COMPARATIVE STUDY REGARDING INTERNATIONAL STANDARDS ON INFORMATION SECURITY MANAGEMENT SYSTEMS IN ORGANIZATIONS: ISO/IEC 27001:2013 vs ISO/IEC 27001:2005

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

Abstract: This paper is a comparative study regarding international standards on information security management systems in organizations. It is about the ISO/IEC 27001:2005 and its revised version, ISO/IEC 27001:2013. The paper presents, in a comparative analysis, aspects regarding: the structure of the standards (with a focus point on the new ISO/IEC 27001:2013 structure), the new concepts or updates and terms introduced in ISO/IEC 27001:2013, the documented information that the new version of the standard mentions etc. Aspects regarding the mapping of ISO/IEC 27001:2013 clauses to ISO/IEC 27001:2005, the new requirements introduced by ISO/IEC 27001:2013 or deleted requirements from the old version of the standard are also focus points of the paper.

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

1. Introducere

Un sistem de management al securităţii informaţiilor – S.M.S.I. cuprinde procese de coordonare (manageriale) între care există legături în scopul asigurării securităţii informaţiilor în organizaţii. Un S.M.S.I. implică o abordare sistematică pentru a gestiona informaţii sensibile/critice ale unei organizaţii astfel încât ele să fie securizate, accesul la acestea fiind permis doar entităţilor care sunt îndreptăţite. Pe scurt, un S.M.S.I. ajută organizaţiile de orice mărime, tip sau sector de activitate să menţină informaţii securizate.

Familia de standarde I.S.O. / I.E.C. 27000 ajută organizaţiile să implementeze, certifice şi menţină un sistem de management al securităţii informaţiilor – S.M.S.I.. Dintre standardele care fac parte din familia 27000 putem aminti:

- ✓ **I.S.O. / I.E.C. 27000:2014** - Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Privire de asamblu şi vocabular.
- ✓ **I.S.O. / I.E.C. 27001:2013** - Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Cerinţe.
- ✓ **I.S.O. / I.E.C. 27002:2013** - Tehnologia informaţiei. Tehnici de securitate. Cod de bună practică pentru managementul securităţii informaţiilor.
- ✓ **I.S.O. / I.E.C. 27003:2010** - Tehnologia informaţiei. Tehnici de securitate. Ghid de implementare pentru sistemul de management al securităţii informaţiei.
- ✓ **I.S.O. / I.E.C. 27032:2012** - Tehnologia informaţiei. Tehnici de securitate. Linii directoare pentru securitatea cibernetică.
- ✓ **I.S.O. / I.E.C. 27004:2009** - Tehnologia informaţiei. Tehnici de securitate. Managementul securităţii informaţiilor – Evaluări.

Standardul I.S.O. / I.E.C. 27001:2013 este cel mai cunoscut document normativ în vederea implementării şi certificării unui S.M.S.I. într-o organizaţie. Trebuie precizat că *ISO nu este organism de certificare*. Ca orice alt standard ISO privitor la sisteme de management, certificarea I.S.O. / I.E.C. este posibilă, dar nu obligatorie. De exemplu, unele organizaţii aleg doar să implementeze cerinţele pentru a benficia de bunele practici din standard, în schimb altele aleg şi certificarea pentru a oferi, suplimentar, încredere tuturor părţilor interesate.

Faţă de ediţia din 2005, noul standard I.S.O. / I.E.C. 27001:2013 arată foarte diferit şi are multe elemente de noutate, care vor fi prezentate în cele ce urmează.

2. Structura noului I.S.O. / I.E.C. 27001:2013 în comparaţie cu I.S.O. / I.E.C. 27001:2005

Dacă ne referim la structura noului standard I.S.O. / I.E.C. 27001:2013 putem spune că acesta respectă noile directive ISO şi a fost scris ca prim standard care este în concordanţă cu formatul prevăzut în „Anexa SL". În tabelul de mai jos se poate vedea corespondenţa dintre structura vechiului standard şi a ediţiei revizuite în 2013.

I.S.O. / I.E.C. 27001:2005	***I.S.O. / I.E.C. 27001:2013***
0. Introducere	0. Introducere
1. Domeniul de aplicare	1. Scop
2. Referinţe normative	2. Referinţe normative
3. Termeni şi definiţii	3. Termeni si definiţii
4. Sistem de Management al Securităţii Informaţiilor	4. Contextul organizaţiei
5. Responsabilitatea managementului	5. Leadership
6. Audit intern	6. Planificare
7. Analizele efectuate de management pentru S.M.S.I.	7. Suport
8. Îmbunătăţirea S.M.S.I.	8. Operare
Anexa A	9. Evaluarea performanţei
Anexa B	10. Îmbunătăţire
Anexa C	Anexa A

Tabelul 1: Structura standardelor I.S.O. / I.E.C. 27001:2005 vs I.S.O. / I.E.C. 27001:2013

În continuare sunt prezentate aspecte comparative cu vechiul standard care ţin de fiecare capitol din noul standard, I.S.O. / I.E.C. 27001:2013.

11. **Introducere** – Modelul P.D.C.A. (Plan-Do-Check-Act) a fost scos din noul standard, întrucât acesta era doar o modalitate de a structura procesele organizaţiei în scopul asigurării îmbunătăţirii continue (vezi capitolul / clauza 10 din standard);
12. **Scop –** Accent deosebit este pus pe evaluarea şi tratarea riscurilor de securitatea informaţiilor;
13. **Referinţe normative –** Singura referinţă normativă este I.S.O. / I.E.C. 27000, nu mai apare ca referinţă ISO 27002;
14. **Termeni şi definiţii –** Termenii şi definiţiile au fost scoşi/scoase din standard şi trecuţi în singura referinţa normativă a standadului, ISO 27000;
15. **Contextul organizaţiei –** Este un capitol nou în standard care obligă organizaţiile să determine cadrul intern şi extern în care acestea îşi desfăşoară activitatea. Există o cerinţă cu privire la stabilirea tuturor părţilor interesate şi a aşteptărilor / cerinţelor acestora. Scopul S.M.S.I. trebuie de asemenea definit, existând o cerinţă privind îmbunătăţirea continuă a S.M.S.I.;
16. **Leadership –** Este un capitol care înlocuieşte vechiul capitol, *Responsabilitatea managementului.* Sunt prevăzute cerinţe pentru top-managementul organizaţiei şi rolul (care trebuie să fie mult mai activ) acestuia în S.M.S.I.. În noul standard se face referire la *politica de securitate a informaţiilor*, în vreme ce în vechiul standard se cerea politica sistemului de management al securităţii informaţiilor;

17. **Planificare –** 6.1.1 înlocuieşte din vechiul standard cerinţele privitoare la acţiunile preventive; 6.1.2 – Evaluarea riscurilor de securitate a informaţiilor – identificarea bunurilor, ameninţărilor şi vulnerabilităţilor nu mai sunt cerute, însă trebuie identificate riscurile care afectează disponibilitatea, confidenţialitatea şi integritatea informaţiilor. Noul standard cere un *responsabil de risc*, nu un *responsabil de bun*, aşa cum se cerea în versiunea din 2005. Cerinţele privind evaluarea riscurilor de securitatea informaţiilor sunt mai generale şi aliniază ISO 27001 cu ISO 31000; 6.1.3 vorbeşte despre tratarea riscurilor de securitate a informaţiilor. Subcapitolul 6.2 vorbeşte despre obiectivele de securitate a informaţiilor şi cerinţele asociate.
18. **Suport –** Capitolul reflectă cerinţe pentru stabilirea, implementarea şi menţinerea unui S.M.S.I eficace cu privire la: resurse, competenţa oamenilor implicaţi, comunicare etc; nu se mai face referire la *controlul documentelor şi înregistrărilor*, se precizează că trebuie să existe *informaţii documentate* (documented information), neexistând o listă a documentelor pe care organizaţiile trebuie să le aibă sau cum să se numească acestea (în noul standard se pune accent pe conţinut, nu pe nume);
19. **Operare –** Cerinţe privind planificarea şi controlul operării proceselor necesare pentru îndeplinirea cerinţelor privind securitatea informaţiilor: păstrarea documentelor, managementul schimbării etc. Sunt precizate cerinţe privind implementarea planului de tratare a riscurilor de securitate a informaţiilor sau de realizare la intervale planificate a evaluării riscurilor de securitate a informaţiilor;
20. **Evaluarea performanţei –** Sunt cerinţe exprese privind monitorizarea, evaluarea, auditul intern (cerinţe aproape indentice cu vechiul standard) şi analizele efectuate de management pentru eficacitatea S.M.S.I.; pentru un S.M.S.I. adecvat, eficace, managementul trebuie să considere orice schimbare internă sau externă organizaţiei;
21. **Îmbunătăţire –** Sunt cerinţe privitoare la orice neconformitate identificată în sensul acţionării pentru înlăturarea acesteia. De asemenea, standardul prevede şi cerinţe cu privire la îmbunătăţirea continuă.

În timp ce standardul I.S.O. / I.E.C. 27001:2005 cuprinde 3 anexe, una normativă şi două informative:

Anexa A (normativă): Obiective şi măsuri de control;

Anexa B (informativă): Principiile OECD şi acest standard internaţional;

Anexa C (informativă): Corespondenţa dintre ISO 9001:2000, ISO 14001:2004 şi acest standard internaţional,

noua versiune de standard cuprinde o singură anexă normativă:

Anexa A (normativă): Măsuri şi obiective de control de referinţă

Anexa B nu a mai fost necesară întrucât principiile O.E.C.D. făceau referire la folosirea modelului P.D.C.A., care în noul standard nu mai este obligatorie. Anexa C nu a mai fost necesară pentru că şi standardele I.S.O. 9001 şi I.S.O. 14001 vor fi revizuite după template-ul prezentat în „Anexa SL", având practic acelaşi core ca I.S.O. 27001.

Numărul de măsuri prevăzute în anexă a fost redus de la 133 la 114, în timp ce numărul de secţiuni a crescut de la 11 la 14, ca urmare a introducerii, comasării sau ştergerii unor măsuri. Secţiunile (selecţie) din noua anexă fac referire la:

- ✓ Securitatea resurselor umane;
- ✓ Politicile de securitate a informaţiilor;
- ✓ Controlul accesului;
- ✓ Criptografie;
- ✓ Managementul incidentelor de securitate a informaţiilor;

- ✓ Aspecte ale securităţii informaţiilor privind managementul continuitatea afacerii.
- ✓ Managementul bunurilor;
- ✓ Securitatea operaţiunilor;
- ✓ Securitatea comunicaţiilor.

3. Analiză comparativă privind elemente ale standardului I.S.O. / I.E.C. 27001:2005 în raport cu ediţia revizuită, I.S.O. / I.E.C. 27001:2013

În raport cu cele două ediţii ale standardului I.S.O. / I.E.C. 27001, se pot observa diferenţe notabile cu privire la următoarele aspecte:

- ✓ ***Noi concepte au fost introduse sau actualizate precum (selecţie):***
  - o părţi interesate – în locul „stakeholders";
  - o proprietar / responsabil de risc – în locul proprietar / responsabil de bun;
  - o leadership – au fost introduse cerinţe specifice managementului de top al organizaţiei;
  - o informaţii documentate – în locul documente şi înregistrări;
  - o comunicarea – există cerinţe clare atât pentru comunicarea internă, cât şi pentru cea externă;
  - o contextul organizaţiei – organizaţia trebuie să cunoască şi să analizeze mediul în care îşi desfăşoară activitatea;
  - o evaluarea performanţei – măsurarea eficacităţii S.M.S.I. şi a planului de tratare a riscurilor;
  - o îmbunătăţire continuă – metoda P.D.C.A. nu mai este obligatorie pentru structurarea proceselor organizaţiei, însă aceasta poate fi în continuare folosită, la fel ca oricare altă metodologie;
- ✓ ***Noul standard prevede informaţii documentate şi nu proceduri şi înregistrări documentate ca în vechea ediţie, precum:***
- ✓ Scopul sistemului de management al securităţii informaţiilor – subcapitolul (4.3);
- ✓ Politica de securitatea informaţiilor – subcapitolul (5.2);
- ✓ Procesul de evaluarea riscurilor de securitatea informaţiilor – subcapitolul (6.1.2);
- ✓ Procesul de tratarea riscurilor de securitatea informaţiilor – subcapitolul (6.1.3);
- ✓ Declaraţia de aplicabilitate – subcapitolul (6.1.3.(d));
- ✓ Obiectivele securităţii informaţiilor – subcapitolul (6.2);
- ✓ Evidenţa cu competenţele personalului – subcapitolul (7.2);
- ✓ Informaţii documentate ce sunt necesare pentru eficacitate – subcapitolul (7.5.1b);
- ✓ Planul operaţional şi informaţii de control – subcapitolul (8.1);
- ✓ Rezultatele evaluării riscurilor de securitate a informaţiilor – subcapitolul (8.2);
- ✓ Rezultatele tratării riscurilor de securitatea informaţiilor – subcapitolul (8.3);
- ✓ Evidenţa monitorizării şi măsurării rezultatelor – subcapitolul (9.1);
- ✓ Evidenţa programelor de audit şi rezultatele auditului – subcapitolul (9.2);

- ✓ Evidenţa rezultatelor revizuirilor manageriale ale S.M.S.I. – subcapitolul (9.3);
- ✓ Evidenţa naturii neconformităţilor identificate şi acţiuni corective – subcapitolul (10.1).

În vechiul standard organizaţia trebuia să aibă ***proceduri documentate*** pentru cel puţin următoarele procese:

- Controlul documentelor;
- Controlul înregistrărilor;
- Audit intern;
- Analiza efectuată de management a S.M.S.I.;
- Acţiuni preventive;
- Acţiuni corective.

- ✓ ***Au fost eliminate cerinţe din vechiul standard, precum (selecţie):***
  - 4.2.1(i) obţinerea autorizării managementului pentru implementarea şi operarea S.M.S.I.;
  - 5.2.1(b) asigurarea ca procedurile de securitate a informaţiilor sprijină cerinţele afacerii;
  - 5.2.1(d) menţinerea adecvată a securităţii prin aplicarea corectă a tuturor măsurilor de control implementate;
  - 6(d) responsabilităţile şi cerinţele pentru planificarea şi conducerea auditurilor, şi pentru raportarea rezultatelor şi menţinerea înregistrărilor ar trebui să fie definite în proceduri documentate;
  - 8.2 procedura documentată pentru acţiuni corective trebuie să definească cerinţe în acest sens;
  - 8.3 procedura documentată pentru acţiuni preventive trebuie să definească cerinţe în acest sens;
  - 8.3(d) rezultatele înregistrărilor pentru acţiunile luate;
  - 8.3(e) revizuirea acţiunilor preventive luate;
  - 8.3(e) prioritatea acţiunilor preventive trebuie determinate pe baza rezultatelor evaluării riscurilor;
- ✓ ***Au fost introduse noi cerinţe în noul standard, precum (selecţie):***
  - 4.2(a) să analizeze părţile interesate care sunt relevante pentru sistemul de management al securităţii informaţiilor;
  - 5.1.(b) să asigure integrarea cerinţelor sistemului de management al securităţii informaţiilor în procesele de afaceri ale organizaţiei;
  - 6.1.1.(b) previnã sau reducă efectele nedorite;
  - 6.2(c) să ia în calcul cerinţele aplicabile pentru securitatea informaţiilor;
  - 7.5.1(b) informaţii documentate determinate de organizaţie ca fiind necesare pentru eficacitatea sistemului de management al securităţii informaţiilor;
  - 8.1 organizaţia trebuie să planifice, implementeze şi controleze procesele necesare pentru a atinge cerinţele de securitate a informaţiilor si să implementeze acţiunile prevăzute în 6.1;
  - organizaţia trebuie să stabilească cine monitorizează şi măsoară (9.1.(d)) şi când (9.1(c)), cine analizează şi evaluează rezultatele (9.1.(f));
  - 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.

✓ ***Pot fi mapate foarte uşor cerinţele standardului I.S.O. 27001:2005 cu cele ale standardului I.S.O. 27001:2013, dar şi invers, existând o relaţie biunivocă. (selecţie):***

- 4.2.1(a) definirea scopului şi limitelor S.M.S.I.... ⟶ 4.3;
- 4.2.1(b) definirea politicii S.M.S.I. ... ⟶ 5.2(a);
- 4.2.1(c) definirea abordării evaluării riscurilor... ⟶ 6.1.2;
- 4.2.1(d) identificarea riscurilor... ⟶ 6.1.1, 6.1.2 (c);
- 6 organizaţia trebuie să conducă un audit intern... ⟶ 9.2.
- 7.2(b) feedback de la toate părţile interesate... ⟶ 9.3(d);
- 8.1 organizaţia trebuie să îmbunătăţească eficacitatea …⟶ 10.2;
- 8.2(a) identificarea neconformităţilor…⟶ 10.1(b)(1);
- 8.3(e) revizuirea acţiunilor preventive luate ⟶ aceasta cerinţă a fost ştearsă.

✓ ***Noi măsuri de control au fost introduse (selecţie):***

- A.6.15. Securitatea informaţiilor în managementul proiectelor;
- A.12.6.2. Restricţii privind instalări de software – trebuie stabilite şi implementate reguli privind instalarea software-ului de către utilizatori;
- A.14.2.8. Testarea sistemelor de securitate;
- A.16.1.5. Răspunsul la incidentele de securitate a informaţiilor – în concordanţă cu procedurile documentate;
- A.16.1.4. Evaluarea şi decizii privind evenimentele de securitatea informaţiilor – evenimentele de securitatea informaţiilor trebuie evaluate şi trebuie să se decidă dacă acestea sunt clasificate ca incidente de securitatea informaţiilor.

✓ ***Unele măsuri de control au fost schimbate (selecţie - mapare schimbare, 2005 vs 2013):***

- Cod maliţios, 10.4.1 ⟶ Malware, 12.2.1.;
- Servicii de comerţ electronic, 10.9⟶ Servicii de aplicaţii, 14.1.2, 14.1.3;
- Managementul continuităţii afacerii, 14 ⟶ Continuitatea securităţii informaţiilor, 17;
- Părţi externe (6.2) şi părţi terţe (10.2) ⟶ Furnizor, 15.

✓ ***Unele măsuri de control au fost scoase / şterse:***

- A.6.1.2 Coordonarea securităţii informaţiilor;
- A.6.2.1 Identificarea riscurilor ce ţin de părţi din exterior;
- A.12.2.3 Integritatea mesajului;
- A.11.4.3 Identificarea echipamentelor în reţele;
- A.11.6.2 Izolarea sistemelor sensibile;
- A.15.3.2 Protecţia uneltelor de audit pentru sistemele de informaţii.

✓ ***Maparea secţiunilor din anexa A corespunzătoare celor două ediţii, din 2005 şi 2013 (adaptare https://bsiedge.bsi-global.com/newiso27001/, accesat la 04.05.2014)***

I.S.O. / I.E.C. 27001:2005	***I.S.O. / I.E.C. 27001:2013***
5. Politica de securitate	5. Politicile de securitate
6. Organizarea securităţii informaţiilor	6. Organizarea securităţii informaţiilor
8. Securitatea resurselor	7. Securitatea resurselor umane

umane	
7. Managementul bunurilor	8. Managementul bunurilor
11. Controlul accesului	9. Controlul accesului
12. Menţinerea, dezvoltarea şi achiziţia sistemelor de informaţii (doar 12.3)	10. Criptografie
9. Securitatea fizică şi ambientală	11. Securitatea fizică şi ambientală
10. Managementul comunicaţiilor şi operaţiilor	12. Securitatea operaţiilor / 13. Securitatea comunicaţiilor
12. Menţinerea, dezvoltarea şi achiziţia sistemelor de informaţii	14. Menţinerea, dezvoltarea şi achiziţia sistemelor
-	15. Relaţiile cu furnizori
13. Managementul incidentelor de securitate a informaţiilor	16. Managementul incidentelor de securitate a informaţiilor
14. Managementul continuităţii afacerii	17. Aspecte ale securităţii informaţiilor privind managementul continuităţii afacerii
15. Conformitate	18. Conformitate

Tabelul 2: Maparea secţiunilor din anexa A corespunzătoare celor două ediţii, din 2005 şi 2013

4. Aspecte finale

Pentru atingerea obiectivelor organizaţionale, orice companie trebuie să investească resurse în asigurarea securităţii informaţiilor cu care lucrează. O modalitate de a furniza încredere tuturor părţilor interesate este implementarea şi certificarea unui sistem de management al securităţii informaţiilor în concordanţă cu ISO 27001. Noul standard ISO 27001:2013 este foarte diferit de vechea variantă din 2005, lucrarea de faţă ajutând organizaţiile în tranziţia către noile cerinţe ale standardului, ca de exemplu, cerinţe privind evaluarea riscurilor ce au fost aliniate cu standardul 31000. Chiar dacă nu este generatoare de profit, securitatea organizaţiei, şi în particular, securitatea informaţiilor contribuie la bunul mers al oricarei companii.

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

[3] B.S.I. Group (https://bsiedge.bsi-global.com/newiso27001/, accesat la 04.05.2014).

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

[5] SAI Global Report: New I.S.O. / I.E.C. 27001:2013 Information Security Management Systems, http://www.saiglobal.com/, accesat în aprilie 2014.

[6] B.S.I. report: Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013, accesat în aprilie 2014.

[7] Bogdan Ţigănoaia, "Considerations regarding some security solutions and standards", FAIMA Business and Management Journal, No 2/2014, ISSN-L 2344-4088, ISSN 2344-4088, http://www.faimajournal.ro, 2014.