române (I.G.P.R.)** și/sau **Inspectoratul General pentru Situații de Urgență (I.G.S.U.)**


ROMÂNIA
Seria N Nr: 0079
CERTIFICAT
DE ABSOLVIRE

ROMÂNIA
Seria N Nr: 0079
CERTIFICAT
DE ABSOLVIRE

Certificatele de competențe profesionale, eliberate de către Ministerul Muncii și Protecției Sociale și Ministerul Educației prin furnizorii de formare profesională acreditați de Autoritatea Națională pentru Calificări (ANC) fac parte din categoria actelor oficiale și sunt recunoscute la nivel național iar dacă sunt apostilate în cadrul instituției prefectului și traduse sunt recunoscute și la nivel internațional.

https://rqmcert.com

Manager de securitate
(Cod COR: 121306)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educației.

Activitatea managerului de securitate cuprinde: Securitatea Fizică * Securitatea personalului * Securitatea documentelor clasificate * Securitatea Industrială * Securitatea Sistemelor Informatice și de Comunicații (INFOSEC) și Instruirea și educația preventivă a personalului.

https://rqmcert.com

Evaluator de risc la securitatea fizică
(Cod COR: 242115)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educației.

Analiza de risc la securitatea fizică constituie fundamentul adoptării măsurilor de securitate a obiectivelor, bunurilor şi valorilor prevăzute de lege, transpuse în planul de pază şi proiectul sistemului de alarmare. Obținerea certificatului de absolvire vă va permite să solicitați înscrierea în Registrul Național al Evaluatorilor de Risc la Securitate Fizică (RNERSF)

[25] FORMARE PROFESIONALĂ SECURITATE

RQM CERT

Your Knowledge Provider

furnizor de formare profesionala acredit de Autoritatea Națională pentru Calificări (ANC)

https://rqmcert.com

https://rqmcert.com

Proiectant sisteme de securitate

(Cod COR: 215119)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educaţiei.

Modulul I - Proiectarea sistemelor tehnice de detecție și semnalizare la afracție și control acces, TVCI și monitorizare

Modulul II - Proiectarea sistemelor tehnice de detecție și alarmare la incendiu/Proiectarea instalațiilor pentru stingere automată a incendiului/Proiectarea sistemului de control și evacuare a fumului și gazelor fierbinți din construcții și de limitare a propagării fumului în caz de incendiu.

https://rqmcert.com

Tehnician Sisteme de Detecție, Supraveghere Video, Control Acces

(Cod COR: 352130)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educaţiei.

Obținerea certificatului de absolvire este obligatorie dacă intenționați să vă licențiați/autorizați propria companie la I.G.P.R./I.G.S.U. sau să lucrați în cadrul unor companii licențiate de I.G.P.R. pentru ˝instalarea, modificarea, monitorizarea, întreţinerea şi utilizarea sistemelor de alarmare împotriva efracţiei˝ sau autorizate de I.G.S.U. pentru ˝instalarea și întreținerea sistemelor și instalațiilor de semnalizare, alarmare și alertare în caz de incendiu˝.

https://rqmcert.com

Tehnician sisteme și instalații de limitare și stingere a incendiilor

(Cod COR: 742106)

Certificat de absolvire eliberat de Ministerul Muncii și Protecției Sociale și Ministerul Educaţiei.

Obținerea certificatului de absolvire este obligatoriu dacă intenționați să vă autorizați propria companie la I.G.S.U. sau să lucrați în cadrul unor companii autorizate de I.G.S.U. pentru ˝instalarea si intretinere a sistemelor si instalatiilor de limitare si stingere a incendiilor, cu exceptia celor care contin anumite gaze fluorurate cu efect de sera.˝

[26]
BIBLIOGRAFIE

- **ISO 18788:2015** Sistem de gestionare a operațiunilor de securitate privată, standard international ISO
- **SR EN ISO/IEC 27001:2018** Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Cerinţe
- **SR ISO 31000:2018** Managementul riscului. Linii directoare
- **SR EN 31010:2010** Managementul riscului. Tehnici de evaluare a riscurilor
- **Metodologia "iQS GDPR Approach",** Ion Iordache
- **Manager de securitate** (COR 121306), curs specializare, RQM Cert
- **LEGEA nr. 333 din 2003** privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor (republicată și actualizată)
- **HOTĂRÂREA nr. 301 din 2012** pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 (actualizată)
- **INSTRUCŢIUNEA nr. 9 din 1 februarie 2013** privind efectuarea analizelor de risc la securitatea fizică a unităţilor ce fac obiectul Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor
- **Phisical Asset Protection** – Standard, ASIS International
- **Security Operations Management,** Robert McCrie Professor & Chair John Jay College of Criminal Justice City University of New York
- **Security Management: A Critical Thinking Approach (Occupational Safety & Health Guide)**, Michael Land, truett Ricks, Bobby Ricks
- **Security Risk Management Body of Knowledge**, Julian Talbot, Miles Jakeman
- **Strategic Security Management**, Karim Vellani
- **Effective Security Management**, Charles A. Sennewald and Curtis Baillie

MANAGEMENTUL OPERAȚIUNILOR DE SECURITATE / GHID ILUSTRAT

Autor:

Ion Iordache, BEc

Consultant și Trainer în Managementul Securității
Data Protection Officer (DPO) și Training & Development Manager la RQM Cert,
CEO și fondator la
Iordache Quality Services (iQS),
companii care oferă servicii de consultanță și cursuri de formare în managementul securității, GDPR și sisteme de management bazate pe standardele internaționale ISO.

www.ioniordache.com ion@ioniordache.com

DATA ȘI VERSIUNEA 25.10.2021, V.00

Copii ale celei mai recente versiuni ale acestui ghid pot fi descărcate de pe https://ioniordache.com.

Dacă aveți nevoie de informații suplimentare, asistență sau recomandări cu privire la conținutul acestui document, vă rog să mă contactați la ion@ioniordache.com.

RQM Certification

RQM Certification cu sediul în Timișoara este un furnizor de formare profesională cu o echipă excepțională de specialiști cu mare experiență în formare profesională, servicii de evaluare și audit. Compania are expertiză în domeniul sistemelor de management al calității, al mediului, al sănătății și securității la locul de muncă, al automobilelor, al securității fizice, al informațiilor și al serviciilor IT. Programele de formare sunt concepute pentru a sprijini învățarea activă în conformitate cu standardele internaționale și cerințele specifice fiecărei industrii.

www.rqmcert.com
office@rqmcert.com
+40 356 173 020