9. PROGRAME DE SECURITATE CIBERNETICĂ

Preliminarii

Actualmente, securitatea cibernetică a devenit un pilon esențial în protejarea datelor și a informațiilor sensibile. Amenințările cibernetice au evoluat și s-au diversificat în mod exponențial, afectând organizațiile la nivel mondial. Programele de securitate cibernetică sunt dezvoltate pentru a face față provocărilor complexe. În această temă sunt explorate conceptele fundamentale, tipologiile și importanța programelor de securitate cibernetică, analizate metodele și instrumentele utilizate pentru a preveni, a detecta și a răspunde la incidentele de securitate. Înțelegerea acestor aspecte este crucială pentru dezvoltarea unor strategii eficiente de protecție împotriva amenințărilor cibernetice în diverse sectoare, inclusiv în domeniul guvernamental, corporativ și educațional.

Scopul:

- *studierea elementelor constitutive ale programelor de securitate cibernetică și a reglementărilor în domeniu pentru a înțelege cum poate fi implementat și gestionat un astfel de program în organizații.*

Obiectivele educaționale:

- *explicarea importanței politicilor de securitate și identificarea diferitor tipuri de politici de securitate;*
- *gescrierea standardelor de securitate din industrie, detalierea procedurilor și liniilor directoare;*
- *identificarea rolurilor-cheie de securitate și implementarea programelor de îmbunătățire continuă.*

Finalitățile de referință:

- *capacitatea de a identifica, analiza și evalua elementele constitutive ale programelor de securitate cibernetică, așa cum sunt politicile de securitate;*
- *capacitatea de a analiza necesitățile organizațiilor cu privire la programele de securitate cibernetică;*
- *cunoașterea și aplicarea politicilor de securitate, standardelor, practicilor și procedurilor pentru a spori securitatea cibernetică în organizații.*

Modalitățile de evaluare

Evaluarea masteranzilor se va efectua în baza testelor formative realizate pe parcursul semestrului de studiu, care vor conține întrebări de tip grilă, întrebări deschise și studii de caz. De asemenea, masteranzii vor îndeplini sarcini practice individuale sau de grup și vor prezenta oral o temă relevantă domeniului de securitate cibernetică. La finele semestrului masteranzii vor susține un examen care va acoperi toate temele din acest suport de curs.

9.1. Politici de securitate

Politica de securitate reprezintă o declarație oficială a filozofiei manageriale a organizației [4]. Politica de securitate este utilizată pentru a-și exprima opiniile cu privire la mediul de securitate al organizației. Această politică devine apoi bază pentru planificarea, managementul și întreținerea profilului de securitate cibernetică. Când politicile sunt proiectate, create, aprobate și implementate, tehnologiile și procedurile care sunt necesare pentru a le îndeplini pot fi proiectate, dezvoltate și implementate. Cu alte cuvinte, politicile includ un set de reguli care dictează un comportament acceptabil și inacceptabil în cadrul unei organizații. Politicile nu trebuie să specifice funcționarea corectă a echipamentelor sau

software-ului - aceste informații ar trebui să fie plasate în alte documente numite „standarde”, „proceduri”, „practici” și „orientări”. Politicile definesc ce poți face și ce nu poți, în timp ce celelalte documente se concentrează pe cum o poți face.

Politicile trebuie să specifice, de asemenea, sancțiunile pentru comportamentul inacceptabil și să definească un proces de contestație. De exemplu, o organizație care interzice vizualizarea site-urilor Web neadecvate la locul de muncă trebuie să implementeze un set de standarde care clarifică și definește exact ce înseamnă „nepotrivit” și ce va face organizația pentru a opri comportamentul nepotrivit. În implementarea unei politici de utilizare inadecvată, organizația ar putea crea un standard conform căruia tot conținutul neadecvat va fi blocat, apoi să enumere materialul care este considerat inadecvat. Mai târziu, în cadrul procesului, controalele tehnice și procedurile asociate acestora pot bloca accesul la rețea sau la site-urile Web neautorizate.

Practicile, procedurile și liniile directoare explică modul în care angajații trebuie să respecte politica de securitate.

Pentru a produce un portofoliu complet de politici de securitate, conducerea trebuie să definească trei tipuri de politici de securitate cibernetică. Cele trei tipuri de politici InfoSec sunt următoarele:

- **Politici de securitate de nivel înalt (sau organizaționale) –** sunt stabilite strategia, domeniul de aplicare și eforturile organizației, numită și politică de securitate generală, politică de securitate TIC, politică InfoSec; acestea necesită modificare doar în cazul modificărilor majore în strategiile organizației.
- **Politici de securitate specifice –** relevante pentru anumite procese sau tehnologii care utilizează tehnologiile informaționale; sunt revizuite periodic, când a fost implementată o nouă tehnologie sau în cazul anumitor incidente de securitate; conțin instrucțiuni clare de utilizare a diverselor tehnologii comunicaționale; pot fi documente modulare, independente sau cumulate într-un singur document cuprinzător.
- **Politici de securitate aplicate tehnologiilor informaționale (bazate pe sistem)** [4] – parte a procesului de configurare sau mentenanță a dispozitivelor de rețea. Pot fi manageriale, așa ca politica de securitate pentru router-e și comutatoare, sau tehnice, așa ca listele de control al accesului, configurările firewall-ului sau ale sistemelor de detecție a intruziunilor, configurarea dispozitivelor de rețea; pot fi implementate înainte de implementarea politicilor specifice și de stabilirea regulilor de utilizare a tehnologiilor informației; sunt actualizate ori de câte ori sunt identificate noi amenințări la adresa securității cibernetice.

Rolul semnificativ al politicii de securitate constă în precizarea drepturilor și responsabilităților utilizatorilor, astfel asigurându-se informarea angajaților despre atitudinea managementului superior față de securitatea cibernetică. Importanța implementării acestui document fiind una nu numai obligatorie (conform standardului ISO 27001), dar și strategică, managementul organizației este responsabil pentru elaborarea și implementarea politicilor de securitate, astfel, manifestând angajament clar de a satisface cerințele de securitate prin setarea obiectivelor pentru securitatea informațiilor, care susțin în mod direct obiectivele strategice ale organizațiilor. Obiectivele de securitate trebuie să fie măsurabile și actualizate periodic, la fel ca și cerințele de securitate [28].

Politica de securitate a informațiilor poate fi un document sau parte a politicii generale de nivel înalt. Conținutul politicii de securitate trebuie să includă declarații scurte și ușor de înțeles pentru toți angajații și partenerii de afaceri [29]. În cazul când politica de securitate conține date sensibile, aceasta poate fi distribuită prin rețeaua intranet a organizației (dacă există), prin email sau utilizând varianta imprimată. Această politică este considerată ca fiind de nivel superior. Pe lângă această politică este necesar a implementa politici de securitate care să vizeze anumite domenii specifice cum ar fi controlul accesului, securitatea fizică și de

mediu, politici orientate pe utilizatorul final, copii de rezervă, transferul informației, protecție anti-malware, managementul vulnerabilităților tehnice, controlul criptografic, comunicații securizate, protecția datelor cu caracter personal (figura 9.1).

Un rol semnificativ al politicii de securitate este acela că se precizează drepturile și responsabilitățile utilizatorilor, astfel se asigură informarea membrilor comunității despre atitudinea administrației față de securitatea cibernetică. Importanța implementării acestui document fiind una nu numai obligatorie (conform standardului ISO 27001), dar și strategică, conducerea organizației este responsabilă pentru elaborare și implementare, astfel, manifestând angajament clar de a satisface cerințele de securitate prin setarea obiectivelor pentru securitatea informațiilor, care susțin în mod direct obiectivele strategice ale organizațiilor. Obiectivele de securitate trebuie să fie măsurabile și actualizate periodic, la fel ca cerințele de securitate [30].

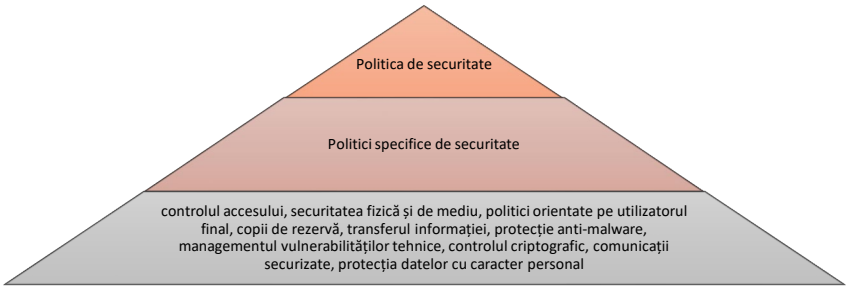

Fig. 9.1. Ierarhia politicilor de securitate [27]

Structura politicilor de securitate este propusă în tabelul 9.1 pentru elaborarea politicii de securitate generală și politicilor specifice de securitate.

Tabelul 9.1. Structura politicii de securitate manageriale [27]

1	***2***
Structura politicii de securitate	***Justificări***
Titlul	Conform prevederilor din standardul ISO 27002, titlul se referă la tehnologia informației pe care o vizează.
Versiune și responsabili de implementare	Deoarece politicile de securitate sunt documente ce necesită permanentă actualizare, este foarte important a stabili la ce versiune se află și pentru când se planifică următoarea actualizare.
Scopul	Descrie așteptările managementului organizației ca rezultat al implementării politicii de securitate.
Domeniul de aplicare	Descrie domeniul ce va fi acoperit. De exemplu: controlul accesului, securitatea comunicațiilor, utilizarea acceptabilă etc.; cui se adresează respectiva politică de securitate și în ce termene poate fi utilizată tehnologia.
Definiții	Definirea tehnologiilor informației ce urmează a fi securizată sau ale conceptelor de securitate: confidențialitate, integritate, disponibilitate, pentru a genera claritate.
Cerințele politicii de securitate	Descrie extins, cât mai clar și explicit cerințele organizației față de utilizarea tehnologiilor informației, care pot fi utilizate de către utilizatori doar pentru a îndeplini procesele de afaceri. Poate fi specificat tot în această secțiune și ce nu este permis.
Excepții	Prezintă excepțiile de la prevederile politicii de securitate, cazurile când această politică de securitate nu se aplică.

1	*2*
Penalități	Trebuie să fie clar ce va întreprinde organizația în cazul când vor fi încălcate prevederile politicii de securitate, în mod echitabil, indiferent de poziția utilizatorului în organizație.
Documente relevante	Descrie alte politici relevante (dacă există) care pot contribui la minimizarea problemelor și incidentelor de securitate sau link-uri pentru suportul adițional.

9.2. Standarde de securitate

Standardele de securitate reprezintă declarații detaliate a ceea ce trebuie făcut pentru a respecta politica de securitate, uneori văzută ca reguli care guvernează respectarea politicii. Dacă politica prevede că angajații trebuie „să folosească parole puternice, schimbate frecvent", standardul ar putea specifica că parola „trebuie să aibă cel puțin 8 caractere, cu cel puțin un număr, o literă și un caracter special".

Standardul ISO 27001 este standardul internațional ce recomandă crearea unui sistem de management al securității informațiilor (SMSI) în cadrul organizațiilor, și anume, sub acest aspect este o resursă ce trebuie preluată drept referință conceptuală în procesul de implementare a programului de securitate și care susține abordarea procesului de securitate de sus în jos [31]. Modelul PDCA (Planificare, Realizare, Verificare, Acțiune) recomandat de ISO 27001, numit ciclul lui Deming, reflectat în figura 9.2, conține un ciclu închis de acțiuni, care asistă procesele sistemice ale programelor de securitate.

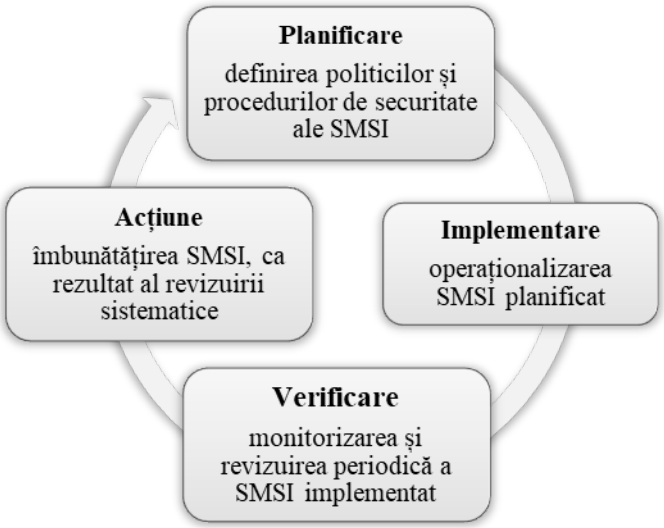

Fig. 9.2. Modelul PDCA

Ciclul lui Deming poate fi utilizat pentru a implementa un sistem de securitate al informației cuprinzător sau poate fi implementat pentru programe de securitate mai mici. Indiferent de domeniul de aplicare, protecția activelor informaționale este realizată prin implementarea SMSI [32], care are la bază evaluarea riscurilor de securitate și se axează pe triada CIA, principiile fundamentale ale securității cibernetice. Sub acest aspect, triada CIA se referă la confidențialitatea datelor și controlul accesului la activele informaționale, integritatea datelor și disponibilitatea rețelelor și a serviciilor.

Standardul ISO 27001 prevede controale de securitate divizate în 4 secțiuni: control organizațional, controlul personalului, control fizic și tehnologic, care recomandă în total 93 de controale de securitate [28]. Nu toate secțiunile standardului sunt aplicabile în organizații de un anumit profil. Decizia se ia prin elaborarea Declarației de aplicabilitate în care se stabilesc controalele de securitate implementate și se prezintă justificări privind excluderea anumitor controale de securitate, considerate irelevante pentru organizație.

Standardul ISO 27001 este generic și necesită adaptări substanțiale pentru a fi implementat în organizații de anumit profil. Controalele de securitate care se regăsesc în anexa

A a standardului ISO 27001 nu dețin instrumente operaționale, dar este important ca programul de securitate să se bazeze pe acesta.

Ghidurile (guidelines) nu sunt recomandări obligatorii pe care angajatul le poate folosi ca referință în conformitate cu o politică. Dacă politica prevede „folosiți parole puternice, schimbate frecvent", îndrumările ar putea sfătui că „vă recomandăm să nu folosiți nume de familie sau de animale de companie sau părți din numărul dvs. de identificare, ID al angajatului sau numărul de telefon în parolă".

Practicile sunt exemple de acțiuni care ilustrează conformitatea cu politicile. Dacă politica prevede „folosiți parole puternice, schimbate frecvent", practicile ar putea sfătui că „conform lui X, majoritatea organizațiilor solicită angajaților să schimbe parolele cel puțin o dată pe an".

Procedurile sunt instrucțiuni pas cu pas concepute pentru a ajuta angajații să respecte politicile, standardele și liniile directoare. Dacă politica prevede „utilizați parole puternice, schimbate frecvent", procedura ar putea recomanda că „pentru a vă schimba parola, faceți mai întâi clic pe butonul Start Windows, apoi...".

9.3. Personalul de securitate

Standardul ISO definește rolul profesioniștilor în securitatea cibernetică. Conform standardului ISO 27000 [33], organizațiile necesită:

- un manager senior responsabil pentru IT și ISM (adesea sponsorul auditului);
- profesioniști în securitatea informațiilor;
- administratori de securitate;
- managerul de securitate fizică și locația și contactele facilităților;
- contact HR pentru chestiuni de HR cum ar fi măsuri disciplinare și formare;
- manageri de sisteme și rețele, arhitecți de securitate și alți profesioniști IT.

Tipurile de poziții de securitate a informațiilor pot fi împărțite după cum urmează:

- definitorii - oferă politici, linii directoare și standarde și includ consultanți care evaluează riscurile și dezvoltă arhitecturi tehnice și de produs și persoane de nivel superior din cadrul unei organizații care au cunoștințe ample, dar nu aprofundate tehnic;
- constructorii - sunt adevărații tehnicieni care creează, instalează și configurează soluții de securitate;
- monitorii - administrează instrumentele de securitate, efectuează funcția de monitorizare a securității și îmbunătățesc procesele.

Rolurile-cheie sunt:

- ***ofițer șef pentru securitatea cibernetică/informației*** care raportează direct managementului de top al organizației, se ocupă de planificare și politicile de securitate, de calculul bugetului necesar pentru implementarea programului de securitate;
- ***manager de securitate*** cu experiență în managementul proiectelor, elaborează politici, standarde și linii directoare de nivel mediu sau inferior;
- ***analist de securitate*** care se ocupă de configurarea firewall-urilor, IDPS-urilor, implementează software de securitate, diagnostichează și depanează problemele; coordonează cu administratorii de sistem și rețea pentru implementarea corectă a tehnologiilor de securitate; deține cunoștințe tehnice și certificări industriale.

În plus, sunt incluși specialiști în evaluarea riscurilor (figura 9.3), persoane care înțeleg tehnicile de evaluare a riscului financiar, valoarea activelor organizaționale și metodele de securitate care trebuie utilizate. Indiferent dacă echipa este repartizată sau nu unui proiect de management al riscului, toate proiectele pot induce riscuri în organizație, sisteme și active informaționale. Prin urmare, este important a se asigura că riscul este examinat pe măsură ce progresează proiectul.

Fig. 9.3. Personal de securitate

De asemenea, importanți sunt și alți profesioniști în securitate cibernetică dedicați (figura 9.4), specialişti instruiţi în toate aspectele securității cibernetice atât din punct de vedere tehnic, cât și din punct de vedere non-tehnic. Echipa va include analiști de securitate suplimentari, manageri și tehnicieni care să ajute la finalizarea proiectului.

Fig. 9.4. Echipa de implemetare a securității cibernetice

La fel, este important să fie incluși administratorii de sistem corespunzători (figura 9.5), oameni cu responsabilitate principală pentru administrarea sistemelor care gestionează informațiile utilizate de organizație, dacă proiectul va presupune utilizarea sau implementarea sistemelor informatice.

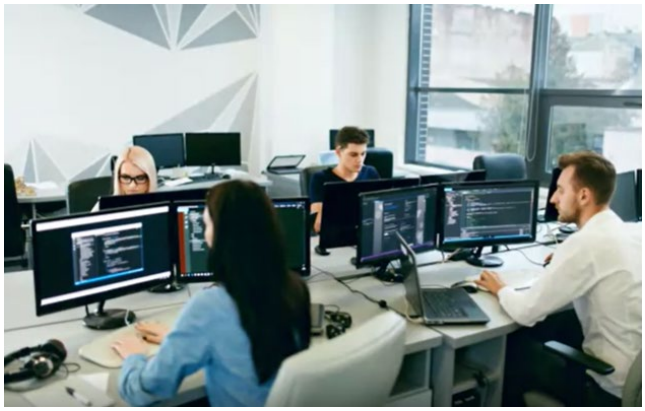

Fig. 9.5. Administatori de sistem

În cele din urmă, utilizatorii finali au un rol definitoriu în orice program de securitate, cei pe care noul sistem îi va afecta direct. În mod ideal, o selecție de utilizatori din diferite departamente, niveluri și grade de cunoștințe tehnice ajută echipa la aplicarea unor controale realiste ce nu perturbă activitățile esențiale de afaceri pe care încearcă să le protejeze. Utilizatorii sunt direct afectați de procesul și rezultatul proiectului și trebuie să fie incluși în procesul de securitate cibernetică.

Numărul profesioniștilor în securitate cibernetică va varia în funcție de mărimea și structura organizației, industria din care face parte, maturitatea și bugetul său atât pentru IT, cât și pentru securitatea cibernetică. Există mai multe opțiuni valide pentru poziționarea departamentului de securitate cibernetică în cadrul organizației.

9.4. Programe de îmbunătățire continuă

Când este implementat un program de securitate cibernetică, organizația va dori să-și îmbunătățească programul. Acest lucru se face de obicei printr-un program de îmbunătățire continuă, în care organizația programează o revizuire periodică a performanțelor sale în toate domeniile, apoi caută modalități de îmbunătățire.

Cea mai comună metodă de a face aceasta este prin stabilirea mai întâi a unei baze sau set de criterii după care vor fi evaluate performanțele viitoare. De asemenea, organizația poate planifica un obiectiv final dorit spre care să se lucreze. Apoi periodic, să zicem în fiecare an, organizația face o altă evaluare. Organizația își compară apoi rezultatele cu anii precedenți. Evaluarea în fiecare an este, de asemenea comparativă cu scopul final sau obiectivele. Stabilirea acelui set inițial de măsurători se numesc BASELINE și comparația viitoare față de performanțele anterioare sau obiectivele viitoare dorite este evaluarea comparativă, sau mai precis, *benchmarking intern*.

Diferența dintre orice criteriu și scop este decalajul de performanță. Se face cam același lucru când se calcă pe un cântar. Este posibil de avut o valoare de referință de la ultima vizită la medic. Poate că doctorul a recomandat a pierde o anumită greutate. Cântărirea săptămânală și compararea acestor valori cu ultima vizită la medic până la atingerea obiectivului final. O altă abordare pe care o poate adopta o organizație pentru a-și îmbunătăți programele sale de securitate cibernetică este de a compara eforturile sale cu ale unei instituții similare. Întregul proces se numește *benchmarking extern* [3].

Evaluarea comparativă poate implica cele mai bune practici, căutarea și studierea practicilor folosite în alte organizaţii care au rezultate ce vor fi dublate în organizație. Premisa este că atunci când o organizație face ceva foarte bine, alte organizații vor dori să o imite. De obicei, o organizație se evaluează pe ea însăși. Apoi organizația măsoară modul în care aceasta îndeplinește sarcina specifică sau altă măsură a performanței față de cea a organizației-țintă. Așadar, presupunem că compania X este recunoscută ca lider în domeniul politicii de securitate cibernetică. Compania Y dorește să elaboreze politici bune. Deci, în timpul unei conferințe de

securitate managerii celor două companii discută despre politicile de securitate necesare. Compania Y poate să-și îmbunătățească politicile pe baza recomandării managerului companiei X. Aceasta este atât o bună practică, cât și un punct de referință. Cea mai bună practică este adoptarea unei politici mai avansate, în timp ce reperul este compararea eforturile unei companii cu cealaltă. De obicei, se face benchmark și dacă compania se plasează în spatele curbei, se caută adoptarea celor mai bune practici.

Un nou nivel cunoscut sub numele de standardul de aur sunt cele mai bune practici din industrie frecvent asociate cu premii și recunoașteri la nivel de industrie.

În securitate există certificări ca de exemplu certificarea cu ISO 27001. Când se decide adoptarea unei bune practici, trebuie să se țină cont de următoarele:

- Organizația implementează deja cea mai bună practică?
- Organizația dvs. este într-o industrie similară? O strategie care funcționează bine într-o organizație de producție s-ar putea să nu funcționeze la fel de bine pentru o organizație de servicii non-profit. Se confruntă organizația dvs. cu provocări similare cu ținta? Evident, o bună practică într-o companie multinațională nu va fi aplicabilă unei afaceri mici.
- Cât poate cheltui organizația dvs. pentru implementarea programului de securitate? Dacă posibilitatea dvs. de a plăti este semnificativ limitată, nu este util să încerci să adopți o bună practică care are un cost semnificativ.
- Este organizația dvs. într-un mediu de amenințare similar cu ținta? O bună practică care a funcționat timp de câteva luni sau chiar ani poate să nu fie potrivită pentru mediul actual de amenințare. Gândiți-vă la cele mai bune practici pentru conectivitate la internet care au fost necesare pentru organizațiile moderne în 2001 și comparați-le cu cele mai bune practici de astăzi.
- Este organizația dumneavoastră la fel de matură ca ținta? O organizație nouă nu va fi la fel de stabilă ca una care există de zeci de ani. Pentru a compara ceva, mai întâi trebuie să ai o măsură de comparație. În securitatea cibernetică acestea sunt denumite criterii de performanță.

Când evaluează comparativ, o organizație folosește de obicei criterii de performanță bazate pe metrici pentru a compara programele. Criteriile bazate pe metrice se axează pe standarde numerice cum ar fi:

- numărul de atacuri reușite;
- ore petrecute de personal pentru a asigura protecția sistemului;
- bani cheltuiți pentru protecție;
- numărul personalului de securitate;
- valoarea estimată în dolari a informațiilor pierdute în atacuri reușite;
- pierderea orelor de productivitate asociate cu atacurile de succes.

O organizație folosește standarde numerice ca cele expuse mai sus pentru a se compara cu organizațiile concurente după dimensiune și/sau piața similară, apoi după rezultate se determină performanța. Lacunele de performanță oferă o perspectivă asupra domeniilor la care o organizație ar trebui să lucreze pentru a-și îmbunătăți securitatea. Uneori, din motive legale, o organizație poate fi obligată să adopte un anumit nivel minim de securitate. În acest caz, organizația poate avea nevoie să demonstreze că a făcut sau ar face orice în circumstanțe similare. Acest lucru este cunoscut ca un standard de grijă cuvenită. Dar o organizație nu poate doar face modificări, apoi să le ignore. Ei trebuie să mențină acest standard, care este cunoscut sub numele de *due diligence*.

Aplicarea controalelor la mai multe niveluri prescrise este standardul de diligență cuvenită, iar menținerea acelor standarde arată că organizația a efectuat *due diligence*. Se așteaptă ca organizația să-și mențină domeniul de securitate cibernetică complex și cuprinzător.

Prin urmare, poate fi imposibil ca o organizație să se claseze ca cea mai bună în toate categoriile.

Pe baza bugetelor alocate pentru protecția informațiilor poate fi și financiar imposibil a furniza un nivel de securitate egală cu cea a organizațiilor cu venituri mai mari. Uneori organizațiile doresc să implementeze cele mai avansate tehnologii și cele mai sigure niveluri de protecție, dar din motive financiare sau din alte motive nu pot să o facă.

Întrebări și subiecte pentru aprofundarea cunoștințelor

1. Cum poate să ajute un standard de securitate la proiectarea și implementarea unei infrastructuri securizate? Ce reprezintă guvernarea securității informațiilor?
2. Cine ar trebui să planifice programul de securitate în organizație?
3. Ce reprezintă seria de standarde ISO 27000? Ce standarde individuale alcătuiesc seria?
4. Cine sunt principalii specialiști implicați în programele de securitate în organizații? Care este rolul acestora?
5. Enumerați și descrieți succint tipurile politicilor de securitate ce trebuie implementate de către orice organizație conștientă de necesitatea asigurării securității cibernetice.
6. Care sunt etapele managementului riscului cibernetic?
7. Care sunt diferențele dintre o politică, un standard și o practică? Exemplificați fiecare categorie.
8. Ce tip de politică de securitate ar fi necesară pentru a ghida utilizarea Web? E-mail? Echipamente de birou pentru uz personal?
9. Care este rolul managementului riscului de securitate într-o organizație?
10. Ce reprezintă benchmarkingul intern și extern? Reflectați asupra exemplelor relevante.