Recomandări Privind Implementarea SMSI după ISO/IEC 27001:2013

Rodica BULAI, Ludmila DUCA
Technical University of Moldova
griniuc@yahoo.com, duca.ludmila@gmail.com

***Abstract* — In this paper is done the comparative analysis of standard ISO/IEC 27001 The System management of information security (SMSI) the versions 2005 and 2013. It is proposed the recommendations according to the implementation or actualization of one SMSI by the version ISO/IEC 27001:2013.**

***Index Terms* — system management of information security, the control objective, security measures, certification, ISO.**

I. INTRODUCERE

Odată cu dezvoltarea sectorului TIC, standardul ISO/IEC 27001 trebuie să țină cont de aceste evoluții, dar și de riscurile pe care acestea le implică.

Revizuirea standardului ISO/IEC 27001 a ținut cont, în primul rând, de experiența practică a utilizării lui, în perioada 2006-2013 peste 100000 de înregistrări la nivel mondial, dintre care peste 21.000 în 2013 [1].

Sondajele ISO privind numărul certificărilor ISO 27001 în lume arată o evoluție de 14% în anul 2013 față de 2012. În figura 1 este prezentat clasamentul țărilor după numărul de certificări.

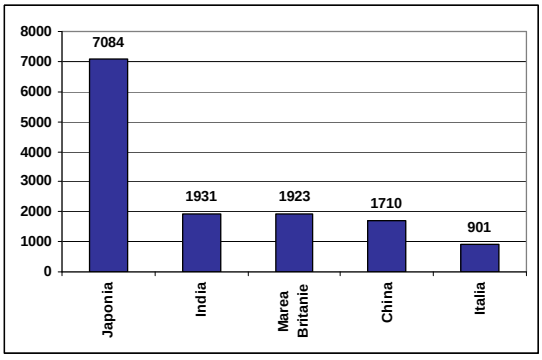

Fig.1. Certificări ISO/IEC 27001 în 2013, ISO survey 2013.

Republica Moldova înregistrează și ea o creștere nesemnificativă, după cum se prezintă în fig.2.

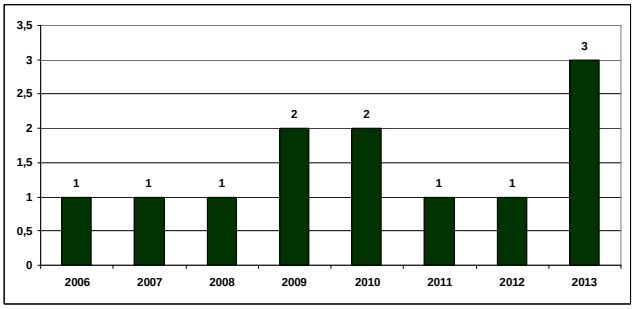

Fig.2. Evoluția certificărilor ISO/IEC 27001 în Republica Moldova, ISO survey 2013.

Totodată, vrem să menționăm impactul major al standardului în domeniul Tehnologiilor informaționale (fig.3), ceea ce ar trebui să se reflecte și în cadrul instrutuției noastre.

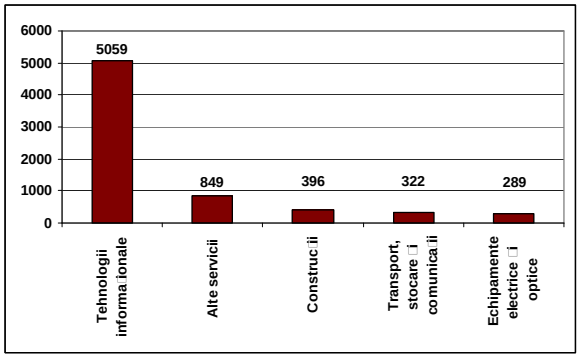

Fig.3. Sectoarele industriale cu cel mai mare număr de certificări ISO/IEC 27001 în 2013, ISO survey 2013.

Cu toate acestea, au existat și alte două influențe majore asupra revizuirii.

Prima este o cerință ISO ca toate standardele referite la sistemul de management să fie conforme cu structura de nivel înalt și textul de bază identic definite în anexa SL la partea 1 a ISO/IEC Directive. Conformitatea cu aceste cerințe au o tendinta de a face toate standardele sistemului de management să arate la fel, cu intenția ca cerințele față de sistemul de management care nu sunt disciplinat specificate, să fie redactate identic. Aceasta este o veste bună pentru organizațiile care operează sisteme de management integrate, conforme cu mai multe standarde, cum ar fi ISO 22301 (Business Continuity Management), ISO 9001 (Standard Quality Management), precum și ISO/IEC 27001 (Information security management).

Cea de a doua influența este decizia de a alinia ISO/IEC 27001 cu principiile și orientările date în ISO 31000 (Risk Management). Acest lucru, de asemenea, este o veste bună pentru sistemele de management integrate, deoarece o organizație poate aplica aceeași metodologie de evaluare a riscului pentru mai multe domenii.

II. ISO/IEC 27001:2005 vs ISO/IEC 27001:2013

Rezultatul este că structural ISO / IEC 27001:2013 arată foarte diferit de ISO/IEC 27001:2005. Nu există cerințe redundante, fiind formulate într-un mod, în care permit o

mai mare libertate de alegere cu privire la modul de punere în aplicare ale acestora. Un exemplu în acest sens este faptul că etapele de identificare a activelor, ameninţărilor şi vulnerabilităţilor nu mai este o condiţie prealabilă pentru identificarea riscurilor informaţionale. Standardul prezintă acum mai clar determinarea măsuri de securitate prin prisma procesului de tratare a riscurilor.

Cele mai semnificative schimbări sunt în Anexa A a standardului, structurat logic în jurul grupurilor de măsuri de securitate. Pentru a evita redundanţa, multe controale au fost atribuite la o singură secţiune şi, în unele cazuri, făcându-se referire la altele. De exemplu, un sistem de carduri de control al accesului într-o sală de calculatoare sau într-o arhivă este atât un control al accesului, cât şi un control fizic, care implică tehnologii, proceduri şi politici de utilizare. Acest lucru a permis ca versiunea revizuită să fie structurată după 14 obiective de control, faţă de 11 în versiunea precedentă, cu 114 măsuri de securitate faţă de 133, fig.4.

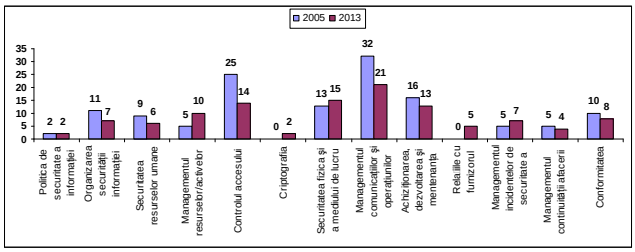

Fig.4. Anexa A
ISO/IEC 27001:2005 vs ISO/IEC 27001:2013

Au fost adăugate două obiective *Criptografia* şi *Relaţiile cu Furnizorul*, care de altfel nu sunt complet noi, deoacere măsurile de securitate sunt transferate de la categoriile *Achiziţionarea, dezvoltarea şi mentenanţa sistemelor informatice, Organizarea securităţii informaţiei* şi *Managementul comunicaţiilor şi operaţiunilor.*

Secţiunea existentă în versiunea precedentă *Managementul comunicaţiilor şi operaţiunilor* a fost divizată în *Securitatea Operaţiunilor* şi *Securitate Comunicaţiilor* [2].

În versiunea revizuită a ISO 27001, accentul este pus pe măsurarea eficacităţii de performanţă a SMSI, sunt indicate concret măsurile de monitorizare. De asemenea, sunt specificate mai eficient controalele privind relaţiile cu furnizorii vizavi de asigurarea securităţii informaţiei.

III. RECOMANDĂRI PRIVIND IMPLEMENTAREA SMSI DUPĂ ISO/IEC 27001:2013

Având în vedere faptul că în perioada 23-25 octombrie 2013, în cadrul celei de-a 27 Adunări Generale a IAF din Korea, s-a adoptat Rezoluţia IAF 2013–13 privind tranziţia la ISO/IEC 27001:2013, organismele de certificare a sistemelor de management al securităţii informaţiei sunt impuse să încheie această tranziţie până la data de 1 august 2015.

În acest context, recomandăm organizaţiilor din Republica Moldova, care au reuşit să se certifice după ISO/IEC 27001:2005 sau au planificat procedura de certificare să ţină cont de următoarele aspecte:

- Dacă cerinţele ISO/IEC 27001 au fost implementate pe deplin după versiunea 2005, este necesar să se treacă la noua versiune în decurs de un an. În prealabil se studiează modificările noii versiuni, se elaborează un plan de acţiuni pentru a realiza pe deplin cerinţele suplimentare ale noii versiuni.
- Dacă cerinţele ISO/IEC 27001:2005 sunt implementate pe deplin şi s-a obţinut certificarea SMSI se recomandă să faceţi actualizarea la noua versiune a standardului, în perioada de la 4 luni la un an. Specialiştii autorizaţi în audit recomnadă o procedură de verificare a modului în care sunt îndeplinite cerinţele suplimentare incluse în noua versiune. După această procedură, se obţine certificatul disponibil pentru noua versiune.
- Dacă cerinţele ISO/IEC 27001 au fost implementate în jur de 60% se recomandă să se finalizeze procedura mai întâi după cerinţele ISO/IEC 27001:2005. Experienţa arată că în cele mai multe cazuri, atunci când o mare parte a SMSI este implementat şi se începe să se corecteze după cerinţele noi, există mulţi factori negativi, punând în pericol succesul proiectului. De aceea, se recomandă după implementarea deplină să se planifice şi să se efectueze ajustările şi completările la noile cerinţe. Această procedură poate dura de la 2 săptămâni la 2 luni. Durata depinde, în principal, de viteza de armonizare a procedurilor şi documentaţiei interne.
- Şi doar în cazul cînd cerinţele ISO/IEC 27001:2005, au fost introduse mai puţin de 60% se recomandă de a se efectua o revizuire cuprinzătoare a planului de implementare a sistemului de management al securităţii informaţiei, de a introduce modificările şi ajustările de rigoare, în funcţie de cerinţele standardului ISO/IEC 27001:2013 [3].

Domeniile în care pot exista modificări minore sunt:

- *Iinformaţii documentate* - un termen nou, care în versiunea 2005 a însemnat *documente* şi *înregistrări*. În perioada de tranziţie la ISO/IEC 27001:2013, înlocuiţi doar termenii *documente* şi *înregistrări* cu termenul *informaţii documentate*. Dacă este necesar să se indice diferenţa, atunci ţineţi cont de faptul că documentele sunt o declaraţie de intenţie, în timp ce înregistrarea este o dovadă a activităţii anterioare.
- *Politica de securitate.*
- *Evaluarea riscurilor.*
- *Controlul documentelor.*
- *Termenii de referinţă la top-managerii.*
- *Responsabilitatea.*
- *Conştientizarea.*
- *Auditul intern.*
- *Analiza conducerii.*
- *Acţiunile corective.*
- *Îmbunătăţirile.*

Respectiv domeniile care necesită îmbunătăţiri, sunt:

- *Domeniul de aplicare a SMSI* - formularea de la alineatul 4.3 (în special 4.3 c)) este destinată pentru a concretiza că SMSI (spre deosebire de zona de certificare) include tot ceea ce este de interes pentru SMSI.
- *Obiectivele de securitate a informaţiilor* - în cazul în care o organizaţie consideră obiectivele sale de securitate ca un obiectiv de politici permanente, cerinţele de la punctul 6.2, care se referă la *funcţiile şi nivelurile relevante* ar putea fi o noutate pentru ei.

Domeniul care necesită actualizare este *Aplicabilitatea*, măsurile de securitate după Anexa A.

Noile cerințe, care ar putea avea deja o conformitate, pot fi:

- *Părțile interesate şi cerințele lor* - p.4.2 cere organizațiilor să determine părțile interesate legate de SMSI şi cerințele lor.
- *Integrarea* - p. 5.1 b) cere top-managerilor să asigure integrarea cerințelor SMSI în procesele de business ale organizației.
- *Comunicarea* - cerințele de la p.7.4 (comunicare) sunt mai specifice decât aceleaşi condiții în versiunea anterioară a standardului.

Cerințele noi, care reprezintă o sarcină complexă includ:

- *Aspectele problematice* - posibil că aspectele menționate la p.4.1 să fie bine cunoscute în organizație, doar că ele nu au fost înregistrate; cu siguranță nu în termenii care ar fi în măsură să demonstreze conformitatea cu cerințele noii versiuni.
- *Acțiunile pentru abordarea riscurilor şi oportunităților de natură generală* - procedurile existente pentru acțiunile preventive vor trebui să fie revizuite sau înlocuite, în scopul de a asigura conformitatea acestora cu prevederile 4.1, 4.2 şi 6.1.1.
- *Monitorizarea, măsurarea, analiza şi evaluarea* - cerințele de la p.9.1 sunt mai detaliate şi mai precise decât cerințele şi controlul eficienței din ISO/IEC 27001:2005. La această etapă, se recomandă să se înceapă, cel mai bine, de la o foaie curată [4].

IV. CONCLUZII

În concluzie, toate organizațiile sunt diferite şi această orientare trebuie să fie interpretată în contextul nevoilor individuale ale fiecărei organizații, ceea ce pe deplin permite standardul ISO/IEC 27001. Ceea ce se poate dovedi a fi uşor pentru unii, poate fi o provocare pentru alții şi vice-versa. Se speră că această orientare va fi un punct de plecare util pentru majoritatea organizațiilor.

BIBLIOGRAFIE

[1] ISO Survey: http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/
[2] ISO 27002:2013 Version Change Summary: www.informationshield.com
[3] Управление информационной безопасностью\ ISO/IEC 27001:2013: http://tms-ua.com/standarts/iso-27001-2013/
[4] http://sic.com.ua/2014/07/rekomendacii-po-perexodu-na-standart-isoiec-270012013/