THEORETICAL AND PRACTICAL CONSIDERATIONS REGARDING THE INFORMATION SECURITY MANAGEMENT SYSTEM WITHIN ORGANIZATIONS IN CONCORDANCE WITH THE NEW INTERNATIONAL STANDARD ISO/IEC 27001:2013

Bogdan Ţigănoaia, Assistant Professor, PhD, Politehnica University of Bucharest

Abstract: This paper presents theoretical aspects regarding the information security management system in an organization, such as (selection): what is an ISMS – Information Security Management System, the importance of the implementation and certification of an information security management system in an organization, a statistics regarding the global growth in certification etc. The focus point of the paper is on the structure of the new standard ISO/IEC 27001:2013. The paper also presents some practical aspects for organizations and offers answers to some Frequently Asked Questions – FAQ regarding new concepts, requirements and changes introduced in the standard, what should do an organization if it is currently certified or is interested in certifying ISO/IEC 27001 now etc.

Keywords: information security, standards, management systems, organizations, ISO.

1. Introducere

Termenul de ***informaţie*** este preluat din limba latină („informatio") prin franţuzescul „information". La începuturi, noţiunea de informaţie semnifica incertitudinea înlaturată prin realizarea unui eveniment din mai multe posibile. Informaţia poate fi măsurată şi tratată matematic la fel ca alte mărimi precum masa, lungimea, energia etc. În organizaţii, informaţia este o resursă foarte importantă pentru luarea deciziilor manageriale, dar nu numai. Comparativ cu resursa umană de exemplu, informaţiile sunt nelimitate, sunt produse şi se consumă cu rapiditate. Eficacitatea şi eficienţa unei organizaţii depind de informaţiile de care aceasta dispune. Se poate spune ca în zilele noastre informaţia înseamnă putere, în deceniile trecute resursa principală fiind capitalul. Organizaţia modernă, dinamică, de astăzi pune alături de resursa umană şi capital, informaţia, care poate fi atât o resursă de intrare într-un proces organizaţional, cât şi de ieşire.

Unul dintre pilonii de bază pentru atingerea obiectivelor organizaţionale este securitatea, implicit asigurarea ***securităţii informaţiilor*** în organizaţii. Conform literaturii de specialitate [1], o ***informaţie este securizată*** dacă sunt asigurate cele cinci atribute/funcţii de securitate (trei de funcţionalitate, două de recuperare a prejudiciului):

Atribut de securitate	Descriere
✓ *Disponibilitate*	*Atribut intrinsec al informaţiei – aceasta trebuie să fie la dispoziţia utilizatorilor legali atunci când aceştia au nevoie.*
✓ *Confidenţialitate*	*Permite blocarea accesului utilizatorilor neautorizaţi / nelegitimi la anumite informaţii*

✓ *Integritate*	*Protejează informaţia de modificări (ştergere, inserare, înlocuire etc) neautorizate/accidentale.*
✓ *Autenticitate*	*Permite asocierea informaţiei cu autorul ei (persoana sau echipament)*
✓ *Non-repudiere*	*Asociază unei informaţii dovada că aceasta a fost trimisă de către expeditor către destinatarul legal, iar acesta a primit-o, fără ca aceştia să poată contesta acest fapt (conferă informaţiei acelaşi regim ca o scrisoare recomandată).*

Un ***sistem de management*** este un *ansamblu de procese de coordonare interconectate desfăşurate în scopul direcţionării unei organizaţii către atingerea obiectivelor generale şi specifice*. Definiţii ale unui sistem de management au fost date de-a lungul timpului în diverse lucrări din literatura de specialitate sau de către organisme internaţionale, în opinia autorului de remarcat fiind definiţia B.S.I. Group, potrivit căreia *un sistem de management* este „*un cadru pentru coordonarea şi îmbunătăţirea continuă a politicilor, procedurilor şi proceselor organizaţiei”*. În particular, un ***sistem de management al securităţii informaţiilor*** - S.M.S.I. este un

ansamblu de procese manageriale interconectate în scopul direcţionării unei organizaţii în ceea ce priveşte securitatea informaţiilor. Potrivit familiei de standarde I.S.O. 27k, un sistem de management al securităţii informaţiilor este parte din întreg sistemul de management al organizaţiei, bazată pe o abordare a riscurilor afacerii, folosită pentru a stabili, implementa, funcţiona, monitoriza, revizui, menţine şi îmbunătăţii securitatea informaţiilor.

2. Noul standard I.S.O. / I.E.C. 27001:2013

Scopul unui S.M.S.I. este de a înţelege şi coordona toate elementele care influenţează securitatea informaţiilor într-o organizaţie. Pentru a furniza încredere clienţilor şi părţilor interesate, organizaţiile au posibilitatea să implementeze şi să certifice, printr-un organism de certificare acreditat R.E.N.A.R., un S.M.S.I. în concordanţă cu standardul internaţional I.S.O. / I.E.C. 27001:2013. Acest standard furnizează cerinţe pe care organizaţia trebuie să le îndeplinească pentru a fi certificată. Printr-un S.M.S.I., organizaţia exprimă importanţa asigurării securităţii informaţiilor. (adaptare după [1]). De ce este necesară ***implementarea şi certificarea*** unui S.M.S.I.? În rapoartele statistice se confirmă ceeea ce experţii în securitatea informaţiilor susţin [2]:

- ✓ securitatea informaţiilor depinde de oameni mai mult decât de tehnologie;
- ✓ securitatea informaţiilor este ca un lanţ – este atât de puternică precum cea mai slabă verigă;
- ✓ angajaţii reprezintă o ameninţare mai mare la adresa securităţii informaţiilor decât cei din afara organizaţiei;

- ✓ securitatea informaţiilor nu este un status, ci un proces ce presupune o continuă dinamică;
- ✓ securitatea informaţiilor nu este un capitol tehnic, adeseori managementul securităţii informaţiilor este foarte important.

Potrivit unei statistici recente a B.S.I. Group prezentată în Figura 1, în ultimii ani s-a observat o creştere a numărului de certificate, tot mai multe organizaţii conştientizând importanţa certificării.

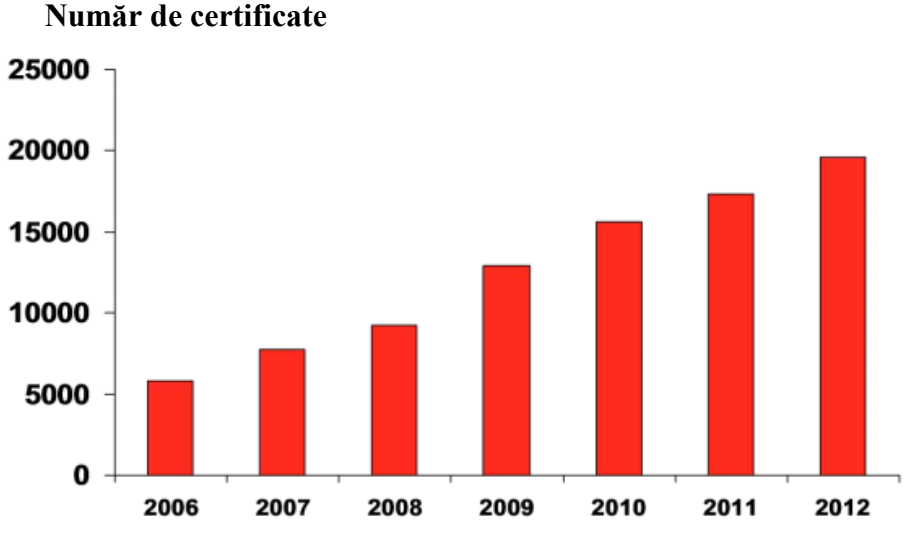

Figura 1: Creşterea globală în certificări (https://bsiedge.bsi-global.com/newiso27001/, 2014)

Revenind la I.S.O. / I.E.C. 27001:2013 ca document normativ pentru certificarea unei organizaţii pe domeniul securităţii informaţiilor, acesta reprezintă o versiunea revizuită a vechiului standard I.S.O. / I.E.C. 27001:2005. Structura noului standard s-a schimbat mult şi este în concordanţă cu noile directive I.S.O. / I.E.C. („Anexa SL"). Se intenţionează ca toate standardele pentru sisteme de management să adopte acest format în ediţiile viitoare revizuite. I.S.O. / I.E.C. 27001 este primul standard care a adoptat noua structură prevazută în „Anexa SL". Noul standard arată foarte diferit de vechea versiune, ***structura noului I.S.O. / I.E.C***. fiind:

0. Introducere
1. Scop
2. Referinţe normative
3. Termeni şi definiţii
4. Contextul organizaţiei
5. Leadership
6. Planificare
7. Suport
8. Operare
9. Evaluarea performanţei
10. Îmbunătăţire

În ***adoptarea noului standard*** I.S.O. / I.E.C. 27001:2013 ***s-a urmărit***:

- ✓ să se ofere un set principal de cerinţe pentru următorii ani (10 ani sau mai mult);
- ✓ standardul să rămână generic şi relevant pentru toate tipurile de organizaţii, indiferent de mărimea, organizarea şi sectorul lor de activitate;

- ✓ să se aplice „Anexa SL" a directivelor ISO pentru a îmbunătăţii compatibilitatea şi alinierea cu alte standarde ale sistemelor de management ISO;
- ✓ să se utilizeze stiluri de exprimare, de vocabular şi scriere simplificate pentru a ajuta înţelegerea şi interpretarea consistentă a cerinţelor standardului; s-a intenţionat a se promova consistenţă în termeni şi definiţii în toate standardele familiei ISO 27k.

Dintre cele mai importante ***schimbări / noutăţi*** pe care le întâlnim în noul standard putem aminti:

- ✓ definiţiile care apar în versiunea 2005 au fost relocate în noul standard ISO 27000;
- ✓ secţiunea referitoare la modelul / ciclul PDCA a fost scoasă întrucât există şi alte abordări pentru a atinge cerinţa de îmbunătăţire (a se vedea clauza /capitolul 10 din standard), PDCA fiind o posibilitate;
- ✓ cerinţele de evaluare a riscurilor sunt mai generale şi sunt prevăzute în capitolele 6 şi 8;
- ✓ unii termeni au fost înlocuiţi în scopul clarificării cerinţelor standardului (de exemplu termenul „acţiuni preventive" a fost scos sau capitolul 10 se numeşte în noul standard doar „Îmbunătăţire", nu „Îmbunătăţire continuă" etc);
- ✓ în timp ce vechiul standard avea ca referinţă normativă ISO 18899:2005, noul standard ISO 27001:2013 are noul ISO 27000.

Pentru a implementa un S.M.S.I. în conformitate cu I.S.O. / I.E.C. 27001:2013, o organizaţie trebuie să îndeplinească ***cerinţele prevăzute de standard***, ca de exemplu (cerinţe noi):

- ✓ 6.2(k) cum rezultatele sunt evaluate;
- ✓ 6.2(c) rezultatele de la evaluarea şi tratarea riscurilor;
- ✓ 7.5.1(b) informaţii documentate determinate de organizaţie care sunt necesare pentru eficacitatea sistemului de management al securităţii informaţiilor;
- ✓ 10.1(e) să facă schimbări sistemului de management al securităţii informaţiilor, dacă este necesar;
- ✓ 10.1(f) natura neconformităţilor şi acţiuni ulterioare luate sau corective.

Lista cerinţelor nou introduse este dată mai jos (numărul subcapitolului din standard): 4.2(a); 4.3(c); 5.1(b); 6.1.1(a); 6.1.1(b); 6.1.1(c); 6.1.2(a); 6.2(b); 6.2(c); 6.2(c); 6.2(f); 6.2(g); 6.2(h); 6.2(i); 6.2(k); 7.3(a); 7.4(a); 7.4(b); 7.4(c); 7.4(d); 7.4(e); 7.5.1(b); 8.1; 9.1(c); 9.1(d); 9.1(f); 9.3(c)(4); 10.1(a); 10.1(a)(1); 10.1(a)(2); 10.1(e); 10.1(f).

Cerinţele prevăzute de noul standard în legatură cu ***informaţiile documentate obligatorii*** (în vechiul standard erau proceduri şi înregistrări documentate) pe care organizaţia trebuie să le aibă sunt:

- ✓ Scopul S.M.S.I. (4.3);
- ✓ Politica de securitate a informaţiilor (5.2);
- ✓ Procesul de evaluare a riscurilor de securitate a informaţiilor (6.1.2);
- ✓ Procesul de tratare a riscurilor de securitate a informaţiilor (6.1.3);
- ✓ Declaraţia de aplicabilitate (6.1.3.(d));
- ✓ Obiectivele privind securitatea informaţiilor (6.2);
- ✓ Evidenţa cu competenţe ale personalului (7.2);
- ✓ Informaţii documentate necesare pentru eficacitate (7.5.1b);
- ✓ Planul operaţional şi informaţii de control (8.1);
- ✓ Rezultatele evaluării riscurilor de securitate a informaţiilor (8.2);
- ✓ Rezultatele tratării riscurilor de securitate a informaţiilor (8.3);
- ✓ Evidenţa monitorizării şi măsurării rezultatelor (9.1);

- ✓ Evidenţa programelor de audit şi rezultatele auditului (9.2);
- ✓ Evidenţa rezultatelor revizuirilor manageriale ale S.M.S.I. (9.3);
- ✓ Evidenţa naturii neconformităţilor identificate şi acţiuni corective (10.1).

3. Aspecte practice pentru organizaţii – Răspunsuri la întrebări frecvente (FAQ)

Prezenta secţiune oferă răspunsuri la întrebări frecvente în legătură cu implementarea şi certificarea unui S.M.S.I. în conformitate cu noul I.S.O. / I.E.C. 27001:2013, în scopul de a ajuta organizaţiile interesate.

1. **Î: Care sunt avantajele şi dezavantajele implementării unui S.M.S.I. ?**
   R: Principalele avantaje ale unui S.MS.I. normativ bazat pe I.S.O. / I.E.C. 27001:2013:
   a) un astfel de S.M.S.I. poate fi certificat de o autoritate de certificare naţională sau internaţională oferind încredere tuturor părţilor interesate;
   b) procese ale organizaţiei sunt verificate prin audit intern şi extern;
   c) sunt evaluate şi tratate riscurile de securitate a informaţiilor.
   Dezavantaje ale unui S.M.S.I. normativ bazat pe I.S.O. / I.E.C. 27001:2013:
   a) un astfel de S.M.S.I. trebuie documentat;
   b) sunt necesare programe periodice de instruire pentru personalul organizaţiei, ceea ce implică adiţionale costuri;
   c) un astfel de S.M.S.I. trebuie verificat periodic prin audit intern şi extern.

2. **Î: Care sunt avantajele certificării unui S.M.S.I.?**
   R: Principalele avantajele ale certificării unui S.MS.I. normativ bazat pe I.S.O. / I.E.C. 27001:2013:
   a) S.M.S.I. oferă încredere într-o organizaţie certificată tuturor părţilor interesate (clienţi, parteneri de afaceri etc);
   b) se realizează periodic managementul riscurilor de securitate a informaţiilor;
   c) un S.M.S.I. reprezintă un puternic instrument de marketing;
   d) facilitatea participării la licitaţii.

3. **Î: Ce reprezintă certificarea?**
   R: Certificarea este procesul de verificare a conformităţii – verificarea îndeplinirii unor
   cerinţe prevăzute, de regulă, într-un document normativ (exemplu I.S.O. / I.E.C. 27001:2013). Se pot certifica, de către un organism de evaluare a conformităţii, de exemplu: sisteme de management, competenţa oamenilor, produse.

4. **Î: Ce se certifică ? / cine certifică ? / ce se acreditează ? / cine acreditează ?**
   R: vezi Figura 2.

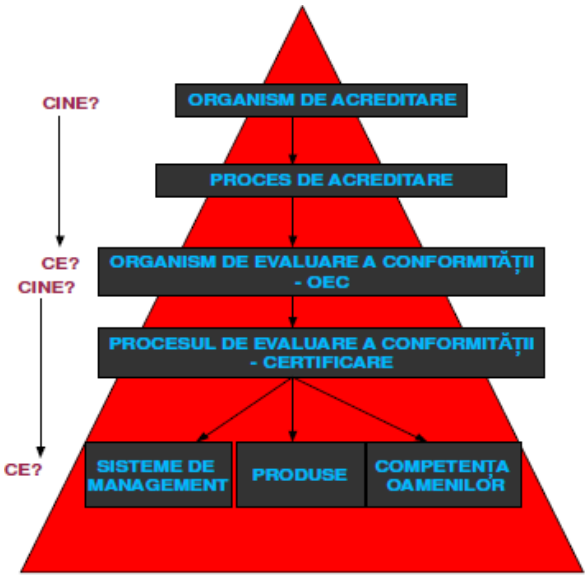

Figura 2: Răspunsuri la întrebări (adaptare după D. Constantinescu, 2005)

5. **Î: Care sunt paşii certificării?**

R:PAS 1: Analiza informală a S.M.S.I. (verificarea existenţei politicii de securitate, a declaraţiei de aplicabilitate etc);

PAS 2: Analiza formală şi detaliată, este verificată îndeplinirea cerinţelor standardului I.S.O. / I.E.C. 27001:2013. Îndeplinirea cerinţelor înseamnă certificarea organizaţiei în concordanţă cu I.S.O. / I.E.C. 27001:2013;

PAS 3: Reevaluare periodică pentru a confirma că organizaţia este în acord cu cerinţele standardului I.S.O. / I.E.C. 27001:2013.

6. **Î: Sunt interesat acum să certific organizaţia conform I.S.O. 27001. Ce trebuie să fac?**

R: Certificarea conform I.S.O. 27001 se poate face, pentru o perioadă de tranziţie, după cele două variante: 2005 sau 2013. În funcţie de gradul de îndeplinire a cerinţelor la care aţi ajuns puteţi decide în consecinţă. În viitor, pe termen scurt - mediu, standardul după care se va face certificarea va fi I.S.O. / I.E.C. 27001:2013.

7. **Î: Sunt certificat conform I.S.O. 27001. Ce trebuie să fac?**

R: Trebuie făcută în timp, pe termen scurt - mediu, tranziţia către respectarea cerinţelor noului standard, astfel să vă puteţi menţine şi în viitor certificarea. În acest sens, câteva recomandări de care aţi putea ţine seama sunt:

- ✓ faceţi schimbări documentaţiei astfel încât să reflecte noua structură;
- ✓ implementaţi noile cerinţe;
- ✓ acordaţi o atenţie deosebită evaluării impactului pe care il au schimbările.

4. Aspecte finale

Securitatea informaţiilor este un domeniu faţă de care orice organizaţie trebuie să aibă atenţie întrucât reprezintă un pilon principal care, într-adevăr nu este aducător de profit, dar care contribuie semnificativ la realizarea obiectivelor organizaţionale. O posibilitate pentru a furniza încredere tuturor părţilor interesate este implementarea şi ulterior certificarea unui S.M.S.I. conform standardului ISO 27001, recent revizuit în 2013 de la vechea versiune din 2005. Noul standard este foarte diferit de cel vechi, atât din punct de vedere al structurii, dar

şi al cerinţelor noi pe care le prevede, aspecte privind familiarizarea cu noul standard fiind descrise în prezenta lucrare.

Acknowledgements

Rezultatele prezentate în acest articol au fost obţinute cu sprijinul Ministerului Muncii, Familiei, Protecţiei Sociale şi Persoanelor Vârstnice, prin Programul Operational Sectorial Dezvoltarea Resurselor Umane 2007-2013, POSDRU / ID 132395 (InnoRESEARCH).

The work has been funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Romanian Ministry of Labour, Family, Social Protection and Elderly, through the Financial Agreement POSDRU / ID 132395 (InnoRESEARCH).

5. Bibliografie

[1] Bogdan Ţigănoaia, *Asigurarea securităţii informaţiilor în organizaţii*, apărută în seria *Studii strategice şi de securitate* la Editura Institutul European, Iaşi, www.euroinst.ro, 228 pagini, tiraj: 300 - 1000 de exemplare, 2013.

[2] E.N.I.S.A. Country Reports, 2008, http://www.enisa.europa.eu.

[3] Constantinescu D., *Managementul calităţii*, Editura Printech, ISBN 973-718-186-7, 2005.

[4] B.S.I. Group (https://bsiedge.bsi-global.com/newiso27001/ accesat la 30.04.2014).

[5] Familia de standarde ISO 27k. (http://www.iso.org/iso/).

[6] B.S.I. report: *Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013*, 2014.