



Cursul universitar

Gestiunea securității informatice

Lidia Popov, dr., lect. univ.

Standarde în domeniul securității informației

Plan

1. Introducere în standardizare
2. Standarde de securitate ISO/IEC 27000
3. Securitatea informației în secolul XXI
4. Standardul ISO 27001: evoluție și obiective
5. Ce este ISO 27001?
6. Implementarea standardului ISO 27001
7. Concluzii

Introducere în standardizare

„Tehnicile de securitate standardizate devin cerințe obligatorii pentru domeniul IT, pentru comerțul electronic, îngrijirea sănătății, telecomunicații, domeniul construcțiilor de mașini și pentru numeroase alte sectoare, atât în domeniul comercial, cât și în cel public.

Standardul ISO/IEC 27000:2009, precum și alte standarde din familia ISO/IEC 27000, **au ca scop** să ajute întreprinderile *să asigure mai eficient un nivel adecvat de securitate a informației*” afirmă profesorul H. Edward, unul dintre responsabilii pentru elaborarea multora dintre standardele de securitate.

Cuvintele sale au fost confirmate de-a lungul timpului de experiență avută după implementarea acestor standarde, ele având un impact major în procesul de asigurare a securității informațiilor în diversele domenii de activitate umană.



Introducere în standardizare

Securitatea informațiilor joacă un rol important în protejarea activelor unei companii, însă, deoarece nu există o formulă unică care poate garanta 100% securitatea, este nevoie de un set de criterii, reguli sau standarde pentru a contribui la asigurarea atingerii unui nivel adecvat de securitate, la utilizarea resurselor în mod eficient, la ***adoptarea celor mai bune practici de securitate***.

Rolul primordial în elaborarea standardelor îi revine **Organizației Internaționale pentru Standardizare (ISO)**, care împreună cu **Comisia Electrotehnică Internațională (IEC)**, formează un sistem internațional specializat pentru standardizarea mondială.



Introducere în standardizare

Organismele naționale, care sunt membre ale ISO și IEC, participă la dezvoltarea *standardelor internaționale* prin intermediul comitetelor tehnice. Astfel, SUA, prin intermediul Institutului Național de Standardizare (ANSI), ocupă poziția de *Secretar*, 24 de țări au statutul de Participanți (Brazilia, Franța, Regatul Unit al Marii Britanii, Coreea, Cehia, Germania, Danemarca, Italia, Canada etc.) și alte 40 de țări au statut de *Observatori*.

Standardul este, prin definiție un document stabilit prin consens și aprobat de un organism recunoscut, care furnizează pentru utilizări comune și repetate, reguli, linii directoare și caracteristici referitoare la activități și rezultatele acestora, în scopul obținerii unui grad optim de ordine într-un context dat.

Această definiție este bazată pe rolul și scopul standardelor în lume la etapa modernă și stabilește importanța standardelor pentru orice organizație/companie, plasându-le, alături de reglementările tehnice, în rândul documentelor de referință care trebuie să stea la baza politicilor și practicilor acestora.

Introducere în standardizare

Standardul este cea mai bună și cea mai simplă cale posibilă pentru a comunica, pentru a cunoaște nivelul tehnic unanim acceptat pe plan național, european sau internațional în domeniul de activitate al oricăror campanii/organizații și, nu în ultimul rând, pentru proiectarea și dezvoltarea practicilor de management.

Standardele pot să joace un rol important în legislație, în special, în reglementările tehnice. În cazul în care un legislator include standardele într-un document legal sau face referințe la ele, într-un fel sau altul, acestea obțin o calitate legală. Doar în așa mod *standardele* devin o parte a cerințelor unui anumit document legislativ sau unui anumit sistem.

La fel ca oricare altele, *standardele* pentru asigurarea securității sistemelor informatice devin esențiale în astfel de circumstanțe. *Standardele* pot defini sfera de aplicare a funcțiilor și caracteristicilor de securitate necesare, politicile de gestionare a informațiilor și a resurselor umane, criteriile de evaluare a eficacității măsurilor de securitate, tehnicile pentru evaluarea continuă a securității și monitorizarea continuă a încălcărilor securității și procedurile de tratare a securității împotriva eșecurilor.

Sistemul internațional specializat pentru standardizarea mondială

```
graph TD; A[Sistemul internațional specializat pentru standardizarea mondială] --> B[ISO]; A --> C[IEC]
```

ISO

IEC

Standarde de securitate ISO/IEC 27000

Cele mai bune practici necesare pentru crearea, dezvoltarea și întreținerea Sistemelor de Management al Securității Informației (SMSI) pentru o bună activitate a companiilor sunt incluse în familia de standarde **ISO/IEC 27000**, care conține, la momentul actual, nu mai puțin de 40 de standarde publicate, altele fiind în proces de elaborare sau sunt planificate pentru a fi elaborate ulterior. Aceste standarde de securitate sunt publicate în comun de către **ISO** și **IEC**.

Ele sunt produsul activității unor comitete sau subcomitete, sunt o comisie internațională ai cărei membri se întrunesc de două ori pe an. Standardele de SI își trag rădăcinile de la sfârșitul anilor 80 ai secolului trecut.



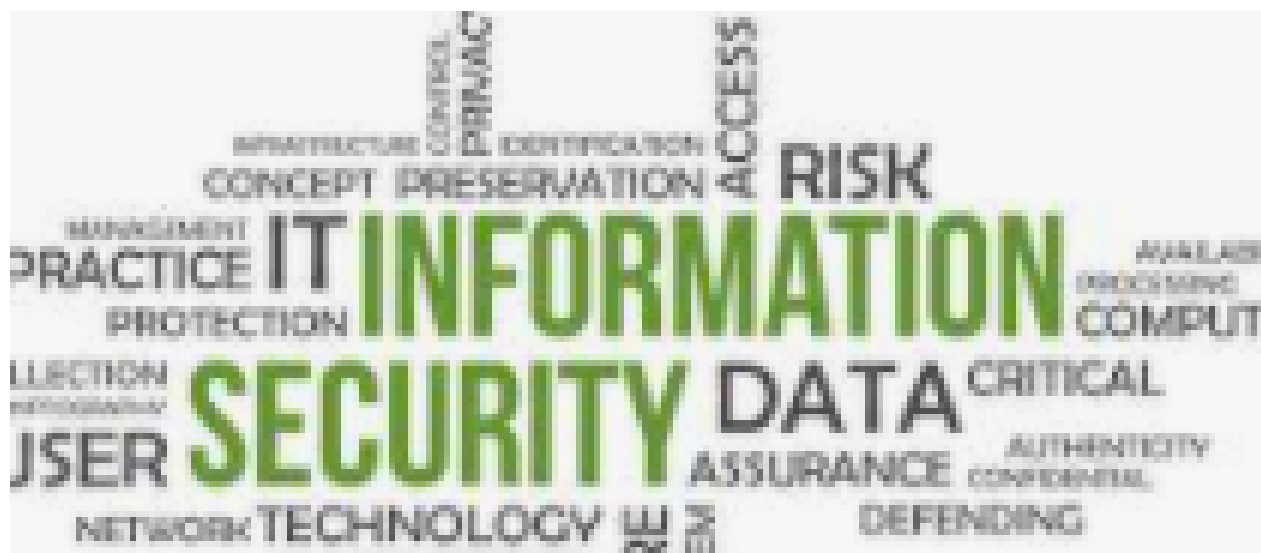
Standarde de securitate ISO/IEC 27000

Seria dispune de un domeniu larg de aplicare, care acoperă problemele conexe triadei **CIA**, dar și problemele de securitate tehnice sau IT. Aceste standarde se aplică pentru toate organizațiile, indiferent de forme și mărimi. Toate organizațiile sunt încurajate să-și evalueze riscurile de securitate a informațiilor și apoi să le trateze, în funcție de nevoile lor, folosindu-se de îndrumări și sugestii, acolo unde e cazul.

Având în vedere natura dinamică a informațiilor care trebuie protejate, SMSI încorporează un concept continuu de feedback și îmbunătățire a activităților, conform ciclului Deming **PCDA** (***Plan-Do-Check-Act***) sau ***Planifică-Implementează-Verifică-Acționează***) de abordare continuă, care caută să abordeze schimbările în amenințări, vulnerabilități de informații sau de impact asupra incidentelor de securitate.

Securitatea informației în secolul XXI

Protecția informațiilor a devenit o preocupare semnificativă pentru multe organizații. Acestea urmăresc să asigure că nimeni nu poate să fure, să utilizeze în alt mod sau să compromită ceea ce a devenit un bun valoros. Una dintre cele mai actuale probleme pe care organizațiile trebuie să le soluționeze atunci când implementează tehnologii moderne de informare este protecția informațiilor confidențiale. Această problemă este deosebit de acută în contextul aplicării legislației privind protecția datelor cu caracter personal.



Securitatea informației în secolul XXI

Informațiile pot exista în mai multe forme. Acestea pot fi tipărite sau scrise pe hârtie, stocate electronic, trimise prin e-mail sau copiate prin utilizarea mijloacelor electronice, pot fi furnizate informații video, audio sau exprimate într-o conversație. Organizațiile, precum și sistemele și rețele lor de informare se confruntă cu amenințări de securitate care provin din diverse surse, inclusiv fraudă informatică, sabotaj, vandalism, incendii sau inundații.

Pe de o parte, un canal de comunicare organizațional, care utilizează o tehnologie de rețea este o țintă pentru hackeri. Pe de altă parte, problema vulnerabilității este unul dintre efectele interconectării. Studiile recente privind securitatea informațiilor indică o tendință de creștere a încălcării securității informațiilor, ceea ce conduce la pierderi semnificative.

Securitatea informației în secolul XXI

Deoarece SI are un rol foarte important în susținerea activității organizațiilor, este oportun să existe un standard de referință care să reglementeze guvernanta în acest domeniu. Există mai multe standarde pentru guvernanta IT care fac referire la securitatea informațiilor.

Cu toate acestea, din mai multe motive, unele dintre aceste standarde nu sunt bine adoptate de organizații. Studiul comparativ, realizat pentru a determina punctele lor tari, concentrarea, componentele principale și nivelul de adoptare, a concluzionat că, la nivel mondial, standardul **ISO27001** este cel mai răspândit standard din domeniul SI.



Standardul ISO 27001: evoluție și obiective



International
Organization for
Standardization



International
Electrotechnical
Commission

Familia standardelor ISO/IEC 27000

ISO/IEC 27000:2016

ISO/IEC 27001:2013

ISO/IEC 27002:2013

ISO/IEC 27003:2017

ISO/IEC 27004:2016

ISO/IEC 27005:2011

ISO/IEC 27006:2015

ISO/IEC 27011:2016

ISO/IEC 27032:2012


ISO/IEC 27035:2016

www.iso.org/ics/35.030/x/

Standardul ISO 27001: evoluție și obiective

În prezent, atât la nivel național, cât și internațional, securitatea informațiilor a cunoscut o evoluție semnificativă în construirea unor sisteme eficiente de management al securității informațiilor (**ISMS**), reflectată într-o serie întreagă de standarde internaționale ale seriei **ISO 27000**.

Bazele implementării unui **SMSI** (Sistem de Management al Securității Informațiilor) au fost puse în anul 1990 prin publicarea unor direcții generale pentru asigurarea securității informațiilor în cadrul sistemelor și rețelelor, de către Organizația pentru Dezvoltare și Cooperare Economică (**OECD**). Aceste direcții generale au stat la baza elaborării unui cod de bune practici în SI, elaborat de către Departamentul Industriei și Comerțului al Guvernului Britanic. Ulterior, acest departament a transmis Institutului de Standardizare din Marea Britanie (**British Standards Institution, BSI**) sarcina să promoveze acest cod.



What is ISO 27001?

Standardul ISO 27001: evoluție și obiective

ISO/IEC 27001 a fost revizuit în septembrie 2013. Actuala ediție a standardului este structurată astfel încât să poată fi ușor integrată cu alte sisteme de management reglementate de **ISO**, cum ar fi sistemul de management al calității, mediului, sănătății și securității ocupaționale etc. Familia de standarde **ISO 27000** va continua să se dezvolte în mod activ. Standardul internațional **ISO 27001** specifică cerințele pentru stabilirea, implementarea, operarea, monitorizarea, revizuirea, menținerea și îmbunătățirea unui sistem **SMSI** documentat, în cadrul unei organizații.

Acesta a fost conceput pentru a asigura selectarea unor controale de securitate adecvate și proporționale pentru a proteja activele informatice. Acest standard este, de obicei, aplicabil tuturor tipurilor de organizații, private sau publice. În standard este introdus un model ciclic cunoscut sub numele de modelul Plan-Do-Check-Act (**PDCA**), care urmărește stabilirea, implementarea, monitorizarea și îmbunătățirea eficacității sistemului **SMSI** al unei organizații.

Standardul ISO 27001: evoluție și obiective

Există numeroase motive pentru a implementa standardul internațional **ISO27001**, care descrie cele mai bune practici pentru un sistem de management al **SI**. El ajută organizațiile să-și îmbunătățească securitatea, să respecte regulamentele de securitate cibernetică, să-și protejeze și să-și consolideze reputația.

Un sistem **SMSI** conform cu standardul **ISO 27001** se bazează pe evaluări periodice ale riscurilor pentru identificarea și tratarea amenințărilor de securitate, în funcție de toleranța la risc a organizației.

De asemenea, un sistem **SMSI** conform cu standardul **ISO27001** poate ajuta organizațiile să identifice și atenueze riscurile legate de **SI**, astfel încât clienții să știe că organizația pune preț pe confidențialitatea informațiilor. În prezent, Standardul **ISO/IEC 27001** este unul dintre cele mai utilizate standarde de securitate a informațiilor și prin urmare, este potrivit pentru implementarea și evaluarea diferitelor măsuri specifice.



Ce este ISO 27001?

ISO 27001



Ce este ISO 27001?

În mod evident, înainte de a obține standardul 27001, ar trebui să aflăm mai multe detalii, ar trebui să descoperim cele mai importante informații despre acest standard.

Standardul **ISO 27001** este unul internațional publicat de Organizația Internațională de Standardizare (ISO) și descrie modul de gestionare a securității informațiilor într-o companie.

Cea mai recentă revizuire a acestui standard a fost publicată în 2013, iar titlul său complet este acum **ISO/IEC 27001: 2013**, publicat pe 25.09.2013.

ISO 27001 poate fi implementat în orice tip de organizație, profit sau non-profit, privată sau de stat, mică sau mare. A fost scris de cei mai buni experți din lume în domeniul **SI** și oferă metodologie pentru implementarea managementului **SI** într-o organizație. De asemenea, permite companiilor să devină certificate, ceea ce înseamnă că un organism independent de certificare a confirmat că o organizație a implementat **SI** conform **ISO 27001**.

Standardul ISO 27001 a devenit cel mai popular standard de securitate a informațiilor la nivel mondial.

Ce este ISO 27001? Cum funcționează?

ISO 27001 vizează protejarea confidențialității, integrității și disponibilității informațiilor într-o companie.

Acest lucru se realizează prin aflarea problemelor potențiale care ar putea descoperi informațiile (de exemplu, evaluarea riscurilor) și apoi definirea a ceea ce trebuie făcut pentru a preveni astfel de probleme (adică, atenuarea riscului sau tratamentul riscurilor).

Prin urmare, filozofia principală a **ISO 27001** se bazează pe gestionarea riscurilor: este necesar de aflat unde sunt riscuri și apoi de le tratat sistematic.

Controalele care urmează să fie puse în aplicare sunt de obicei sub forma de politici, proceduri și implementare tehnică (de exemplu, software și echipamente).

Cu toate acestea, în cele mai multe cazuri, companiile au deja toate componentele hard și soft, dar le utilizează într-un mod nesigur – prin urmare, aplicarea în practică a standardului **ISO 27001** sunt legate de stabilirea regulilor de organizare (adică scrierea documentelor) care sunt necesare pentru a preveni încălcările de securitate.

Implementarea standardului ISO 27001

Standardul **ISO 27001**, ca **SMSI**, se impune din ce în ce mai mult ca standard de securitate în diverse companii. Până în prezent au fost certificate peste 5000 de organizații pe plan mondial. Cu toate acestea, înregistrarea unui sistem **SMSI** nu mai spune nimic despre calitatea și performanța implementării sale. Astfel, politicianul German B. Wolfgang a susținut că este esențial să existe un instrument care să măsoare eficiența și eficacitatea economică a implementării unui **SMSI**, bazat pe standardul **ISO 27001**, într-o companie.

Amplificarea dependenței organizaționale față de tehnologia informației, precum și agravarea impactului incidentelor de **SI**, au determinat ca anume **SI** să devină una dintre cele mai importante preocupări ale managementului. Deși, standardul **ISO 27001** oferă îndrumări pentru un **SMSI**, costurile de implementare și de acreditare pot fi, de asemenea, considerabile. Autorii studiului privind impactul certificării **ISO27001** asupra performanței organizației au constatat că, în ansamblu, majoritatea studiilor actuale privind standardul **ISO27001** se concentrează asupra procesului de implementare, inclusiv luarea deciziilor în timpul implementării, motivul și obiectivul implementării, precum și evaluarea eficienței implementării **SMSI**.

Implementarea standardului ISO27001

În opinia autorilor Susanne Dobratz et al., SI, în special în domeniul informațiilor digitale, este o condiție prealabilă pentru asigurarea încrederii. Spre deosebire de siguranță, securitatea ia în considerare, de asemenea, aspectele sociale și organizaționale. Informația este elementul de bază al unei arhive digitale, iar pentru gestionarea acestor arhive ne putem referi la standardele deja existente, în special la seria **ISO27000**. Procedurile de certificare și de autoevaluare sunt, de asemenea, abordate de această serie de standarde.

Standardul **ISO27001** oferă un model pentru stabilirea, implementarea, funcționarea, monitorizarea, revizuirea, menținerea și îmbunătățirea unui Sistem de Management al Securității Informațiilor.

SMSI ISO27001 este construit pe ideea că **SI** este determinată de evaluarea și tratarea riscurilor. Fundamental pentru succesul evaluării și tratării riscurilor este procesul de luare a deciziilor care realizează evaluarea riscului și stabilește decizii pentru acest rezultat, în ceea ce privește acțiunile de tratare.

Implementarea standardului ISO27001

Odată cu creșterea rolului tehnologiei informației, există o necesitate stringentă de măsuri adecvate pentru securitatea informațiilor. Gestionarea sistematică a securității informațiilor este una dintre cele mai importante inițiative pentru managementul IT. În contextul în care rapoartele privind încălcările vieții private și ale securității, practicile contabile frauduloase și atacurile asupra sistemelor informatice sunt publice, organizațiile și-au recunoscut responsabilitățile de a proteja bunurile materiale și informaționale. Standardele de securitate pot fi folosite ca îndrumare sau cadru pentru dezvoltarea și menținerea unui sistem adecvat de management al securității informațiilor.

Deși **SI** are un rol foarte important în susținerea activităților organizației, fiind aprobate reglementări juridice pentru a se asigura păstrarea unui nivel adecvat de securitate, pentru a asigura resursele utilizate în mod corect și pentru a asigura cele mai bune practici de securitate adoptate într-o organizație, totuși unele dintre aceste standarde nu sunt bine adoptate de organizații.

Diferite studii și experiențe de succes la nivel național și internațional, arată că punerea în aplicare a bunelor practici de implementare a ISO27001 în organizații poate reduce riscurile, amenințările și vulnerabilitățile.

Țările care cunosc această situație și țin cont de următoarele aspecte:

Orice risc sau amenințare la adresa SI poate conduce la pierderi reale și potențiale ale organizațiilor cu repercusiuni financiare, juridice și reputaționale;

Faptul că informația nu este doar valoroasă și critică, în schimb este cel mai important activ al organizației;

Organizația este vulnerabilă la o varietate de atacuri atât din interiorul, cât și din afara organizației,

au creat cadrul de reglementare pentru a proteja informații de stat.

Implementarea standardului ISO27001

Provocările în materie de securitate a informațiilor, dar și incidentele de securitate din ce în ce mai accentuate, determină practicienii și experții să își îndrepte tot mai mult atenția către aceste probleme. Respectarea standardelor de securitate a informațiilor este recomandată, deoarece asigurarea resurselor sistemului informatic este extrem de importantă pentru a garanta o protecție fiabilă a resurselor.

SI devine o componentă foarte importantă pentru activele necorporale ale organizației, nivelul de încredere și încrederea părților interesate fiind indicatori de performanță pentru organizații.

Implementarea standardului ISO 27001

Standardul internațional **ISO27001** permite organizației să stabilească un proces de securitate care optimizează în mod sistematic securitatea organizației la un anumit nivel. Acest proces conduce la o serie întreagă de avantaje:

- ✓ dovada securității față de terți (pentru clienți, parteneri și în scopuri legale);
- ✓ avantaj competitiv: calitate documentată de către o autoritate independentă;
- ✓ reducerea costurilor prin structuri transparente și optimizate;
- ✓ securitatea devine o parte integrantă a proceselor de afaceri;



Implementarea standardului ISO 27001

- ✓ cunoașterea și monitorizarea riscurilor IT și a riscurilor IT reziduale;
- ✓ documentarea structurilor și proceselor;
- ✓ creșterea conștientizării angajaților cu privire la securitate;
- ✓ evaluarea proceselor organizației din punct de vedere al securității;
- ✓ prioritizarea securității operațiunilor de afaceri: managementul continuității afacerii;
- ✓ recunoașterea standardului la nivel mondial;
- ✓ reducerea potențială a primelor de asigurare;
- ✓ referirea standardului de management al proceselor IT la ISO 27001.



De ce anume ISO 27001 este bun pentru o companie?



Cum arată ISO 27001?

ISO/IEC 27001 este împărțit în 11 secțiuni, plus o anexă, care ofera un catalog de 114 controale. Secțiunile 0 – 3 *sunt introductive* (și nu sunt obligatorii pentru implementare), în timp ce secțiunile 4-10 *sunt obligatorii* – ceea ce înseamnă ca toate cerințele lor trebuie să fie implementate într-o organizație dacă vrea să fie conform standardului respectiv.

Controalele din anexă trebuie puse în aplicare numai dacă sunt declarate ca aplicabile în Declarația de aplicabilitate.



Secțiuni introductive

0. Introducere – explica scopul ISO 27001 și compatibilitatea acestuia cu alte standarde de management.
1. Domeniul de aplicare – explica faptul că acest standard este aplicabil oricărui tip de organizație.
2. Referințe normative – se referă la ISO/IEC 27000 ca standard în care sunt dați termeni și definiții.
3. Termeni și definiții – se referă din nou la ISO/IEC 27000.

Secțiuni obligatorii

4. Contextul organizației – aceasta secțiune face parte din faza Planului în ciclul PDCA și definește cerințele pentru înțelegerea problemelor externe și interne, părțile interesate și cerințele acestora, precum și definirea sferei ISMS.
5. Conducere – aceasta secțiune face parte din faza Planului din ciclul PDCA și definește responsabilitățile de conducere superioară, stabilind rolurile și responsabilitățile și conținutul politicii de securitate a informațiilor de nivel superior.
6. Planificare – aceasta secțiune face parte din faza Planului din ciclul PDCA și definește cerințele pentru evaluarea riscurilor, tratamentul riscurilor, declarația de aplicabilitate, planul de tratare a riscurilor și stabilirea obiectivelor de securitate a informațiilor.
7. Sprijin – aceasta secțiune face parte din faza Planului din ciclul PDCA și definește cerințele privind disponibilitatea resurselor, competențelor, conștientizării, comunicării și controlului documentelor și înregistrărilor.

Secțiuni obligatorii

8. Operare – aceasta secțiune face parte din faza de Do in ciclul PDCA si definește implementarea evaluării si tratamentului riscurilor, precum si controale si alte procese necesare pentru atingerea obiectivelor de securitate a informațiilor.
9. Evaluarea performantei – aceasta secțiune face parte din faza de verificare a ciclului PDCA si definește cerințele pentru monitorizare, măsurare, analiza, evaluare, audit intern si revizuire a managementului.
10. Îmbunătățire – aceasta secțiune face parte din faza Act in ciclul PDCA si definește cerințele pentru neconformități, corecții, acțiuni corective și îmbunătățiri continue.

Concluzii

Standardul **ISO/IEC 27001** este unul dintre cele mai acceptate standarde de securitate a informațiilor și are mai multe avantaje. Acesta ajută organizațiile să-și îmbunătățească securitatea, să respecte regulamentele de securitate cibernetică, să-și protejeze și să-și consolideze reputația etc. Certificarea unui sistem ISMS conform standardului **ISO 27001** promovează, de asemenea, o imagine pozitivă prin verificarea unui management sistematic al securității informațiilor.

Standardul **ISO 27001** este de primă importanță în comparație cu alte standarde, în special în ceea ce privește **ISMS**, fiind implementat mai ușor și fiind bine recunoscut de către părțile interesate (managementul superior, personal, furnizori, clienți, autorități de reglementare).

Concluzii

Există bune practici și experiențe la nivel organizațional și național privind implementarea standardului **ISO/IEC 27001**. Există totuși anumite motive care stau la baza gradului scăzut de implementare a standardului **ISO 27001** în diverse organizații, de exemplu: probleme legate de managementul resurselor umane, cum ar fi lipsa expertizei în domeniul securității informațiilor, lipsa programelor de instruire, educație și sensibilizare, precum și costul ridicat în bani și timp, dar și cantitatea mare de documente necesare.

Mulumim pentru atenție!