Universitatea
Transilvania
din Brașov

ȘCOALA DOCTORALĂ INTERDISCIPLINARĂ

Facultatea: Design de Produs și Mediu

Mihai Bârsan

TITLU (română): Cercetări privind implementarea Sistemelor de Management al Securității Informațiilor în arhivele digitale

TITLU (engleză): Research Regarding the Implementation of Information Security Management Systems in Digital Archives

REZUMAT / ABSTRACT

Conducător ştiinţific

Prof.dr.ing., dr. marketing Angela Repanovici

BRAȘOV, 2020

D-lui Mihai BÂRSAN

COMPONENȚA

Comisiei de doctorat

Numită prin ordinul Rectorului Universității Transilvania din Braşov
Nr. ..... din .....

PREŞEDINTE:	Prof.dr.ing. Codruța JALIU
CONDUCĂTOR ŞTIINȚIFIC:	Prof.dr.ing. Angela REPANOVICI
REFERENȚI:	Prof. univ. dr.ing. Anca DRĂGHICI
	Prof. univ. dr. Mircea REGNEALĂ
	Prof. univ. dr.ing. Anișor NEDELCU

Data, ora şi locul susținerii publice a tezei de doctorat: 04.09.2020, ora 11.00, sala .....

Eventualele aprecieri sau observații asupra conținutului lucrării vor fi transmise electronic, în timp util, pe adresa mihai.barsan@unitbv.ro

Totodată, vă invităm să luați parte la şedința publică de susținere a tezei de doctorat.

Vă mulțumim.

CUPRINS

CONTENT

INTRODUCERE

Teza de doctorat *Cercetări privind implementarea Sistemelor de Management al Securității Informațiilor în arhivele digitale* își propune să analizeze metodele și mijloacele de implementare a unui Sistem de management al Securității Informațiilor (ISMS) în organizații, indiferent dacă acestea sunt publice sau private, precum și de mediul în care evoluează. În acest sens, prin prezenta lucrare se vor analiza atât standardul internațional de securitate a informației, ISO/IEC 27001:2013, cât și prevederile Regulamentului nr. 679 din 27 aprilie 2016 privind protec ia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circula ie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protec ia datelor).

Lucrarea este structurată în șase capitole și va evidenția avantajele implementării unui Sistem de Management al Securității Informațiilor în organizații, prezentând totodată principalele proceduri pe care le implică procesul de implementare. Necesitatea acestor a fost evidențiată atât prin analiza stadiului actual al cercetării, precum și prin rezultatele cercetării statistice, iar elementele de originalitate sunt în conformitate cu cele patru obiective propuse.

Primul capitol analizează stadiul actual al cercetării din domeniul securității informațiilor, rezumând principalele direcții de cercetare referitoare la standardul ISO 27001, atât în versiunea actuală, din anul 2013, cât și cea precedentă (2005). Studiul a scos în evidență lipsa unor cercetări în domeniul corelării standardului cu GDPR, precum și necesitatea elaborării unui ghid complet, care să abordeze toate clauzele și controalele standardului, într-o manieră care să faciliteze implementarea.

Cel de-al doilea capitol tratează obiectivele tezei și metodologia cercetării. Cercetarea propusă vizează un obiectiv principal (*Elaborarea unui instrument de analiză GAP, pentru verificarea simultană a conformității unei organizații cu prevederile standardului ISO27001:2013 și ale Regulamentului GDPR*), precum și trei obiective secundare, care se află într-o relație de interdependență cu obiectivul principal:

O2. Elaborarea unei analize a standardului ISI27001:2013, care să faciliteze implementarea Sistemului de Management al Securității Informațiilor în organizații, prin detalierea procedurilor pe care o organizație trebuie să le adopte, pentru a se pregăti în vederea auditului independent de certificare a conformității cu cerințele standardului ISO 27001.

O3. Maparea Clauzelor și controalelor standardului ISO27001:2013 cu prevederile Regulamentului GDPR, prin care se vor analiza principalele elemente de corespondență dintre cele două ducumente, pentru a se observa în ce măsură sunt complementare în contextul unei organizații care gestionează date cu caracter personal și care și-a fixat ca obiectiv implementarea Sistemului de Management al Securității Informațiilor (ISMS).

O4. Elaborarea unui chestionar de evaluare a nivelului de conformitate al organizațiilor cu cerințele standardului ISO27001: 2013. Prin acest obiectiv, s-a urmărit analizarea nivelului de conformitate al organizațiilor cu cerințele standardului, pentru a fi identificate principalele dificultăți cu care se confruntă organizațiile. Astfel, s-au identificat o serie de proceduri a căror implementare este deficitară

într-un număr considerabil de organizații, iar rezultatele vor constitui puncte de plecare pentru cercetări ulterioare.

Cel de-al treilea capitol constă într-o analiză obiectivă asupra procedurilor prin care organizația poate obține conformitatea cu standardul ISO 27001. Astfel, au fost abordate fiecare clauză din conținutul standardului, precum și controalele din Anexa A, oferind interpretări privind modalitatea de implementare. Conținutul acestui capitol constituie totodată un îndrumar util atât persoanelor din managementul organizațiilor care gestionează arhive de date, precum și personalului care este responsabil cu implementarea procedurilor specifice, contribuind la înțelegerea cerințelor.

Cel de-al patrulea capitol vizează corelarea standardului cu Rewgulamentul european GDPR și cuprinde o mapare a fiecărui articol din Regulament, cu clauzele și controalele din standard, fiind astfel identificate toate elementele de corespondență dintre cele două documente.

Cel de-al cincilea capitol valorifică rezultatele capitolului precedent și pornind de la maparea celor două documente, propune un instrument de analiză GAP pentru verificarea conformității organizației, în raport cu cele două documente, simultan. Totodată, instrumentul de analiză corelează cerințele cu documentele livrabile pe care organizația trebuie să le elaboreze.

Cel de-al șaselea capitol constă într-o cercetare statistică, realizată asupra unui eșantion de 192 de organizații, privind conformitatea cu prevederile standardului ISO 27001. Totodată, sunt prezentate corelări cu implementarea măsurilor cerute de Regulamentul GDPR, interpretarea acestora fiind făcută în baza analizei GAP și a matricei de mapare dezvoltate tot în cadrul tezei.

Ultimul capitol prezintă concluzii asupra cercetării și evidențiază contribuțiile originale pe care teza le propune, prin prisma atingerii celor patru obiective de cercetare. Totodată, este analizată și măsura în care rezultatele obținute pot fi valorificate, atât în sectorul economic, cât și pentru dezvoltarea unor direcții viitoare de cercetare.

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 și 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.

Implementarea GDPR de către organizații ar trebui privită în contextul atingerii obiectivelor lor specifice. Există o necesitate clară de a sublinia beneficiile sale pentru organizații și valorile adăugate pentru afaceri. Este absolut greșit să înțelegeți GDPR ca o altă restricție la mediul de operare. GDPR este un instrument pentru generarea unui avantaj strategic bazat pe încrederea între organizație, angajații săi, clienți și parteneri.

CONSIDERAȚII INTRODUCTIVE. STADIUL ACTUAL AL CERCETARII IN DOMENIUL IMPLEMENTARII STANDARDULUI ISO 27001

I.1. 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.

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 frauda 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 [41].

Deoarece securitatea informațiilor are un rol foarte important în susținerea activității organizațiilor, este oportun să existe un standard de referință care să reglementeze guvernanța în acest domeniu. Există mai mult0e standarde pentru guvernanță IT care fac referire la securitatea informațiilor. Cu toate acestea, din mai multe motive, unele dintre aceste standarde nu sunt bine adoptate de organizații [44]. Studiul comparativ, realizat pentru a determina punctele lor tari, concentrarea, componentele principale și nivelul de adoptare, a concluzionat că, la nivel mondial, standardul ISO 27001 este cel mai răspândit standard din domeniul securității informațiilor.

I.2. 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 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 securitatea informațiilor, 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.

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 ISMS documentat, în cadrul unei organizații [31]. 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-Ac* (PDCA) [12], care urmărește stabilirea, implementarea, monitorizarea și îmbunătățirea eficacității sistemului ISMS al unei organizații.

Există numeroase motive pentru a implementa standardul internațional ISO 27001, care descrie cele mai bune practici pentru un sistem de management al securității informațiilor. El ajută organizațiile să-și îmbunătățească securitatea, să respecte regulamentele de securitate cibernetică, să-și protejeze și să-și consolideze reputația.

Un sistem ISMS 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 ISMS conform cu standardul ISO 27001 poate ajuta organizațiile să identifice și atenueze riscurile legate de securitatea informațiilor, 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 [36] și prin urmare, este potrivit pentru implementarea și evaluarea diferitelor măsuri specifice.

I.3. Cercetări privind implementarea standardului ISO 27001

Mai mulți autori au investigat aspectele legate de standardele de securitate, precum și practicile de implementare la nivel organizațional și național.

Cheng-Yuan Ku, Yi-Wen Chang și David C. Yen de la Taiwan National Chung Cheng University [35] au analizat factorii-cheie privind implementarea unui sistem ISMS de succes, bazat pe standardul BS 7799. Rezultatele acestei cercetări indică faptul că experiențele de succes, disponibilitatea documentelor, constrângerile legate de costuri, instruirea organizațională, precum și cultura organizațională reprezintă motivații importante pentru implementarea ISMS.

Standardul ISO 27001, ca Sistem de Management al Securității Informațiilor, se impune din ce în ce mai mult ca standard de securitate în organizații. În 2008 au fost certificate peste 4457 de organizații pe plan mondial. Cu toate acestea, înregistrarea unui sistem ISMS nu mai spune nimic despre calitatea și performanța implementării sale. Astfel, Wolfgang Boehmer [9] a susținut că este esențial să existe un instrument care să măsoare eficiența și eficacitatea economică a implementării unui Sistem de Management al Securității Informației, bazat pe standardul ISO 27001, într-o organizație. În lucrare, autorul a introdus un instrument de măsurare a indicatorilor-cheie de performanță (Key Performance Indicator, KPI), bazat pe patru niveluri ierarhice, care ar permite unei organizații să evalueze eficiența și eficacitatea implementării unui sistem ISMS, bazat pe standardul ISO 27001.

Ulterior, Wolfgang Boehmer [8] a analizat modul în care managementul organizației trebuie să ia decizii cu privire la selectarea controalelor corespunzătoare în timp ce implementează ISO 27001, pornind de la anumite studii de caz. Boehmer a evaluat eficiența și eficacitatea implementării sistemului ISMS prin utilizarea KPI și a concluzionat că indicatorii – cheie de performanță ale acestor două dimensiuni sunt compromisuri.

Carol W. Hsu [28] a investigat comportamentele diferitelor grupuri sociale implicate în procesele de implementare ale standardului ISO 27001. Pe baza unui studiu de caz realizat în Taiwan, autorul a demonstrat cum diferite persoane, cu diferite roluri acționează în mod diferit în timpul implementării ISO 27001.

Analizând accesul și securitatea informațională în contextul Marii Britanii, Elizabeth Lomas concluzionează că, prin integrarea standardului ISO 27001, împreună cu standardul de management al înregistrărilor ISO 15489, vor fi furnizate strategii de guvernanță informațională holistice, care sunt receptive la schimbare [37].

Amplificarea dependenței organizaționale față de tehnologia informației, precum și agravarea impactului incidentelor de securitate a informațiilor, au determinat ca securitatea informațiilor să devină una dintre cele mai importante preocupări ale managementului. Deși, standardul ISO 27001 oferă îndrumări pentru un Sistem de Management al Securității Informațiilor, costurile de implementare și de acreditare pot fi, de asemenea, considerabile. Autorii studiului privind impactul certificării ISO 27001 asupra performanței organizației [29] au constatat că, în ansamblu, majoritatea studiilor actuale privind standardul ISO 27001 se concentrează asupra procesului de implementare, inclusiv luarea deciziilor în timpul implementării, motivul și obiectivul implementării, precum și evaluarea eficienței implementării sistemului de management al securității informațiilor.

În opinia autorilor Susanne Dobratz et al. [20], securitatea informațiilor, 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 ISO 27000. Procedurile de certificare și de autoevaluare sunt, de asemenea, abordate de această serie de standarde. Rezumând rezultatele studiului privind relevanța și utilizarea standardelor de management al calității pentru conservarea pe termen lung și nevoia specifică de standardizare a arhivelor digitale, autorii constată că adoptarea de standarde pentru managementul calității, procese și securitate, ca factori importanți în crearea unor depozite digitale demne de încredere, nu a ajuns încă într-un număr mare de organizații, care au obligația de conservare pe termen lung a obiectelor digitale. Rezultatele studiului arată, de asemenea, că participanții, în general, recunosc importanța deosebită a acestor standarde pentru instituțiile locale, dar au probleme în utilizarea acestor standarde în practică. Organizațiile participante la sondaj le folosesc mai mult în scop de orientare.

J. Stuart Broderick [10] susține că un Sistem de Management al Securității Informațiilor aflat în responsabilitatea exclusivă a departamentului de securitate al organizației este doar un mit. În realitate, un sistem ISMS trebuie să fie gestionat de conducerea executivă a organizației, în caz contrar implementarea ISMS fiind sortită eșecului.

Syed Irfan Nabi și colegii [39] au efectuat un studiu pentru a evalua statutul securității informațiilor în organizațiile din Arabia Saudită. Studiul a vizat aspectele tehnice ale securității informațiilor, gestionarea riscurilor și gestionarea asigurării informațiilor. Rezultatele obținute de autori oferă o perspectivă asupra nivelului actual de securitate a informațiilor din diferite sectoare, care poate fi util pentru o mai bună înțelegere a detaliilor complexe privind securitatea informațiilor de la nivel global. De asemenea, rezultatele pot fi foarte utile pentru factorii de decizie în domeniul securității informațiilor din cadrul Guvernului, precum și pentru organizațiile din sectorul privat.

Ulterior, Khalid I. Alshitri și Abdulmohsen N. Abanumy [3] și-au propus să investigheze motivele care stau la baza adoptării scăzute a standardului ISO 27001 în organizațiile publice din Arabia Saudită. Problemele legate de managementul resurselor umane, cum ar fi lipsa expertizei în domeniul securității informațiilor, lipsa programelor de instruire, educație și sensibilizare, precum și cererea de salarizare ridicată pentru profesioniștii din domeniul securității, au fost considerate cele mai importante bariere în calea implementării cu succes a standardului ISO 27001 în organizațiile publice din Arabia Saudită. Autorii menționează că este nevoie de cercetări suplimentare pentru a obține o mai bună înțelegere a factorilor care afectează implementarea ISO 27001 în organizațiile publice din Arabia Saudită. Prin urmare, studiile viitoare s-ar putea concentra pe colectarea datelor de la alte organizații pentru a valida și a spori rezultatele din studiul menționat și pentru a investiga dacă diferite structuri organizaționale încurajează sau interzic implementarea ISO 27001. De asemenea, autorii menționează că, în cele din urmă, rezultatele acestui studiu pot să nu fie generalizabile altor tipuri de organizații (de exemplu, private), care diferă în multe privințe de organizațiile publice și, prin urmare, pot fi observate diferențe. Autorii sugerează că studiile viitoare s-ar putea concentra pe examinarea relației dintre problemele de gestionare a resurselor umane și implementarea ISO 27001 în organizațiile private din Arabia Saudită.

Potrivit lui Fomin et al. [22] un motiv pentru adoptarea scăzută a standardului ISO 27001 în comparație cu standardele similare, cum ar fi ISO 9001 și ISO 14001, este lipsa interesului științific cu privire la standardul ISO 27001. Autorii au constatat că numărul de publicații dedicate standardului ISO 27001 este relativ scăzut comparativ cu cele dedicate sistemelor de management al securității informației. În plus, costul ridicat în bani și timp, precum și volumul mare de documente necesare au jucat un rol major în adoptarea scăzută a standardului, în comparație cu standardele referitoare la sistemele de management (MSS), cum ar fi ISO 9001 și ISO 14001.

Standardul ISO 27001 oferă un model pentru stabilirea, implementarea, funcționarea, monitorizarea, revizuirea, menținerea și îmbunătățirea unui Sistem de Management al Securității Informațiilor [11]. Lucrarea autorului Alan Gillies [23] încearcă să ia în considerare implementarea globală a seriei de standarde ISO 27000 și să le compare cu ratele de adoptare pentru ISO 9000 și ISO 14000. Totodată, lucrarea a urmărit să compare barierele în calea implementării pentru diferitele standarde. Studiile anterioare sugerează că implementarea ISO 27001 este mai lentă decât celelalte standarde [16, 22]. Absorbția ISO 27001 a fost mai lentă decât standardele ISO 9001 și ISO 14001 asociate sistemelor de management, cu aproximativ jumătate din certificările în comparație cu ISO 14001. Ca răspuns la problemele ridicate în studiile precedente, Alan Gillies analizează modul în care o abordare bazată pe un model de maturitate poate fi utilizată pentru a ajuta la depășirea acestor bariere, în special în organizațiile mai mici. Principala contribuție a acestei lucrări este dată de elaborarea unui cadru etapizat pentru a simplifica procesul pentru organizațiile care lucrează în direcția ISO 27001 și pentru a oferi beneficii semnificative înainte ca sistemele să fie suficient de mature pentru a obține certificarea.

Tolga Mataracioglu și Sevgi Ozkan [38] susțin că legislația privind securitatea informațiilor publice, pe care o organizație trebuie să o respecte, joacă un rol semnificativ în acceptarea de către utilizator. Modelul propus de autori a fost construit pe baza a patru elemente care au avut un efect substanțial asupra acceptării de către utilizatori a implementării ISO 27001 în organizațiile din Turcia. Cele patru componente incluse în acest model au fost: utilitatea percepută, atitudinea față de utilizare, normele sociale și speranța de performanță. Rezultatele studiului arată că legislația privind securitatea informației publice, pe care organizațiile trebuie să o respecte, este semnificativ legată de acceptarea de către utilizatori a procesului de implementare a standardului ISO 27001, în caz contrar legislația încetinind productivitatea organizației.

Incidentele de securitate IT reprezintă o amenințare majoră pentru executarea eficientă a strategiilor corporative. Deși standardele de securitate a informațiilor oferă o abordare holistică pentru a atenua aceste amenințări, iar actele juridice solicită punerea în aplicare a acestora, companiile se abțin de multe ori de la aplicarea standardelor de securitate a informațiilor. Un colectiv de autori de la Secure Business Austria [40] a realizat o analiză a cauzelor de abținere de la aplicarea standardelor de securitate a informațiilor, cum ar fi ISO 27001. Astfel, autorii au susținut, în ciuda recunoașterii de către organizații a importanței aplicării standardelor de securitate a informațiilor, că respectivele organizații

se abțin de multe ori să facă acest lucru din cauza costurilor mai ridicate ale implementării unui astfel de standard și a lipsei de dovezi că un astfel de standard are raportul cost / beneficiu pozitiv. În lucrare, autorii au sugerat o abordare în două faze, care ar ajuta factorii de decizie să definească cele mai bune seturi de contramăsuri, pentru a respecta standardele de securitate, cum ar fi ISO 27001. Ca prim pas, au sugerat o ontologie de securitate care ar servi drept bază de cunoștințe pentru implementarea potențialelor contramăsuri. Al doilea pas constă în implementarea unui sistem de sprijin al deciziilor care ar genera soluții alternative pentru factorii de decizie, care sunt atât fezabile în raport cu constrângerile date, cât și eficiente în ceea ce privește obiectivele multiple. Abordarea a fost implementată într-un instrument și testată printr-un studiu de caz. Acesta nu numai că sprijină factorii de decizie în definirea controalelor necesare pentru certificare, dar le oferă și informații privind eficiența controalelor alese în ceea ce privește obiective multiple definibile.

Odată cu dezvoltarea comerțului electronic, multe organizații se confruntă cu provocări de securitate fără precedent. Tehnicile de securitate și instrumentele de management au atras atenția atât specialiștilor din mediul academic, cât și a practicanților. Cu toate acestea, nu există un cadru teoretic pentru gestionarea securității informațiilor. Hong et al. [27] au încearcat să integreze teoria politicii de securitate, teoria managementului riscului, teoria controlului și auditului, teoria sistemelor de management și teoria contingenței pentru a construi o teorie cuprinzătoare a managementului securității informației (ISM). Autorii au sugerat un sistem integrat de gestionare a securității informațiilor. Totodată, această lucrare sugerează că o teorie a sistemelor integrate este utilă pentru înțelegerea managementului securității informațiilor, explicarea strategiilor de management al securității informațiilor și prezicerea rezultatelor managementului. În opinia autorilor această teorie poate constitui o bază teoretică solidă pentru cercetarea și aplicarea empirică.

Standardul de management al securității informațiilor ISO 27001 este construit pe ideea că securitatea informațiilor 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. Autorii articolului *The Information Security Ownership Question in ISO/IEC 27001 – an Implementation Perspective* [18] susțin că dreptul de proprietate asupra securității informațiilor este unul dintre elementele-cheie, care sunt pertinente pentru succesul realizării unor decizii măsurabile, eficiente, ușor de implementat. Cercetarea s-a concentrat pe două aspecte ale dreptului de proprietate asupra securității informațiilor: proprietatea asupra activului și proprietatea acțiunilor de tratare a riscurilor. Această lucrare prezintă, de asemenea, unele observații din încercările practice de implementare a unei metodologii de evaluare a riscului de securitate a informațiilor la nivelul întregii organizații. Observațiile au fost făcute în cadrul vizitelor de evaluare a certificării ISO/IEC 27001.

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 securitatea informațiilor 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.

În lucrarea *Information Security Management System Standards: A Comparative Study of the Big Five* [45] sunt prezentate rezultatele unui studiu comparativ privind standardele utilizate pe scară largă pentru securitatea informației, și anume: ISO 27001, BS 7799, PCIDSS, ITIL și COBIT. Această analiza comparativă a urmărit scopul de a determina punctele forte, concentrarea, principalele componente și adoptarea acestor standarde pe baza sistemului ISMS. Concluzia la care au ajuns autorii constă în faptul că fiecare standard are propriul rolul în implementarea ISMS. În unele standarde, cum ar fi ISO 27001 și BS 7799, accentul se pune pe Sistemul de Management al Securității Informațiilor ca domeniu principal, pe când PCIDSS se concentrează pe securitatea informațiilor legate de tranzacțiile de afaceri și smart card, iar ITIL și COBIT se concentrează asupra securității informațiilor și a relației acesteia cu managementul proiectelor și guvernanța IT. Cu referire la gradul de utilizare a standardelor la nivel mondial, se menționează că ISO 27001 este de primă importanță în comparație cu celelalte patru standarde, în special în ceea ce privește sistemul ISMS. Prin urmare, standardul este implementat mai ușor și este mai bine recunoscut de către părțile interesate (managementul superior, personal, furnizori, clienți, autorități de reglementare).

Diferite studii și experiențe de succes la nivel național și internațional, arată că punerea în aplicare a bunelor practici de implementare a ISO 27001 în organizații poate reduce riscurile, amenințările și vulnerabilitățile. Țările care cunosc această situație și care țin cont de aspecte cum ar fi:

- orice risc sau amenințare la adresa securității informației poate conduce la pierderi reale și potențiale ale organizațiilor cu repercusiuni financiare, juridice, și reputaționale;
- faptul că informația nu este doar valoroasă și critică, fiind și 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.

Un grup de cercetători din universitățile din Norvegia [25] a efectuat un sondaj care a implicat organizațiile norvegiene pentru a evalua eficiența implementării măsurilor de securitate a informațiilor.

Constatările autorilor au arătat că măsurile tehnice, cum ar fi politicile și procedurile de securitate, sunt cel mai frecvent implementate. Activitățile de conștientizare sunt aplicate de către organizații într-o măsură mult mai mică, dar în același timp acestea sunt evaluate ca fiind măsuri organizaționale mai eficiente decât cele tehnico-administrative. În consecință, studiul arată o relație inversă între implementarea măsurilor organizaționale de securitate a informațiilor și rezultatele evaluării percepției privind măsurile organizaționale de securitate a informațiilor.

Dr. Lakhwinder Pal Singh și colegii de la National Institute of Technology din India [43] au realizat un studiu în cadrul organizațiilor indiene pentru a măsura impactul certificării ISO asupra parametrilor de ieșire. Constatările lor au arătat că implementarea ISO sporește performanța de ieșire a firmelor; are efecte pozitive asupra majorității aspectelor parametrilor unei organizații.

În anul 2007 Grupul Wolcott a realizat un studiu pentru a explora utilizarea ISO 27001 în calitate de cadru pentru evaluarea și reglementarea eficientă a securității informațiilor [4]. Autorii acestui studiu au afirmat că protejarea sistemelor informatice și demonstrarea conformității cu standardele acceptate de bună practică reprezintă o parte tot mai importantă a unui bun management al afacerilor. Grupul Wolcott a susținut că majoritatea organizațiilor sunt atât de concentrate pe provocările individuale ale securității informațiilor, încât le lipsește imaginea de ansamblu.

David Henning [26] a studiat eficiența utilizării Project Management Body of Knowledge în implementarea standardului ISO 27001. Ca și concluzie, autorul a indicat că implicarea și sprijinul superior al managementului, precum și al managementului de proiecte sunt factori-cheie pentru succesul procesului de implementare al standardului ISO 27001.

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. De fapt, securitatea informațiilor devine o componentă foarte importantă pentru activele necorporale ale organizației, nivelul de încredere și încrederea părților interesate fiind indicatori de performanță pentru organizații. În lucrarea *Information Security Challenge and Breaches: Novelty Approach on Measuring ISO 27001 Readiness Level* [44] se discută despre provocările și încălcările securității informațiilor. Totodată, articolul face referire la câteva cercetări din domeniul securității informațiilor ca date secundare, cum ar fi sondajul privind încălcările securității informațiilor și sondajul global privind securitatea informațiilor, care au determinat autorii să ofere un cadru pentru înțelegerea termenului și conceptului standardelor de management al securității informațiilor. **De asemenea, autorii s-au exprimat în favoarea implementării acestui standard în aplicațiile software, pentru evaluarea nivelului de pregătire a unei organizații pentru implementarea standardului de securitate a informațiilor ISO 27001.**

Standardul internațional ISO 27001 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;
- 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.

Widhi Johanes Candra et al. [14] consideră că cea mai mare provocare în planificarea securității informațiilor ține de obținerea preciziei în etapa de analiză a breșelor. Conform ghidului de implementare al ISMS bazat pe ISO/IEC 27001:2013, planificarea sistemului ISMS are 5 etape. Cele 5 etape sunt: definirea intervalului, efectuarea analizei breșelor, realizarea evaluării riscurilor, determinarea controlului și țintei și determinarea politicii și procedurii ISMS.

Etapa de analiză a breșelor este necesară pentru a evalua poziția actuală a organizației privind implementarea sistemului ISMS. Cercetarea realizată a sugerat utilizarea procesului de ierarhie analitică pentru a determina ce control de securitate a informațiilor se potrivește cel mai mult nevoilor și obiectivelor organizației. Studiul a fost realizat pe baza unei organizații din Indonezia, numită Institutul XYZ. Institutul XYZ este o organizație non-profit, care realizează colectarea de informații din spațiul cibernetic. Institutul depinde de punerea în aplicare a tehnologiei informației și prin urmare, are obligația de a-și asigura informațiile și infrastructura. Riscurile ridicate care vizează sistemele de informații, cum ar fi accesul neautorizat și atacul virușilor, au determinat Institutul să prevadă implementarea sistemului ISMS, bazată pe standardul ISO/IEC 27001:2013, la procesele de afaceri ale organizației.

Metoda procesului de ierarhie analitică, folosită în cadrul Institutului XYZ, a determinat succesul analizei breșelor și a permis prioritizarea recomandărilor pentru eliminarea lacunelor, din cele mai potrivite pentru organizație. Pentru Institutul XYZ, cea mai mare prioritate este abordarea controalelor de securitate din secțiunea A.11, din Anexa A a standardului ISO/IEC 27001:2013 (securitatea fizică și securitatea mediului), iar a doua prioritate este dată de secțiunea A.9 (controlul de acces). Lista rezultată din această analiză poate fi utilă pentru a ajuta organizația să-și fixeze prioritățile în ceea ce

privește direcțiile de acțiune și alocarea resurselor privind cei mai importanți factori de securitate a informațiilor. Totodată, această listă poate ajuta organizația în implementarea și certificarea sistemului ISMS pe baza standardului ISO/IEC 27001:2013, adaptată special pentru nevoile organizației.

Adoptarea metodologiilor și principiilor pentru dezvoltarea proceselor care iau în considerare securitatea informațiilor, devine din ce în ce mai răspândită. Multe organizații din întreaga lume au Sisteme de Management al Securității Informațiilor care îndeplinesc cerințele standardului ISO 27001. Pentru a îndeplini cerințele acestui standard, organizația trebuie să cheltuiască timp și bani. Aceste eforturi depind, în principal, de dimensiunea organizației și de statutul sistemului de management al securității informațiilor. Studiul, realizat de B. Si Ahmed și F. Nibouche [2], s-a axat pe identificarea unui model matematic privind estimarea efortului pentru implementare a unui sistem ISMS certificat de ISO 27001. Pentru atingerea obiectivelor cercetării, care a fost efectuată între 2016 și 2017, au fost trimise chestionare către 1040 de organizații din diferite domenii, ceea ce constituie 9% din numărul total de organizații certificate din lume în anul 2015. Autorii studiului au ajuns la concluzia că efortul și costul de implementare al unui sistem ISMS certificat de ISO 27001 depind de starea sistemului înainte de lansarea proiectului, raportată la obiectivul standardului. Rezultatele studiului oferă un model de estimare bazat pe dimensiunea organizației și gradul de neconformitate, acest model de predicție fiind valid statistic, dar, totuși, eroarea de estimare rămânând semnificativă. În perspectivă, autorii preconizează să continue analiza statistică, pentru îmbunătățirea modelului de predicție și reducerea intervalului de prognoză.

Standardele internaționale ISO pentru sisteme de management standardizate ajută organizațiile să îndeplinească cerințele pentru îmbunătățirea proceselor lor de funcționare. Începând cu anul 2012, ISO a început să dezvolte o nouă structură numită Anexa SL, pentru standardele sistemului de management. Această structură sugerează o nouă abordare concepută cu intenția de a armoniza standardele sistemului de management pentru a integra mai ușor standardele multiple.

Această nouă structură pune accentul pe aspectele de conducere în standardele sistemului de management. Obiectivul principal al lucrării *Study on Integration and Leadership Styles of Management Systems Based on a High Level Structure* [33] este, în primul rând, de a găsi în cadrul organizațiilor dovada că structura de înalt nivel conduce la o mai ușoară integrare a sistemelor de management. Autorii au identificat că Anexa SL are un efect pozitiv asupra integrării sistemelor de management. Această cercetare este unul dintre primele studii care iau în considerare efectele Anexei SL. Rezultatele, atunci când sunt utilizate în mod corespunzător de către organizații, ar putea conduce, în mod concret, la identificarea soluțiilor pentru probleme comune legate de standardele sistemului de management din cadrul acestora. Autorii au întâmpinat dificultăți la momentul redactării lucrării, deoarece a existat un număr mic de organizații cu experiență în Anexa SL. Standardul ISO 27001:2013 este unicul standard cu o structură de înalt nivel care a fost disponibilă în ultimii doi ani.

Studiul *Theory and Practice of Integrating Management Systems with High Level Structure* [34] se concentrează asupra organizațiilor care operează cel puțin două sisteme de management bazate pe standarde ISO și analizează abordările privind implementarea și operarea acestor sisteme. Autorii prezintă, în primul rând, rezultatele empirice bazate pe un sondaj și, în al doilea rând, două studii de caz care sunt comparate între ele. O atenție specială se acordă aspectului de integrare în contextul structurii de înalt nivel a standardelor sistemului de management ISO. Rezultatul studiului arată că majoritatea companiilor cu mai mult de un standard de sistem de management încearcă să integreze sistemele de management care utilizează Anexa SL (secțiunea ISO/IEC), fapt ce ajută la îmbunătățirea integrării prin structurarea proceselor și a documentației necesare într-un mod similar. În ciuda structurii de înalt nivel și a proceselor principale, există multe diferențe în integrarea organizațiilor analizate. Pe baza acestor constatări, autorii sugerează îmbunătățirea Anexei SL.

Problemele implementării standardului ISO 27001 sunt abordate inclusiv în studii realizate de cercetătorii din România. Astfel, Valerica Greanu-Șerban [24] menționează că avantajele unui Sistem standardizat de Management al Securității Informațiilor sunt regăsite în reducerea riscurilor la adresa securității informatice și abordarea structurată și standardizată a sistemului informațional. Familiarizarea conducerii cu problemele legate de securitatea informațiilor și controalele asociate va determina, în mod direct, îmbunătățirea mediului de control, implicând, în același timp, revizuirea cu regularitate a politicilor și procedurilor de securitate.

În prezent, odată cu amplificarea incidentelor de securitate a informațiilor, standardul ISO 27001 dezvăluie clienților angajamentul de a asigura niveluri înalte de securitate a informațiilor. Astfel, clienții pot avea încredere că informația lor este protejată, integritatea sa este păstrată, fiind accesibilă numai persoanelor autorizate. De asemenea, sincopele în securitatea informațiilor pot permite preluarea, furtul, degradarea sau pierderea datelor critice. Întrucât informația este o resursă prețioasă care solicită o protecție adecvată, autorii constată că standardul ISO 27001 pentru Sistemele de Management al Securității Informațiilor influențează pozitiv ESI. În plus, ISO 27001 ajută la o supraveghere sporită a activelor informaționale și aplică măsuri de control pentru a proteja informațiile.

Aspectele privind implementarea și certificarea, în cadrul unei organizații, a unui sistem de management al securității informațiilor bazat pe standardul internațional ISO 27001:2006 este abordat în lucrarea unui grup de autori de la Universitatea Politehnică din București [42]. Abordarea bazată pe procese, compatibilitatea cu alte sisteme de management și cerințele generale, de exemplu gestionarea riscurilor de securitate, controlul documentelor, auditul intern, îmbunătățirea continuă, sunt descrise în această lucrare. De asemenea, lucrarea explică diferența dintre certificare și acreditare. Pe baza standardului internațional ISO 27001:2006, sunt prezentate și comentate cerințele de documentare, procesele și cerințele generale ale unei organizații pentru implementarea unui sistem ISMS. O altă contribuție a lucrării se referă la procesul de certificare și la avantajele acestuia, compatibilitatea cu alte sisteme / standarde de management.

Implementarea și certificarea unui sistem de management al securității informațiilor în concordanță cu standardul ISO 27001 este o modalitate de a furniza încredere tuturor părților interesate. Astfel, organizațiile trebuie să cunoască particularitățile noului standard ISO 27001:2013 care este foarte diferit de vechea variantă din 2005. Lucrarea lui Țigănoaia Bogdan [49] este un studiu comparativ al standardelor internaționale privind sistemele de management al securității informațiilor în cadrul organizațiilor. Este vorba despre ISO/IEC 27001:2005 și versiunea revizuită a acestuia, ISO/IEC 27001:2013. Lucrarea prezintă, într-o analiză comparativă, aspecte referitoare la: structura standardelor, noile concepte sau actualizări și termeni introduși în ISO/IEC 27001:2013. Totodată, lucrarea oferă suport organizațiilor în tranziția către noile cerințe ale standardului, cum ar fi cerințe privind evaluarea riscurilor ce au fost aliniate cu standardul ISO 31000.

În lucrarea *Some Aspects Regarding the Information Security Management System within Organizations – Adopting the ISO/IEC 27001:2013 Standard. Studies in Informatics and Control,* autorul prezintă o analiză a corelației dintre riscurile de afaceri și caracteristicile și avantajele standardului ISO/IEC 27001. De asemenea, se propune un ghid pentru adoptarea standardului ISO/IEC 27001:2013, care presupune o autoevaluare a organizației și a strategiilor. În același timp, în lucrare este propusă metodologia pentru implementarea ghidului cu o etapă pregătitoare (autoevaluarea organizației) și o analiză finală a conformității (auditul ISMS). Autorul consideră că această abordare poate ajuta organizațiile în utilizarea practică a standardului, precum și să înțeleagă relația dintre ISO/IEC 27001:2013 și standardul precedent ISO/IEC 27001:2005.

Câteva aspecte practice pentru organizații privind implementarea standardului ISO/IEC 27001:2013 sunt prezentate, de asemenea, în lucrarea *Theoretical and practical considerations regarding the information security management system within organizations in concordance with the new international standard ISO / IEC 27001: 2013* . Același autor oferă răspunsuri la unele întrebări frecvente cu privire la conceptele, cerințele și modificările introduse în standardul ISO/IEC 27001:2013, precum și ce ar trebui să facă o organizație dacă este certificată sau este interesată de certificarea ISO/IEC 27001.

I4. 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 și 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).

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.

CAPITOLUL 2. OBIECTIVELE TEZEI ȘI METODOLOGIA CERCETĂRII

Cercetarea de față își propune să analizeze cerințele de conformitate ale standardului ISO 27001:2013, precum și procesele pe care managementul organizației, împreună cu departamentele de securitate, trebuie să le implementeze, pentru a obține conformitatea cu acest standard. Totodată, pe tot parcursul studiului se pune accentul pe corelarea standardului cu prevederile Regulamentului General de Protecția Datelor (GDPR).

Astfel a fost exprimată necesitatea existenței unui set de valori care să determine nivelul de conformitate al unei organizații, în raport cu cele două documente. Această nevoie se regăsește în sfera organizațiilor, publice sau private, indiferent de mărimea lor, care doresc să devină conforme din punct de vedere al Standardului, respectiv Regulamentului.

Astfel, obiectivul principal al tezei (O1) constă în elaborarea unui instrument de analiză GAP, pentru verificarea simultană a conformității unei organizații cu prevederile standardului ISO27001:2013 și ale Regulamentului GDPR.

În acest scop, va fi dezvoltată o analiză a oportunităților și bunelor practici în domeniul utilizării instrumentului GAP în domeniul celor două documente, nefiind identificat niciun element care să contribuie la analizarea simultană a amândurora.

Pentru elaborarea instrumentului, este necesară maparea celor două documente, pentru a fi identificate toate punctele de corespondență, precum și livrabilele obligatorii și/sau opționale. Astfel, pentru atingerea obiectivului principal, este necesară atingerea obiectivelor secundare O2 și O3, care vor reprezenta punctele de plecare, în vederea obținerii rezultatului final.

Obiectivul O2 - Elaborarea unei analize a standardului ISI27001:2013, care să faciliteze implementarea Sistemului de Management al Securității Informațiilor în organizații este piatra de temelie a studiului, în această etapă fiind analizate cerințele celei mai noi versiuni a Standardului ISO 27001.

Analizarea celor 10 clauze, precum și a controalelor din Anexa A, au ca scop identificarea procedurilor necesare pentru implementarea Sistemului de management al Securității Informații (ISMS) într-o organizație. Astfel, în urma parcurgerii conținutului standardului, un pas important va fi dat de rezumarea conținutului fiecărei clauze și a fiecărui control din Anexa A, pentru a înțelege oportunitatea aplicării respectivei măsuri la nivelul unei organizații.

Totodată, se vor evidenția livrabilele (diverse politici și regulamente) pe care organizația trebuie să le adopte.

Nu în ultimul rând, prin atingerea acestui obiectiv se va urmări și redactarea unui îndrumar, destinat managementului organizațiilor care doresc să implementeze standardul. Un astfel de ghid are scopul de a facilita înțelegerea cerințelor de către managementul organizației, precum și de către personalul implicat în implementarea măsurilor, în vederea certificării conformității.

Obiectivul secundar O3 vizează maparea Clauzelor și controalelor Standardului ISO27001:2013 cu prevederile Regulamentului GDPR.

Atingerea acestui obiectiv va contribui esențial la obiectivul principal, respectiv dezvoltarea instrumentului de analiză GAP, care se va raporta la ambele documente, urmărind atingerea conformității, de către o organizație, în ambele direcții.

Procesul de mapare se va realiza pornind de la articolele din Regulamentul GDPR, cărora le vor fi asociate clauzele sau controalele corespunzătoare.

Cel de-al patrulea obiectiv al tezei vizează elaborarea și implementarea unui chestionar de evaluare a nivelului de conformitate al organizațiilor cu cerințele standardului ISO27001: 2013.

Astfel, prin acest chestionar, se are în vedere analizarea nivelului de conformitate al organizațiilor, cu privire la implementarea unui Sistem de Management al Securității Informației. Chestionarul va fi elaborat pornind de la structura formularului de analiză GAP și va include principalele controale din Anexa A a Standardului. În etapa de analiză și interpretare a rezultatelor, se va analiza, prin corelare, conformitatea cu cerințele GDPR, prin prisma punctelor de corespondență dintre cele două documente.

CAPITOLUL 3. ELEMENTE PRIVIND IMPLEMENTAREA STANDARDULUI ISO/IEC 27001:2013

III.1. Considerații introductive

Abordarea riscurilor de securitate a informațiilor reprezintă o provocare în contextul societății informaționale bazată pe cunoaștere.

Una dintre soluțiile abordate de organizațiile preocupate să protejeze în mod corespunzător informațiile a fost înființarea și menținerea unui sistem de management al securității informațiilor (ISMS). Acest obiectiv poate fi atins prin implementarea ISO 27001: 2013.

În același timp, numeroase alte organizații privesc standardele referitoare la securitatea informațiilor ca pe niște simple liste de verificare, sau ca pe politici și proceduri dificile, care nu fac decât să le invalideze activitatea curentă.

Pornind de la aceste convingeri, organizațiile eșuează în procesul de proiectare a unui Sistem de Management al Securității Informațiilor (ISMS), fapt ce le diminuează privește performanța operațională.

Prezentul capitol cuprinde o analiză a conținutului standardului ISO/IEC 27001, referitor la implementarea Sistemului de Management al Securității Informațiilor. În cadrul analizei clauzele din secțiunile 4 - 10, precum și controalele de securitate din Anexa A. Totodată, au fost analizate și situații ipotetice care pot apărea în cadrul organizației, atât în faza de implementare, cât și în cea de mentenanță, acestea având rolul de a facilita înțelegerea standardului.

Abordarea clauzelor a fost făcută în aceeași ordine ca în conținutul standardul ISO 27001: 2013.

Astfel, **secțiunile 1 – 3** ale standardului se referă la domeniul de aplicare, concepte și abordări ale proceselor legate de implementare, precum și la termenii și definițiile aplicabile, în acest caz realizându-se o strânsă legătură cu standardul ISO 27000.

Secțiunile 4 – 10 ale standardului cuprind clauzele necesare pentru a certifica un Sistem de Management al Securității Informațiilor în conformitate cu ISO 27001: 2013:

4. Contextul organizației

5. Leadership

6. Planificare

7. Suport

8. Operarea

9. Evaluarea performanței

10. Îmbunătățiri

Totodată, prezentul capitol analizează conținutul anexei A, cuprinzând controalele de securitate de la A.5 la A.18. Trebuie menționat faptul că în anexa A controalele sunt numerotate începând cu A5, deoarece acestea se află într-o relație directă cu controalele enumerate în standardul ISO 27002. ISO 27002 este un standard care oferă instrucțiuni de implementare pentru fiecare control, unde secțiunile 1-4 cuprind clauze introductive, în timp ce comenzile sunt enumerate în secțiunile 5-18.

III.2. Analiza conținutului clauzelor cuprinse în standardul ISO 27001: 2013

Impactul abordării proceselor

Respectarea cerințelor standardului ISO 27001: 2013 este obligatorie în vederea certificării organizației, dar o îndeplinire formală a respectivelor cerințe nu garantează capacitatea unei organizații de a asigura securitatea informațiile. Este necesar ca organizația să politicile de securitate în conformitate cu obiectivele specifice și cu contextul în care evoluează. În acest sens, o abordare corectă a ciclului PDCA este deosebit de utilă pentru implementarea Sistemului de Management al Securității Informațiilor.

Astfel, ciclul PDCA reprezintă o bază solidă pentru un Sistem de Management al Securității Informațiilor, fiind o modalitate optimă de a organiza și gestiona procesele de securitate din cadrul organizației.

Ciclul Plan – Do – Check – Act (PDCA)

Ciclul PDCA (planificare – implementare – verificare – acționare) este un model repetitiv în patru etape pentru îmbunătățirea continuă a proceselor de management.

Ciclul PDCA a fost popularizat de W. Edwards Deming, inginer american, consultant statistician și de management, adesea considerat un pionier al sistemelor de control al calității.

Teoriile lui Deming constituie baza pentru standardele de calitate TQM (Total Quality Management) și ISO 9001. Deming a preluat structura ciclului de la Walter Andrew Shewhart, fizician american, inginer și statistician care este adesea considerat părintele controlului statistic al calității.

Orice organizație evoluează într-un mediu dinamic, cu influențe interne și externe. Sistemul de Management al Securității Informațiilor trebuie să fie capabil să se adapteze schimbărilor pentru a răspunde unor provocări din ce în ce mai diverse. Standardul ISO 27001: 2013 urmărește să asigure adaptarea la schimbări și îmbunătățirea rezilienței prin adoptarea ciclului PDCA.

Ciclul PDCA reprezintă o metodologie recunoscută la nivel global, care este utilizată în numeroase standarde și sisteme de management.

Clauza 4: Contextul organizației

Organizația trebuie să determine toate aspectele interne și externe care ar putea fi relevante pentru scopurile sale și pentru atingerea obiectivelor Sistemului de Management al Securității Informațiilor.

Clauza 4.1 este a fost introdusă odată cu revizuirea din 2013 a standardului ISO 27001, având o formulare generalistă, fapt ce a creat oarecare dificultăți în cadrul proceselor de implementare. Clauza se regăsește și în standardul ISO 22301, referitor la continuitatea afacerii și reziliență.

Implementarea corectă a standardului ISO 27001 presupune ca organizația să identifica aspectele interne și externe care ar putea influența Sistemul de Management al Securității Informațiilor. În acest sens, se face trimitere la clauza 5.3 din standardul ISO 31000, care oferă explicații detaliate.

ISO 31000 este un standard de referință în domeniul managementul riscului, putând fi utilizat pentru identificarea factorilor interni și externi. Totodată, elemente similare sunt incluse și în standardul ISO 27004: 2014, referitor la evaluarea performanțelor securității informațiilor și eficacității unui sistem de management al securității informațiilor.

În contextul standardului ISO 27001, pentru determinarea aspectelor interne se vor analiza următorii factori: structura organizatorică, rolurile și responsabilitățile atribuite, strategia și obiectivele organizației, capacitățile și resursele, cultura organizațională, strategia de comunicare, etc.

Înțelegerea nevoilor și așteptărilor părților interesate

Standardul ISO 27001 presupune identificarea părților interesate în ceea ce privește Sistemul de Management al Securității Informațiilor, nevoile și interesele acestor părți, cerințele legale, precum și obligațiile contractuale. În acest sens, este necesar să se analizeze care dintre aceste aspecte ar deveni relevante în ceea ce privește conformitatea cu standardul.

Clauza 4.2 se regăsește atât în standardul ISO 27001, cât și în ISO 22301. Identificarea părților interesate reprezintă o componentă crucială pentru dezvoltarea Sistemului de Management al Securității Informațiilor (ISMS) sau a celui de Management al Continuității Afacerii (BCMS).

Conceptul de părți interesate este unul simplu, care include totalitatea persoanelor fizice, juridice sau a structurilor care pot influența securitatea informațiilor precum și persoanele sau structurile care pot fi afectate de activitățile organizației.

Determinarea sferei de aplicare a Sistemului de Management al Securității Informațiilor

Domeniul Sistemului de Management al Securității Informațiilor a fost introdus în forma actuală odată cu revizuirea standardului, în 2013, fiind incluse o serie de concepte noi, precum interfețele și dependențele, care creează o viziune structurată asupra acestuia.

Domeniul de aplicare și limitele Sistemului de Management al Securității Informațiilor trebuie să fie analizate și definite pornind de la aspectele interne și externe, părțile interesate și cerințele acestora, activitatea organizației și direcțiile strategice, precum și interdependența cu alte organizații. Domeniul de aplicare să fie documentat.

Scopul principal al stabilirii domeniului Sistemului ISMS este definirea informațiilor pe care organizația urmărește să le protejeze, indiferent de suportul pe care acestea se află, de modalitatea de stocare, de locul în care acestea se află sau de modalitatea în care informațiile pot fi accesate.

Prin urmare, scopul ISMS trebuie să includă toată infrastructura, mobilă și imobilă a organizației.

În cadrul procesului de certificare, auditorul va verifica doar elementele cuprinse în domeniul de aplicare. Cu toate acestea, analizate prin prisma unei relații de interdependență, elementele trebuie să fie eficiente.

Clauza 5. Leadership

Persoanele implicare în managementul organizației, trebuie să se orienteze către implicarea resurselor umane în sprijinul Sistemului de Management al Securității Informațiilor.

Clauza 5.1 cuprinde numeroase elemente referitoare la responsabilitățile pe care persoanele din managementul organizației trebuie să și le asume, pentru a asigura conformitatea unor aspecte precum:

- Alinierea obiectivelor politicii de securitate cu politicile strategice și cu direcția generală a organizației.
- Integrarea conceptelor legate de securitatea informațiilor în activitatea organizației
- Asigurarea resurselor necesare implementării Sistemului de Management al Securității Informațiilor
- Respectarea cerințelor Sistemului ISMS și îndeplinirea obiectivelor specifice.
- Definirea responsabilităților în materie de securitate a informațiilor pentru persoanele implicate în implementarea și mentenanța sistemului ISMS, precum și sprijinirea și instruirea corectă pentru a-și îndeplini sarcinile specifice.

Rolul organizațional, responsabilitățile și autoritățile

Standardul ISO 27001 prevede că este responsabilitatea managementului să atribuie rolurile și responsabilitățile și să le comunice părților vizate în mod corespunzător. Responsabilitățile vor fi

atribuite astfel încât să se asigure că sistemul ISMS îndeplinește cerințele standardului ISO 27001: 2013, iar performanțele sistemului pot fi monitorizate, evaluate și raportate constant.

Standardul ISO 27001 nu impune organizațiilor să desemneze un o anumită persoană care să coordoneze activitatea referitoare la securitatea informațiilor. Acest aspect nu reprezintă o omisiune în cadrul standardului, fiind o abordare care oferă flexibilitate, astfel încât standardul să fie aplicabil oricărei organizații, indiferent de dimensiune sau de domeniul de activitate.

Responsabilitatea principală a unui ofițer CISO trebuie să fie dezvoltarea unei culturi a securității, bazată pe managementul riscului, întreaga activitate fiind orientată către atenuarea riscului prin măsuri de protecție.

Clauza 6. Planificarea

Clauza face referire la acțiunea preventivă menționată în vechia versiune a standardului, respectiv ISO 27001: 2005. Organizația trebuie să includă în planul de securitate principii și proceduri de gestionare a riscurilor, precum și aspecte relevante referitoare la părțile interesate, pentru a se asigura că sistemul ISMS își poate atinge scopul urmărit: prevenirea, atenuarea și îmbunătățirea continuă.

Procedurile trebuie să fie în deplină concordanță cu obiectivele sistemului ISMS, iar eficacitatea acestora trebuie să fie măsurată.

Evaluarea riscului de securitate a informațiilor

În cadrul organizației este necesar să fie implementat un proces de evaluare a riscului de securitate a informațiilor, care va cuprinde definiții ale riscurilor, criterii de acceptare a riscurilor, precum și criterii pe baza cărora se vor efectua evaluările.

Procesul de evaluare a riscurilor trebuie să fie cuprins într-un document livrabil și trebuie să conțină informații referitoare la identificarea, analiza și evaluarea riscurilor.

Evaluarea riscurilor reprezintă o etapă complexă a procesului de implementare a standardului ISO 27001. Pentru eficiența procesului de implementare, este important să se parcurgă corect această etapă în cadrul căreia se va redacta un document livrabil - Metodologia de evaluare a riscurilor. Importanța documentului este întărită chiar de rezultatele incerte pe care le poate genera demararea procesului de evaluare în lipsa unei metodologii clare.

Identificarea riscului – Prin revizuirea din 2013 a standardului ISO 27001, a fost eliminată procedura prevăzută în ISO 27001Ș 2005, astfel că riscurile se pot identifica în baza unor proceduri interne ale organizației, prin raportarea activelor la vulnerabilitățile, amenințările, riscurile și pericolele potențiale.

Revizuirea din 2013 a eliminat totodată obligativitatea efectuării unei evaluări a riscurilor bazată pe active, aceasta putând fi realizată pe baza unor proceduri interne, simplificate. Cu toate acestea

evaluarea riscurilor pe baza activelor va continua să fie metoda cea mai utilizată pentru evaluarea riscului, deoarece conturarea unor proceduri proprii ar putea complica procesul în sine. Cea mai simplă metodă de a realiza evaluarea riscurilor pe baza activelor este aplicarea controalelor A.8.1.1 (identificarea activelor) și A.8.1.2 (atribuirea proprietarilor de active).

În concluzie, metodologia de evaluare a riscurilor trebuie adaptată la circumstanțele și la nevoile de securitate ale fiecărei organizații în parte. Utilizarea unei metodologii predefinite, care poate fi complet inadecvată pentru organizație, poate compromite întregul proces de evaluare și implicit implementarea standardului.

Tratarea riscului de securitate a informațiilor

Organizația trebuie să definească și să implementeze un proces de tratare a riscului de securitate a informațiilor, prin care să definească procesele și controalele adecvate. Controalele aplicabile sunt cele enumerate în Anexa A a standardului.

Procesul de tratare a riscurilor se realizează sub forma unui document livrabil. În urma procesului, se elaborează Declarația de aplicabilitate (SoA) și Planul de tratare a riscurilor.

Evaluarea riscurilor reprezintă o etapă complexă a implementării standardului ISO 27001, deoarece este procesul care pune bazele securității informațiilor în organizație.

Importanța acestui proces rezultă chiar din concepția standardului ISO 27001, care urmărește să identifice incidentele care ar putea apărea, precum și cele mai potrivite modalități le trata. Totodată, procesul urmărește o ierarhizare a riscurilor, astfel încât să se acorde importanță sporită celor care sunt mai accentuate.

Declarația de aplicabilitate SoA (Clauza 6.1.3) are o importanță deosebită pentru sistemul ISMS definind modul în care organizația va aborda securitatea informațiilor. Declarația reprezintă principala legătură dintre evaluarea și tratamentul riscurilor și implementarea proceselor de securitate definind care din cele 114 controale prevăzute în Anexa A a standardului vor fi aplicate, precum și modul de implementare.

Obiectivele de securitate a informațiilor și planurile de realizare a acestora

Clauza vizează obiectivele de securitate a informațiilor și definește proprietățile pe care respectivele obiective trebuie să le dețină. În conținutul clauzei se regăsește sintagma *funcții și niveluri relevante*, prin aceasta făcându-se referire la funcțiile organizației și la nivelurile de management.

Obiectivele asumate de organizație trebuie să fie comunicate tuturor părților implicate în gestionarea sistemului ISMS, precum și părților vizate și trebuie să fie actualizate ori de câte ori este necesar.

Standardul ISO 27001 necesită definirea a două niveluri diferite de obiective de securitate:

1. Obiective generale, raportate la întregul sistem ISMS
2. Obiective sectoriale, raportate la fiecare control de securitate.

În funcție de mărimea organizației, pot fi definite și obiective la niveluri intermediare (spre exemplu, la nivelul fiecărui departament intern)

Clauza 7. Sprijin

Disponibilitatea resurselor reprezintă o condiție *Sine qua non* pentru implementarea sistemului se management al securității informațiilor.

Conținutul clauzei 7.1 nu este deosebit de cuprinzător, făcând referire doar la necesitatea disponibilității unui nivel adecvat al resurselor. Cu toate acestea, cerințe referitoare la resursel sunt răspândite în întregul standard.

În ceea ce privește resursele, clauza 7.1 din prevede necesitatea de a fi definite și alocate resursele necesare pentru ciclul de viață al sistemului ISMS: de la implementare, la îmbunătățirea continuă.

Competența

Calificarea indivizilor cărora li se atribuie responsabilități în cadrul sistemului ISMS trebuie să respecte termenii standardului ISO 27001: 2013.

Competența presupune experiență și formare profesională în domeniu. Organizația trebuie să asigure accesul la formare și să evalueze periodic personalul, pentru a se asigura că dispune de resursă umană calificată.

Conștientizarea

Personalul organizației trebuie să conștientizeze importanța politicii de securitate a informațiilor și conținutul acesteia, să înțeleagă rolurile și responsabilitățile în cadrul sistemului ISMS, precum și consecințele eventualelor neconformități.

Conștientizarea este strâns legată de modul în care managementul organizației face diseminarea informațiilor relevante, referitoare la sistemul ISMS.

Comunicarea

Clauza vizează atât comunicarea internă, în cadrul organizației, cât și comunicarea cu terții și presupune identificarea mijloacelor și a mesajelor relevante pentru sistemul ISMS, luând în considerare conținutul comunicării, momentul comunicării și destinatarii mesajelor.

Comunicarea este o activitate esențială în orice organizație, având o importanță însemnată în gestionarea securității. O comunicarea eficientă în ceea ce privește conținutul și modalitatea de

transmitere poate consolida încrederea personalului și a terților în organizație. Standardul ISO 27001 abordează problema comunicării de trei ori.

Planul de comunicare reprezintă un instrument care contribuie activ la dezvoltarea capacității de răspuns la incidentele de securitate și la capacitatea de reziliență a organizației. Planul reprezintă un element central al unui sistem de management centrat pe provocările societății informaționale.

Informații documentate

Sintagma *Informații documentate* face referire atât la documente livrabile, cât și la înregistrările stabilite de organizație ca fiind necesare pentru eficiența sistemului de management al securității informațiilor. Clauza are ca scop facilitarea gestionării documentelor și înregistrărilor prevăzute de standard, precum și a celor considerate critice de către management.

Standardul ISO 27001: 2013 cuprinde atât documente livrabile obligatorii, cât și facultative pentru funcționarea ISMS. Referiri la documentele livrabile se regăsesc atât în clauze, cât și în conținutul controalelor din Anexa A. Documentele din anexă sunt obligatorii doar în măsura în care există riscuri care ar necesita implementarea acestora.

Crearea și actualizarea

O cerință esențială a standardului vizează identificarea și descrierea tuturor informațiilor documentate, precum și revizuite și actualizate.

Toate aceste operațiuni se vor realiza prin raportarea informațiilor la scopul sistemului ISMS.

Controlul informațiilor documentate

Standardul prevede obligativitatea de a se asigura disponibilitatea tuturor informațiilor documentate, acestea urmând a fi protejate împotriva daunelor sau pierderii integrității. Pentru asigurarea unui management eficient al informațiilor documentate, organizația va implementa proceduri adecvate privind accesul, utilizarea, prelucrarea, recuperarea și stocarea acestora.

Standardul ISO 27001 definește modul în care trebuie gestionate informațiile documentate (în special documentele livrabile), instituind totodată obligația de implementare a unei proceduri de gestionare, sub forma unui document livrabil distinct. Documentul este esențial pentru certificarea conformității.

Informațiile documentate pe care trebuie să gestioneze organizația provin atât din surse interne, cât și externe (spre exemplu, corespondența) și pot fi disponibile atât pe suport printat, cât și în format electronic, făcând ca procesul de gestionare să fie unul complex, care implică mai multe departamente.

În cadrul procesului de certificare a conformității, auditorul va urmări modul în care gestionarea informațiilor documentate respectă procedura stabilită la nivelul organizației.

În practică, procesul de certificare a conformității ISO 27001 determină organizațiile să îmbunătățească sistemul de gestionare și arhivare, evidențiind totodată importanța organizării registrelor.

Clauza 8. Operarea

Planificarea și controlul operațional

Clauza 8.1 face referire executarea proceselor care fac obiectul unor clauze anterioare, urmărind funcționarea sistemului ISMS prin integrarea politicilor de securitate, a procedurilor și a controalelor în activitatea de zi cu zi a organizației.

Standardul ISO 27001 reglementează tratarea riscurilor și oportunităților (clauza 6.1), pentru îndeplinirea obiectivelor de securitate (clauza 6.2). Astfel, Sistemul de Management al Securității Informațiilor trebuie să proiecteze, să implementeze și să controleze procesele interne și externe pentru a-și atinge scopul.

Evaluarea riscului de securitate a informațiilor

Standardul prevede obligativitatea efectuării evaluărilor periodice ale riscurilor, în conformitate cu criteriile clauzei 6.1.2 (a), iar rezultatele evaluării trebuie să fie stocate ca informații documentate.

Evaluarea riscurilor, în contextul standardului ISO 27001: 2013, presupune asocierea activelor cu riscurile și vulnerabilitățile potențiale. Mijloacele de identificare a riscurilor rămân la latitudinea organizației.

Pornind de la active, se vor identifica riscurile potențiale, iar pentru fiecare risc, vulnerabilitățile existente. Procesul de evaluare a riscurilor presupune identificarea problemelor potențiale, înainte ca acestea să intervină și promovează conduita preventivă, în detrimentul tratării.

Tratarea riscului de securitate a informațiilor

Standardul prevede, de asemenea, obligativitatea implementării unui Plan de tratare a riscurilor, rezultatele acestuia urmând a fi păstrate sub forma de informații documentate.

Planul de tratare a riscurilor este unul din documentele fundamentale pentru standardul ISO 27001, care însă este confundat, de multe ori, cu documentația care rezultă în urma desfășurării a unui proces de tratare a riscurilor.

Procesul de tratare a riscurilor reprezintă o etapă a procesului de gestionare a riscurilor, care urmează după faza de evaluare a riscului.

În contextul standardului ISO 27001, se vor documenta rezultatele procesului de tratare a riscului în Raportul de evaluare a riscurilor, rezultatele fiind principalele înregistrări folosite pentru redactarea Declarației de aplicabilitate SoA. Astfel, rezultatele procesului de abordare a riscurilor nu sunt

documentate direct în Planul de tratare al riscului, care poate fi întocmit numai ulterior Declarației de aplicabilitate.

Planul de tratare a riscurilor va cuprinde, în mod obligatoriu, o descriere a tuturor controalelor utilizate, responsabilii cu implementarea acestora, resursele alocate, precum și termenele de realizare. Alegerea controalelor de securitate se face, însă, prin Declarația SoA.

O evaluare corectă a riscurilor, precum și o Declarație de aplicabilitate cuprinzătoare și bine documentată vor genera un Plan de tratare eficient pentru implementarea Sistemului de Management al Securității Informațiilor.

Clauza 9. Evaluarea performanței

Monitorizarea, măsurarea, analiza și evaluarea

Organizația nu numai că trebuie să stabilească și să evalueze metricile de performanță cu privire la eficacitatea și eficiența proceselor, procedurilor și funcțiilor care protejează informațiile, dar trebuie să ia în considerare și valori pentru performanța ISMS, în ceea ce privește respectarea standardelor, acțiuni preventive ca răspuns la tendințele adverse , gradul în care se realizează politica de securitate a informațiilor, obiectivele și obiectivele.

Auditul intern

Auditurile interne trebuie efectuate la intervale planificate, luând în considerare relevanța proceselor și rezultatele auditurilor anterioare, pentru a asigura implementarea și întreținerea efectivă, precum și respectarea cerințelor standardului și a oricăror cerințe definite de organizație. Criteriile și domeniul de aplicare al fiecărui audit trebuie să fie definite. Auditorii trebuie să fie independenți și să nu aibă conflict de interese în ceea ce privește subiectul auditului.

Revizuirea efectuată de management

Clauza 9.3 cuprinde cerințe privind subiectele care trebuie examinate în timpul revizuirii. Revizuirile se desfășoară la intervale planificate, acoperind toate aspectele relevante, simultan sau etapizat. A fost eliminat termenul de un an prevăzut în versiunea precedentă a standardului. Revizuirea are rolul de a menține Sistemul de Management al Securității Informațiilor la un nivel adecvat de eficiență.

Scopul clauzei 9.3 este de a determina managementul organizației să se reunească periodic pentru a lua decizii cu un impact major asupra sistemului ISMS, într-un mod sistematic. Spre exemplu, managementul poate decide sporirea bugetului destinat asigurării securității informațiilor, sau adaptarea infrastructurii la cerințele specifice.

Clauza 10. Îmbunătățirea

Neconformitate și acțiuni corective

Clauza cuprinde o serie de cerințe care au rolul de a urmări controlul și corectarea neconformităților, pentru a face față consecințelor, precum și de a determina dacă există sau ar putea să apară neconformități similare.

Revizuirea din 2013 a standardului a introdus o nouă cerință pentru a se asigura că acțiunile corective sunt adecvate efectelor neconformităților întâlnite. Cerința de îmbunătățire continuă a fost extinsă pentru a acoperi eficiența Sistemului de Management al Securității Informațiilor, fără a fi specificate modalitățile în care o organizație trebuie să acționeze în această direcție.

Rezultatele revizuirilor efectuate de managementul organizației, ale auditurilor interne și ale evaluării performanțelor sistemului ISMS trebuie să fie folosite pentru a identifica neconformitățile și acțiunile corective ce se impun.

Îmbunătățirea continuă

Îmbunătățirea continuă este un aspect-cheie al ISMS în efortul de a realiza și menține adecvarea, adecvarea și eficacitatea securității informațiilor, în corelație cu obiectivele organizațiilor.

Realizarea îmbunătățirii continue prin utilizarea modelelor de maturitate.

Ca orice alt sistem de management ISO, ISO 27001 are o cerință de îmbunătățire continuă (clauza 10.2). Acest lucru se întâmplă deoarece nici un proces, indiferent cât de bine stabilit și implementat, care respectă standardele ISO sau nu, poate menține niveluri ridicate de performanță fără a face în mod constant ajustări pentru a se adapta schimbărilor scenariului.

Analiza Anexei A - Obiective și controale de control de referință

Anexa A cuprinde controalele de securitate aplicabile, acestea fiind numerotate de la A.5 la A.18. Numerotarea creează o relație directă cu controalele enumerate în standardul ISO 27002, referitor la bunele practici din domeniul securității informațiilor.

A.5 Politica de securitate a informațiilor

Controalele din această secțiune urmăresc să ofere direcții generale pentru Sistemul de Management al Securității Informațiilor în ceea ce privește implementarea, comunicarea și revizuirea politicilor de securitate a informațiilor.

A.6 Organizarea securității informațiilor

Controalele din secțiunea A.6 vizează asigurarea cadrului de bază pentru implementarea și funcționarea securității informațiilor prin introducerea unor cerințe minimale în ceea ce privește organizarea internă și prin luarea în considerare a aspectelor organizaționale ale securității informațiilor.

A.7. Securitatea resurselor umane

Controalele din această secțiune urmăresc să asigure că persoanele care activează în cadrul organizației și care pot afecta securitatea informațiilor, sunt apte să lucreze și își cunosc responsabilitățile și că orice modificare a politicii de resurse umane nu va afecta securitatea informațiilor.

A.8. Managementul activelor

Controalele din această secțiune urmăresc să asigure identificarea, în cadrul organizației, a activelor relevante pentru securitatea informațiilor, precum și stabilirea unor responsabilități specifice pentru personalul implicat în gestionarea respectivelor active.

A.9. Controlul accesului

Standardul ISO 27001 definește conceptul de control al accesului în secțiunea A.9 din Anexa A, unde se regăsesc nu mai puțin de14 controale, numărul ridicat al acestora demonstrând importanța acestor proceduri.

Controalele A.9 urmăresc să asigure limitarea accesului la informații, prin procese documentate de acordare sau revocare a drepturilor de acces.

A.10. Criptografie

În contextul societății informaționale, schimburile de date au devenit o parte a realității cotidiene. Informațiile sunt transformate prin mijloacele de comunicație, prin suporturi media sau în cadrul rețelelor, fiind în tot acest timp accesate de persoane din afara organizației, care pot urmări un scop ilegitim. Pentru prevenirea accesului neautorizat, este necesară criptarea informațiilor.

Controalele A.10 au ca scop furnizarea unor soluții pentru utilizarea corectă a soluțiilor criptografice pentru a proteja confidențialitatea, autenticitatea și integritatea informațiilor.

A.11. Securitatea fizică și de mediu

Controalele din această secțiune urmăresc să asigure prevenirea accesului neautorizat la infrastructura fizică a organizației. Standardul ISO 27001: 2013 tratează securitatea fizică și de mediu prin intermediul a controale, grupate în două secțiuni: Zonele de securitate și Echipamente.

Protecția fizică a perimetrului este o componentă esențială pentru întregul concept de securitate. În cadrul Sistemului de Management al Securității Informațiilor, securizarea incintei vizează o serie de măsuri menite să minimalizeze potențialul de dezastru sau costul contra-măsurilor de protecție.

Securitatea fizică joacă un rol esențial în protecția informațiilor, deoarece chiar și cele mai bine concepute, implementate și întreținute controale tehnice și administrative, fie legate de IT, fie din alte domenii, au puțin ajutor dacă un eveniment afectează fizic mediul sau bunurile pe care aceste controale funcționează.

A.12. Securitatea operațiunilor

Controalele din această secțiune urmăresc să se asigure că funcționarea facilităților de procesare a informațiilor, inclusiv a sistemelor de operare, este securizată și protejată împotriva malware-ului și a pierderii datelor.

În plus, controalele din această secțiune necesită mijloacele de înregistrare a evenimentelor și de generare a dovezilor, verificarea periodică a vulnerabilităților și stabilirea unor măsuri de precauție pentru a împiedica activitățile de audit să afecteze operațiunile.

A.12.1 Proceduri și responsabilități operaționale

A.12.1.1 Proceduri de operare documentate

A.13. Securitatea comunicațiilor

Comenzile din această secțiune urmăresc să protejeze infrastructura și serviciile de rețea, precum și informațiile care călătoresc pe ele.

Pe măsură ce tot mai mulți oameni și organizații devin interconectate, se schimbă din ce în ce mai multe informații, de la cele considerate triviale la cele mai sensibile și necesare vieții oamenilor și supraviețuirea afacerilor.

Putem defini managementul securității rețelelor ca proces menit să protejeze o rețea și datele care circulă prin ea de riscuri cum ar fi accesul neautorizat, utilizarea incorectă, funcționarea defectuoasă, modificarea, distrugerea sau divulgarea necorespunzătoare, permițând în același timp computerelor, utilizatorilor și aplicațiilor autorizate să efectueze activitățile lor.

Trebuie implementat un set de controale generale, cum ar fi definirea responsabilităților și procedurilor pentru gestionarea echipamentelor de rețea, segregarea sarcinilor între rețele și activitățile computerelor, utilizarea soluțiilor criptografice pentru protejarea datelor în tranzit și interconectarea.

A.14. Achiziționarea, dezvoltarea și întreținerea sistemului

Clauza de achiziție, dezvoltare și întreținere a sistemului acoperă controale pentru identificarea, analiza și specificarea cerințelor de securitate a informațiilor, asigurarea serviciilor de aplicații în procesele de dezvoltare și asistență, restricții de revizuire tehnică a modificărilor pachetelor de software, principii de inginerie sigure a sistemului, mediu de dezvoltare sigur, dezvoltare subcontractată , testarea securității sistemului, testarea acceptării sistemului și protecția datelor de testare. Acesta poate fi gândit ca un control care nu numai că guvernează procesele de achiziții pentru sisteme noi, dar care stabilește, de asemenea, criterii pentru sisteme noi care pot fi testate înainte de utilizare.

A.15. Securitatea informațiilor în relațiile cu furnizorii

Controalele din această secțiune urmăresc să se asigure că activitățile externalizate efectuate de furnizori iau în considerare și controalele de securitate a informațiilor și că acestea sunt gestionate corespunzător de către organizație.

Dat fiind că din ce în ce mai multe date sunt procesate și stocate cu terțe părți, protecția acestor date devine o problemă din ce în ce mai importantă pentru profesioniștii în domeniul securității informațiilor, iar noua revizuire 2013 a ISO 27001 a dedicat o întreagă secțiune a anexei A această problemă.

A.16. Managementul incidentelor privind securitatea informațiilor

Complexitatea software, conectivitatea la nivel mondial și infractorii hotărâți să profite de acești factori fac ca incidentele de securitate a informațiilor să fie inevitabile. Obiectivul unei strategii eficiente de gestionare a incidentelor de securitate a informațiilor este un echilibru de reducere a impactului incidentelor, în timp ce procesarea incidentelor este cât mai eficientă. O bună gestionare a incidentelor va ajuta, de asemenea, la prevenirea incidentelor viitoare. Din perspectiva managementului, aceasta implică identificarea resurselor necesare pentru gestionarea incidentelor, precum și dezvoltarea și comunicarea proceselor formale de detectare și raportare. Un program de securitate eficient include aspecte importante ale detectării, raportării și răspunsului la evenimente adverse de securitate, precum și puncte slabe care pot duce la evenimente, dacă acestea nu sunt abordate în mod adecvat.

A.17. Aspectele privind securitatea informațiilor în managementul continuității afacerii

Având în vedere că nu toate evenimentele pot fi prevenite și că unele riscuri pot fi considerate acceptabile, planificarea corespunzătoare este esențială pentru întreținerea sau restaurarea serviciilor atunci când un eveniment neașteptat sau inevitabil perturbă activitatea normală a organizației. Planificarea continuității afacerii include identificarea vulnerabilităților, priorităților, dependențelor și măsurilor pentru elaborarea de planuri care să faciliteze continuitatea și recuperarea înainte, în timpul și după evenimentul perturbator. Planurile cuprinzătoare de continuitate de afaceri sunt concepute și puse în aplicare pentru a asigura continuitatea operațiunilor în condiții anormale. Planurile promovează disponibilitatea organizațiilor pentru recuperarea rapidă în fața evenimentelor sau a condițiilor adverse, minimizează impactul unor astfel de circumstanțe și oferă mijloace care să faciliteze funcționarea în

timpul și după situații de urgență. Planurile se bazează pe o evaluare a riscurilor și o analiză a impactului asupra afacerilor curente și includ un proces de întreținere regulată.

A.18. Conformitatea

Organizațiile sunt supuse numeroase legi, reglementări și obligații contractuale care specifică cerințe legate de gestionarea corespunzătoare și protecția diverselor seturi de informații. Înțelegerea și menținerea respectării acestor cerințe diferite este uneori dificilă. Calea către stabilirea conformității aruncă o privire completă asupra domeniilor în care Organizația are responsabilități, fie ele legale, de reglementare, contractuale sau auto-impuse.

Concluzii

ISO 27001: 2013 furnizează organizațiilor îndrumări cu privire la modul de gestionare a riscurilor legate de securitatea informațiilor, cu scopul final de a păstra confidențialitatea, integritatea și disponibilitatea informațiilor prin aplicarea unui proces de gestionare a riscurilor și de a da încredere părților interesate că riscurile sunt gestionate în mod adecvat. Și, prin implementarea tuturor clauzelor standardului și înțelegerea cu adevărat a impactului acestora, organizația dvs. poate obține multe alte beneficii.

Certificarea și conformitatea pot aduce beneficii reputaționale, motivaționale și financiare organizației dvs. prin intermediul clienților care au mai multă încredere că puteți să vă protejați informațiile la niveluri de securitate convenite, împreună cu îmbunătățiri ale securității lanțului dvs. de aprovizionare. Toate aceste elemente sunt strâns legate de capacitatea organizației dvs. de a satisface clienții dvs. și de a îndeplini așteptările și dorințele părților interesate, protejând în același timp capacitatea organizației de a face afaceri pe termen lung. Având în vedere toate acestea, organizația dvs. vă poate permite să nu aveți standardul ISO 27001: 2013?

CAPITOLUL 4. CORELAREA STANDARDULUI CU GDPR

Domeniul de aplicabilitate al Regulamentului GDPR își găsește corespondența în controlul A.18.1.4 Confidențialitatea și protecția informațiilor de identificare personală.

Hassan Mokalled, Daniele Debertol, Ermete Meda, Concetta Pragliola[1], în lucrarea *Importanța gestionării protecției datelor în mod corect: probleme și soluții*, arată că toate activitățile desfășurate de o organizație pentru obținerea conformității în domeniul protecției datelor, implică analize de reglementare pentru a asigura conformitatea cu legile aplicabile la nivel mondial și local. Conformitatea poate fi orientată spre politicile și regulile interne sau către legile și reglementările externe, dar, în orice caz, reprezintă un pas fundamental pentru menținerea controlului organizației în interiorul mediului de reglementare specific. În acest context, conformitatea se va raporta la toată legislația națională și internațională în materie de confidențialitate și cu standardele internaționale de securitate a informațiilor, cum ar fi ISO / IEC 27001, GDPR, sau alte bune practici / reglementări echivalente cerute de întreprindere.

Ed Conley și Matthias Poch[2], în lucrarea *Condițiile de conformitate cu GDPR pentru schimburile de informații interoperabile privind sănătatea și mediile de cercetare de încredere*, arată că, într-un Mediu de cercetare de încredere accesul legitim al cercetătorilor la colecțiile de date și invocarea serviciilor analitice permise este controlat prin aplicații informatice, iar acest mijloc de protecție se realizează în conformitate cu standardele ISO 27001: 2013; aceste procese de conformitate reprezintă chestiune de îmbunătățire continuă, vigilență și conștientizare organizațională. Furnizarea de date furnizează, de asemenea, infrastructură de fluxuri de lucru care permite producerea de conducte de date, care automatizează transformarea extraselor și pregătirea setului de date, dar și utilizarea datelor pentru realizarea unor studii, cu respectarea prevederilor GDPR.

Lauri Tammelin[3] În lucrarea *Auditul sistemului de management al securității informațiilor*, arată că numeroase companii au un plan de management al calității și un plan general de protecție a datelor conceput să îndeplinească cerințele standardelor ISO 27001 și ISO 27002. În plus, planul ia în considerare Regulamentul UE privind protecția datelor (GDPR) și sistemul de management al calității ISO 9001.

[1] Hassan MokalledDaniele DebertolErmete MedaConcetta Pragliola, The Importance to Manage Data Protection in the Right Way: Problems and Solutions, în volumul Optimization and Decision Science: Methodologies and Applications pp 69-82, 2017

[2] Conley E., Pocs M. - GDPR Compliance Challenges for Interoperable Health Information Exchanges (HIEs) and Trustworthy Research Environments (TREs), în European Journal for Biomedical Informatics, Volume 14 (2018), Issue 3

[3] Lauri Tammelin - Tietoturvallisuuden hallintajärjestelmän auditointi, Metropolia Ammattikorkeakoulu, 2018

Bartolini, C., Gheorghe, G., Giurgiu. A, Sabetzadeh, M., Sannier, N.[4] , în lucrarea *Evaluarea standardelor de securitate IT în contextul GDPR pentru sistemele Cloud* au analizat preocupările legate de securitate pentru sistemele informatice, și au recomandat implementarea familiei de standarde ISO / IEC 27000, care oferă un cadru care să se ocupe de concepte precum politica de securitate și obiectivele, definițiile și evaluarea riscurilor, angajamentul de evaluare continuă și documentare.

Autorii au subliniat importanța analizării standardului ISO 27001 și a Regulamentului GDPR, cu scopul de a se creiona o cartografiere a conceptelor exprimate de fiecare dintre documente.

O astfel de analiză poate fi utilizată ca punct de pornire pentru definirea criteriilor de respectare a GDPR. În absența unor reguli și constrângeri clare, identificarea standardelor de securitate care pot fi aplicate protecției datelor pentru a reduce decalajul dintre practicile actuale și cerințele legale viitoare poate spori încrederea DS și poate oferi avantaje competitive. De asemenea, poate facilita trecerea la o nouă abordare consolidată a protecției datelor cu caracter personal.

Pornind de la interpretarea clauzelor și a controalelor din standardul ISO 27001: 2013, în prezentul capitol s-a urmărit realizarea unei cartografieri a standardului cu prevederile Regulamentului GDPR.

Datorită domeniului de aplicare, conformitatea cu prevederile Regulamentului GDPR nu duce automat la îndeplinirea cerințelor descrise în clauzele și controalele din conținutul standardului ISO 27001. Cu toate acestea, o corelare a celor două documente prezintă relevanță pentru majoritatea organizațiilor Europene.

Articol GDPT	Corespondent ISO 27001
1	A.18.1.4
2	
3	A.18.1.4
4	3
5	6.1.2,A.8.1.1,A.8.2,A.8.3, A.9.1.1,A.9.4.1, A.10,A.13.2, A.14.1.1,A.15,A.17,A.18
6	6.1.2,A.14.1.1,A.18.1.1
7	A.8.2.3, A.12.1.1, A.13.2.4, A.18.1.3, 6.1.2, A.14.1.1, A.8.3.2, A.13.2
8	A.8.2.3, A.12.1.1, A.13.2.4, A.18.1.3, 6.1.2, A.14.1.1, A.8.3.2, A.13.2
9	A.8.2.1, A.8.2.3, A.14.1.1

[4] Bartolini, C., Gheorghe, G., Giurgiu. A, Sabetzadeh, M., Sannier, N. Assessing IT Security Standards Against the Upcoming GDPR for Cloud Systems. In: Proceedings of the Grande Region Security and Reliability Day (GRSRD 2015), pp. 40-42, March 2015.

10	A.7.1, A.8.2.1, A.8.2.3, 6.1.2, A.14.1.1, A.7.1
11	A.8.2.1, A.8.2.3, 6.1.2, A.14.1.1
12	A.12.1.1 A.14.1.1 A.16
13	A.8.2., A.8.2.3, A.12.1.1, A.14.1.1, A.16
14	A.8.2.1, A.8.2.3, A.12.1.1, A.14.1, A.16
15	A.8.1.1, A.8.2.1, A.12.1.1, A.13.2.1, A.14.1.1
16	A.12.1.1, A.14.1, A.9, A.16, A.12.3, A.18.1.3
17	6.1.2, A.14.1.1, A.9, A.16, A.12.3, A.8.3.2
18	6.1.2, A.8.2.1, A.8.2.3, A.12.1.1, A.14.1.1, A.16, A.12.3, A.18.1.1
19	A.12.1.1, 6.1.2, A.14.1.1, A.16
20	6.1.2, A.13, A.14.1.1, A.8.3, A.10, A.18.1.3
21	6.1.2, A.12.1.1, A.14.1.1, A.16, A.12.3
22	6.1.2, A.12.1.1, A.14.1.1, A.16
23	A.18.1.1
24	4-10
25	6, Anexa A
26	5.3 9.1 A.13.2 A.15 A.16 A.18.1
27	5.3, 7.5.1, A.15, A.18.1.4
28	8.2, 9.1, A.15, A.18.1.1, A.18.1.3, A.18.1.4
29	Anexa A
30	7.5
31	A.6.1.3
32	8.2, 8.3
33	A.16, A.18.1.4
34	A.16, A.18.1.4
35	6.1.2, A.6.1.3, A.8.2.1
36	6.1.2, A.6.1.3, A.8.2.1
37	5.3, A.6.1.1, A.18.1.4
38	
39	
40	
41	
42	
43	
44	-

45	A.18.1.4
46	
47	
48	A.18.1.4, A.16
49	A.18.1.4
50 - 81	-
82	A.18.1.4
83	6, A.18.1.4
84	
85	6, A.18.1.1, A.18.1.4
86	
87	
88	
89	
90	
91	A.18.1.4
92	A.18.1.1
93	
94	
95	
96	
97	
98	
99	

CAPITOLUL 5. Utilizarea analizelor GAP PENTRU ISO 27001 și GDPR

V.1. Analiza GAP pentru sisteme de management și de securitate informațională

Sistemele de management reprezintă un element-cheie în cadrul unei organizații, permițând organizației să atingă un succes sustenabil. Este o maturitate a sistemului de management pentru care este important succesul competitiv al organizației cu produsele, procesele și dezvoltarea culturii de calitate, prin utilizarea cunoștințelor și a experienței.

Standardele de management oferă organizațiilor un set de cerințe și principii, urmând ca organizația să poată atinge efectul dorit de îmbunătățire continuă și succes durabil. Efectul deplin al aplicării standardelor de management al calității și securității informației poate fi văzut doar printr-o implementare capabilă să utilizeze acest potențial. Sistemul de audit intern și extern reprezintă un instrument de bază pentru a determina gradul de conformare al sistemului de management al organizației cu criterii stabilite și care dezvăluie potențialul de îmbunătățire. În practică, auditurile interne se concentrează mai mult pe realizarea specifică a cerințelor standardelor sistemului de management prin obținerea de probe, mai degrabă decât pe evaluarea implementării și eficacității sistemului de management relevant și pe explorarea oportunităților de îmbunătățire continuă [88]. Verificările inconsecvente pot exacerba doar lacunele care rezultă din implementarea superficială a sistemului de management. Acest lucru poate contribui la apariția unor îndoieli cu privire la beneficiile unui standard al sistemului de management al calității și securității informației pentru o organizație [94]. Potrivit unui studiu, managerii a 35% din organizațiile care dețin certificate de sistem de management exprimă o anumită dezamăgire rezultată din așteptările și beneficiile nerealizate ale aplicației standardelor respective [78]. În același timp, conducerea organizației nu a specificat în mod clar, în cadrul scopului și obiectivelor sale, beneficiile așteptate din implementarea sistemului de management în avans (cu excepția așteptării obținerii certificatului).

Implementarea sistemului de management pentru securitatea informației și certificarea ISO 27001 a companiei demonstrează angajamentul pentru protecția datelor procesate, continuitatea activităților (business continuity) și respectarea legislației naționale și internaționale în domeniu.

Standarde SMSI pe lângă beneficii au potențiale probleme. În general, recomandările sunt elaborate utilizând modele generice sau universale, care nu pot fi aplicabile pentru toate organizațiile. Recomandările bazate pe metode tradiționale general acceptate iau în considerare diferențele dintre organizații și cerințele specifice de securitate ale organizației [101].

Auditul servește pentru examinarea potrivirii unei abordări a implementării sistemului de management. Standardul ISO 19011 prezintă o orientare pentru sistemele de management de audit, dar nu specifică în mod explicit nici o abordare a evaluării procesului de implementare în sine [78]. Una dintre abordările

adecvate este oferită de analiza GAP, care are ca scop, în general, evaluarea retrospectivă a proceselor și a interacțiunilor dintre procese. O utilizare adecvată a analizei GAP ar trebui să ducă la dezvăluirea potențialului de îmbunătățire, care este prezent în procese și interfața acestora, iar scopul său este de a umple lacunele identificate prin măsuri rezonabile [82].

Analiza GAP (*Gap Analysis* – denumita și analiza lipsurilor, analiza lacunelor sau a decalajelor) reprezintă o evaluare a conformității față de o serie de cerințe ale standardului. Aceasta analiză se desfășoară, de obicei, în cadrul unui audit intern sau extern al practicilor de afaceri ale companiei sau organizației. Auditorii clasifică lacunele în abateri majore sau minore. Abaterile majore trebuie tratate și rezolvate înainte ca o companie sau organizație să poată primi certificarea.

Folosirea analizei GAP ca mijloc de legătură dintre proces și evaluarea conformității, precum și de pregătire a conformității a fost studiată în lucrarea *Measuring readiness for compliance: a gap analysis tool to complete the TIPA process assessment framework* [92].

Conceptul de analiză GAP, precum și poziționarea sa în raport cu o evaluare a procesului în contextul evaluării conformității trebuie clarificat. În lumea afacerilor, o analiză a decalajelor permite unei organizații să măsoare modul în care aceasta se comportă în raport cu potențialul său [72].

Analiza GAP este un instrument sau o tehnică care permite unei organizații să compare performanța reală cu standardele [83]. Analiza GAP este diferită de evaluarea riscului prin compararea obiectului cu o anumită țintă (care ar putea fi nivelul de performanță sau standardul dorit), în timp ce evaluarea riscului nu este măsurată în raport cu un obiectiv. Atât analiza GAP, cât și evaluarea riscurilor evaluează răspunsul la „unde suntem?", dar în cazul analizei GAP se măsoară încă „unde vrem să fim".

Analiza GAP reprezintă, prin urmare, o diferență între înțelegerea și utilizarea potențialului de implementare a standardului sistemului de management pentru realizarea viziunii și asigurarea unui succes durabil al organizației [78].

Analiza GAP este o activitate care este utilizată pentru a evalua cantitativ starea reală în comparație cu posibilitatea de a obține performanțe optime în contextul securității informațiilor. De asemenea, este necesar să se ia măsuri pentru a avansa mai departe de starea sa actuală la starea sa dorită, viitoare [53]. Analiza GAP ar putea fi utilizată ca bază pentru determinarea cerințelor de investiție, cum ar fi timpul, resursele și costurile pentru stabilirea securității informațiilor. În realizarea analizei diferențelor, managerul de vârf și ofițerul de securitate, ca coordonator, trebuie să fie implicați pentru a obține rezultate valide în procesul de analiză a decalajelor.

Analiza GAP este realizată efectiv datorită unui chestionar structurat, organizat pe teme. Chestionarul abordează întregul set de cerințe și este ierarhizat pentru a fi eficace în timpul evaluării. Acesta este alcătuit din întrebări generale, care oferă o imagine de ansamblu asupra temelor evaluate în fiecare subiect, cărora trebuie să li se răspundă în timpul unei evaluări. Aceste întrebări generale sunt

completetate cu întrebări de precizare, evaluând fiecare cerință elementară în mod individual, dar utilizată numai dacă este necesar (adică dacă răspunsul la întrebarea generală nu satisface evaluatorul). Indiferent de tipul de întrebare, una sau mai multe cerințe elementare sunt legate de fiecare întrebare pentru a asigura trasabilitatea.

V.2. Analiza GAP pentru ISO 27001

Actualmente, ne confruntăm nu doar cu efectele digitalizării, a big data și a Internetului obiectelor, ci și cu cerințele crescânde ale globalizării, reglementării și protecției împotriva amenințărilor cibernetice.

Protejarea informațiilor înseamnă gestionarea riscurilor, la fel cum este gestionat riscul apariției oricărui alt tip de pericol. Cu toate acestea, riscurile legate de securitatea informațiilor sunt prea adesea ignorate sau trecute cu vederea – percepția este că doar corporațiile multinaționale uriașe suferă încălcări ale datelor, iar cu noi nu se va mai întâmpla niciodată. Dar se poate întâmpla cu orice afacere.

Ceea ce oferă ISO 27001 este o metodă cu cele mai bune practici de implementare a unui sistem de management al securității informațiilor (SMSI). Având acest sistem și obținând certificarea ISO se presupune că organizația poate demonstra clienților și partenerilor că este angajată în securitatea informațiilor. Mai mulți marii giganți în diverse sfere de activitate se confruntă cu probleme de securitate a datelor [3]. Astfel, câteva corporații și organizații mari – NHS [76], Wonga [110] și Twitter [98] – au căzut victime unor încălcări grave ale securității. Studiul Guvernului UK privind încălcările securității cibernetice *Cyber Security Breaches Survey* [84] a arătat că 7 din 10 întreprinderi mari au suferit o formă de încălcare sau atac, care au costat, în medie, în jur de 20.000 de lire sterline, iar, în multe cazuri, chiar costuri mult mai mare.

Construirea unui SMSI care să îndeplinească cerințele standardului ISO 27001 este un proiect provocator și, adesea, este dificil să se determine cu ce trebuie să înceapă. O modalitate de a simplifica procesul este de a efectua o analiză a decalajelor ISO 27001, un proces în care starea actuală de conformitate este măsurată în raport cu standardul.

Rezultatul evaluării ne va arăta despre starea actuală de securitate a informațiilor în comparație cu starea preconizată în conformitate cu standardul ISO / IEC 27001. Analiza GAP compară situația existentă, dacă controalele ISO / IEC 27001: 2013 au fost realizate bine, inclusiv politici, proceduri, instrucțiuni de lucru, până la documentație [85]. Înainte de a efectua analiza, în primul rând, evaluarea trebuie făcută prin interviu și observare, folosind direcția de evaluare a listei de conformitate, care este adecvată standardului ISO / IEC 27001: 2013. Analiza GAP trebuie realizată doar o singură dată pentru a obține o listă a activităților specifice necesare conformității [80].

Metodele care sunt utilizate în timpul analizei GAP sunt evaluarea de birou și evaluarea pe teren. O evaluare pe birou presupune colectarea de documente aplicabile, cum ar fi informații scrise, grafice,

electronice și fotografii care deja există, în timp ce evaluarea pe teren observă și examinează implementarea securității informațiilor în domeniu.

Rezultatul ambelor metode de evaluare va fi folosit ca bază pentru determinarea diferenței. Analiza GAP oferă o imagine de ansamblu asupra condițiilor existente, astfel încât managementul să poată lua în considerare eforturile și prioritățile.

Ca finalitate a analizei GAP privind conformitatea ISO 27001 se întocmește un raport de constatări care indică starea de conformitate actuală. În baza acestui raport se elaborează un proiect de plan de management al proiectului care detaliază acțiunile specifice necesare pentru respectarea normelor, în ordinea importanței și cu câmpurile de date alocate pentru datele de buget, resurse și finalizare, pentru a ajuta organizația să gestioneze eforturile pentru programul de conformitate.

V.3. Exemple de utilizare a analizei GAP privind conformitate ISO 27001

Articolul *Gap analysis of approaches to implementation of management systems* [78] prezintă analiza GAP și rezultatele acesteia, care dezvăluie problemele și rezultatele procesului de implementare a sistemului de management al calității. Structura formei introduse a analizei GAP are ca scop retrospectiv completarea diferențelor în ceea ce privește modul în care procesul de implementare a sistemului de management ar fi trebuit să fie realizat pentru a fi legat de viziunea și politicile organizației care se bazează pe propriile cercetări și experiențe ale autorului.

Lucrare *ISO 27001 Gap Analysis - Case Study* (AL-MAYAHI) [52] descrie pașii inițiați pentru dezvoltarea unui sistem de management al securității informațiilor pentru e-guvernarea din Emiratele Arabe Unite. Pentru a atinge acest obiectiv, s-a decis obținerea certificării ISO 27001, care este standardul principal în securitatea informațiilor. Analiza GAP a fost efectuată pe patru organizații selectate din cadrul e-guvernării din EAU pentru a determina conformitatea acestora cu standardele ISO 27001. Autorul menționează că analiza GAP a fost inițial utilizată pentru a identifica punctele slabe ale procedurilor organizațiilor. Totodată, această analiză ar trebui să fie un proces continuu, deoarece organizația trebuie revizuită pentru a actualiza analiza lacunelor. Acest lucru este realizat pentru a asigura protecția pe termen lung împotriva încălcărilor de securitate. S-a constatat că acest proces va ajuta la identificarea punctelor slabe ale sistemului existent și la evidențierea oricăror riscuri asociate pentru e-guvernarea EAU. În această lucrare este prezentat un model de management, tehnic și operațional (Management, Technical and Operationa - OTM). Acest model se focusează și oferă un cadru orientat către structurile și responsabilitățile organizației. Sunt prezentate rezultatele benchmarking-ului bazate pe standardul ISO 27001, precum și metoda care este utilizată pentru măsurarea nivelului de maturitate pentru fiecare domeniu de control al securității.

Rezultatele analizei GAP au arătat că în cadrul unor controale organizațiile au fost în totalitate neconforme standardului ISO 27001. Acest lucru se datorează inexistenței unei politici de securitate

aprobate, precum și faptului că nu sunt puse în aplicare politicile de securitate eficiente în cadrul a două controale. Totodată, restul controalelor au arătat un procent mai ridicat de conformitate, ceea ce se datorează faptului că procedura de securitate internă este pusă în aplicare de o echipă responsabilă pentru fiecare secțiune.

Pa baza analizei GAP autorii au ajuns la concluzia că pregătirea implementării ISO 27001 la întreprinderi este mai bună decât la IMM-uri. În plus, că nivelul de maturitate al politicii de securitate a informațiilor este cel mai înalt nivel atât pentru întreprinderi, cât și pentru IMM-uri. Acest lucru înseamnă că conducerile întreprinderilor și ale IMM-urilor au luat în considerare în mare măsură în politica de securitate a informațiilor.

Ajutorul pentru certificarea IMM-urilor pentru ISO / IEC 27001 este o provocare. În acest context, etapa inițială a unui proiect de implementare SMSI este semnificativă: o analiză GAP care evidențiază starea actuală a întreprinderii în ceea ce privește standardul și, prin urmare, resursele necesare pentru a reuși în acest proiect. Lucrarea *A Gap Analysis Tool for SMEs Targeting ISO/IEC 27001 Compliance* [55] prezintă metodele și lucrările de cercetare efectuate pentru a proiecta, experimenta și îmbunătăți un instrument de analiză GAP orientat către IMM-uri pentru ISO / IEC 27001.

Pentru a implementa acest standard, majoritatea organizațiilor încep prin evaluarea decalajului dintre starea lor actuală și cerințele standardului. Acest pas este esențial pentru a estima resursele necesare și pentru a oferi o imagine de ansamblu asupra a ceea ce ar putea fi refolosit în cadrul sistemului actual. Analiza GAP este adesea complexă. Într-adevăr, standardul este compus din aproximativ 150 de cerințe normative pentru SMSI și peste 100 de controale de securitate. Evident, în contextul unui IMM, evaluarea fiecăruia dintre aceste elemente este ineficientă. Astfel, este necesar să se reducă costul și complexitatea acestui pas esențial.

Scopul studiului a prevăzut definirea un instrument eficient de analiză a decalajelor care să ofere o imagine de ansamblu asupra statutului unei organizații în ceea ce privește standardul și anexele acestuia. Cu acest scop, după ce a fost efectuată o analiză a golurilor, în timpul unui experiment inițial, au fost trase concluzii. În primul rând, nu este necesară trecerea prin fiecare dintre cerințele standardului: unele dintre ele sunt redundante în standard și ar trebui să fie combinate. În al doilea rând, diferitele întrebări implică diferite roluri și responsabilități între IMM-uri și, prin urmare, diferite persoane. Aceste schimbări repetate ale interlocutorului și ale subiectului sunt ineficiente. De exemplu, implicarea și angajamentul de management ar trebui verificate într-un flux simplu și unic, în loc să se evalueze separat diferitele cerințe legate de acest subiect și să se răspândească peste standard. În cele din urmă, mai multe cerințe sunt prea complexe pentru persoanele care nu cunosc securitatea și SMSI. De exemplu, întrebările legate de diferite etape ale managementului riscului nu sunt ușor de înțeles pentru un non-specialist. Prin urmare, este necesar să se furnizeze informații

Rezultatul analizei GAP este un raport detaliat și o declarație de aplicabilitate ISO 27001 privind conformitatea proceselor și controalelor de management al securității informațiilor ale clientului cu standardul ISO 27001. Aceasta include rezultatele evaluării în raport cu modelul de maturitate a capacității, pentru a evalua maturitatea clientului în fiecare din cele 12 zone de interes ISO 27001 (Sistemul de management al securității informațiilor plus cele 11 secțiuni din Anexa A).

V.4. Analiza GAP pentru GDPR

Venirea erei digitale a avut multe beneficii, dar, totodată, trebuie luate în considerare și unele riscuri, inclusiv problemele de confidențialitate care au fost recunoscute ca o posibilă parte negativă a tehnologiei informației. Mai multe, perspectivele privind confidențialitatea informațiilor au fost discutate de-a lungul anilor, cum ar fi aspectele tehnologice, filosofice, psihologice, sociologice și juridice (A. Heravi [77]; H. Smith et al.[102]; R. Clarke [62,63]; F. Bélanger et al. [58]; S. Zeadally ET AL. [61]). Pe măsură ce utilizarea tehnologiei informației este în creștere, mai multe riscuri legate de manipularea datelor cu caracter personal determină necesitatea unei legislații adecvate [62].

Fiecare plan de implementare GDPR trebuie să includă șase etape, printre care evaluarea riscului și efectuarea analizei GAP. Este necesar să fie efectuat inventarul de date și procese și să fie comparat cu cerințele GDPR, asigurându-se că sunt incluși furnizorii și vânzătorii terți. Analizele trebuie să identifice unde sunt lacunele în conformitate, dacă vor exista zone în pericol de neconformitate în viitor, care sunt nevoile cele mai imediate pe care trebuie să le îndeplinească compania pentru a se deplasa spre respectarea GDPR.

Odată ce au fost identificate toate eventualele lacune de conformare cu GDPR, organizația ar trebui să elaboreze o foaie de parcurs care să descrie modificările cerute proceselor și sistemelor pentru a se conforma cerințelor GDPR. Unele dintre aceste modificări pot duce la înăsprirea controalelor existente, în timp ce altele pot necesita dezvoltarea unor noi controale și procese noi.

Analiza GAP pentru GDPR oferă organizației o înțelegere clară a locului în care organizația se află în legătură cu GDPR și ce este necesar pentru a demonstra conformitatea. Analiza diferenței GDPR se bazează pe cele 6 principii ale GDPR și oferă o analiză transparentă a gradului de compatibilitate cu GDPR.

1. *Legalitate, echitate și transparență*: acesta este un principiu esențial, strâns asociat cu drepturile fundamentale ale omului. Datele cu caracter personal trebuie să fie prelucrate „în mod legal, echitabil și transparent față de persoana vizată";
2. *Limitări legate de scop - legal, corect și transparent:* datele personale trebuie să fie colectate în scopuri bine determinate, explicite și legitime, iar prelucrările ulterioare nu trebuie să se abată de la aceste scopuri;

3. *Reducerea la minimum a datelor colectate - adecvate, limitate și relevante*: prin acest principiu operatorii sunt avizați de faptul că orice colectare de date personale trebuie foarte bine analizată înainte de obținerea efectivă a datelor, care trebuie să fie cele mai relevante și strict limitate la ceea ce este absolut necesar pentru scopurile în care sunt prelucrate;
4. *Verificarea corectitudinii datelor și actualizarea acestora:* operatorii trebuie să ia toate măsurile pentru a asigura validitatea datelor, iar cele dovedite inexacte trebuie actualizate rapid sau șterse;
5. *Limitări legate de stocare:* datele trebuie păstrate atâta timp cât sunt necesare pentru prelucrarea asumată. Perioadele mai lungi de stocare sunt excepții asociate cu activități publice de arhivare, cercetare sau statistică;
6. *Integritate și confidențialitate – securitatea datelor:* prelucrarea datelor personale trebuie făcută în cele mai proprii condiții de siguranță, care să includă „protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare" (ex. certificări ISO 27001).

Rezultatele auditului și analiza GAP ajută la identificarea domeniilor principale de risc și la ceea ce trebuie făcut pentru a reduce decalajul de a deveni conform GDPR. Angajatorii ar trebui să ia în considerare, de asemenea, cum să construiască considerații privind confidențialitatea în sistemele de resurse umane încă de la început și în permanență, pentru a contribui la îndeplinirea standardului GDPR privind „confidențialitatea prin design și implicit".

O analiză GAP ar trebui întotdeauna să se bazeze pe o strategie de evaluare a riscurilor și să o compare cu cele mai bune practici din cadrul GDPR și securității IT. GlobalSequr se bazează pe cadrul ISO 27000 și face analiza GAP pentru GDPR [20].

În unele cazuri GlobalSequr combină două analize GAP, iar în altele se concentrează exclusiv pe una din zone.

Control		Sarcini	Relevant DA / NU	Conform DA / NU / P	Cerințe GDPR	Documente livrabile
A.5	**Politici de securitate a informațiilor**					
A.5.1.1	Politici de securitate a informațiilor	Există politici de securitate?				
		Politicile de securitate sunt aprobate de management?				
		Dovadă de conformitate				
A.5.1.2	Revizuirea politicilor de securitate a informațiilor	Politicile sunt revizuite constant?				
A.6	**Organizarea securității informațiilor**					
A.6.1.1	Roluri și responsabilități de securitate	Rolul și responsabilitățile definite și atribuite			37, 38, 39, 40, 41, 42, 43	
A.6.1.2	Separarea atribuțiilor					
A.6.1.3	Contactul cu autoritățile	Identificarea autorităților competente Stabilirea unei forme de cooperare			31, 35, 36	
A.6.1.4	Contactul cu grupuri de interese speciale	Identificarea grupurilor Stabilirea unei forme de cooperare				
A.6.1.5	Securitatea informațiilor în managementul proiectelor	Definirea politicilor și procedurilor specifice				
A.6.2.1	Politica privind dispozitivele mobile	Definirea politicilor și procedurilor specifice				Politica privind propriul dispozitiv (BYOD) (o) Politica privind dispozitivele mobile și lucrul la distanță (o)
A.6.2.2	Telemunca	Definirea politicilor și procedurilor specifice				
A.7	**Securitatea resurselor umane**					
A.7.1.1	Screening	Definirea politicilor și procedurilor specifice			10	
A.7.1.2	Termeni și condiții de angajare	Definirea politicilor și procedurilor specifice				**Definirea rolurilor și a responsabilităților**
A.7.2.1	Responsabilități ale managementului	Definirea politicilor și procedurilor specifice				
A.7.2.2	Conștientizarea, educația și instruirea în materie de securitate a informațiilor	Definirea politicilor și procedurilor specifice				
A.7.2.3	Proceduri disciplinare	Definirea politicilor și procedurilor specifice				

A.7.3.1	Încetarea sau schimbarea responsabilităților angajatului	Definirea politicilor și procedurilor specifice				
A.8	**Managementul activelor**					
A.8.1.1	Inventarul activelor	Lista de inventar			5, 15	**Inventarul activelor**
A.8.1.2	Dreptul de proprietate asupra activelor	Lista proprietarilor activelor				
A.8.1.3	Utilizarea acceptabilă a activelor	Definirea politicilor și procedurilor specifice				**Utilizarea acceptabilă a activelor**
A.8.1.4	Returnarea activelor	Definirea politicilor și procedurilor specifice				
A.8.2.1	Clasificarea informațiilor	Definirea politicilor și procedurilor specifice			5, 9, 10, 11, 13, 14, 15, 18, 35, 36	**Politica de clasificare a informațiilor**
A.8.2.2	Etichetarea informațiilor	Definirea politicilor și procedurilor specifice			5, 13	**Politica de clasificare a informațiilor**
A.8.2.3	Manipularea activelor	Definirea politicilor și procedurilor specifice			5, 7, 8, 9, 10, 11, 13, 14	**Politica de clasificare a informațiilor**
A.8.3.1	Managementul suporturilor mobile	Definirea politicilor și procedurilor specifice			5, 20	
A.8.3.2	Eliminarea dispozitivelor media	Definirea politicilor și procedurilor specifice			5, 7, 8, 17, 18, 20	Politica de eliminare și distrugere (o)
A.8.3.3	Transferul suporturilor fizice	Definirea politicilor și procedurilor specifice			5, 20	
A.9	**Controlul accesului**					
A.9.1.1	Politica de control a accesului	Definirea politicilor și procedurilor specifice			5, 16, 17	**Politica de control al accesului**
A.9.1.2	Accesul la rețele și servicii de rețea	Definirea politicilor și procedurilor specifice			16, 17	
A.9.2.1	Înregistrarea utilizatorilor	Definirea politicilor și procedurilor specifice			16, 17	Politica privind parolele (o)
A.9.2.2	Furnizarea accesului	Definirea politicilor și procedurilor specifice			16, 17	
A.9.2.3	Gestionarea drepturilor privilegiate de acces	Definirea politicilor și procedurilor specifice			16, 17	Politica privind parolele (o)
A.9.2.4	Managementul informațiilor de autentificare a utilizatorilor	Definirea politicilor și procedurilor specifice			16, 17	Politica privind parolele (o)
A.9.2.5	Revizuirea drepturilor de acces ale utilizatorilor	Definirea politicilor și procedurilor specifice			16, 17	
A.9.2.6	Eliminarea sau ajustarea drepturilor de acces	Definirea politicilor și procedurilor specifice			16, 17	
A.9.3.1	Utilizarea informațiilor secrete de autentificare	Definirea politicilor și procedurilor specifice			16, 17	Politica privind parolele (o)
A.9.4.1	Restricții de acces la informații	Definirea politicilor și procedurilor specifice			5, 16, 17	
A.9.4.2	Proceduri securizate de logare	Definirea politicilor și procedurilor specifice			16, 17	
A.9.4.3	Sistem de management al parolelor	Definirea politicilor și procedurilor specifice			16, 17	Politica privind parolele (o)

A.9.4.4	Utilizarea programelor utilitare privilegiate	Definirea politicilor și procedurilor specifice			16, 17	
A.9.4.5	Controlul accesului la codul sursă al programului	Definirea politicilor și procedurilor specifice				
A.10	**Criptografie**					
A.10.1.1	Politica de utilizare a controalelor criptografice	Definirea politicilor și procedurilor specifice			5, 20	
A.10.1.2	Managementul cheilor	Definirea politicilor și procedurilor specifice			5, 20	
A.11	**Securitatea fizică și de mediu**					
A.11.1.1	Perimetrul de securitate fizică	Definirea politicilor și procedurilor specifice				
A.11.1.2	Controlarea accesului fizic	Definirea politicilor și procedurilor specifice				
A.11.1.3	Securizarea birourilor, camerelor și a facilităților	Definirea politicilor și procedurilor specifice				
A.11.1.4	Protecție împotriva amenințărilor externe și de mediu	Definirea politicilor și procedurilor specifice				
A.11.1.5	Lucrul în zonele de securitate	Definirea politicilor și procedurilor specifice				Procedurile de lucru în zone de securitate (o)
A.11.1.6	Zonele de livrare și încărcare	Definirea politicilor și procedurilor specifice				
A.11.2.1	Amplasarea și protecția echipamentului	Definirea politicilor și procedurilor specifice				
A.11.2.2	Sprijinirea utilităților	Definirea politicilor și procedurilor specifice				
A.11.2.3	Securitatea cablajelor	Definirea politicilor și procedurilor specifice				
A.11.2.4	Întreținerea echipamentelor	Definirea politicilor și procedurilor specifice				
A.11.2.5	Eliminarea activelor	Definirea politicilor și procedurilor specifice				
A.11.2.6	Securitatea echipamentelor și a activelor în afara incintelor	Definirea politicilor și procedurilor specifice				
A.11.2.7	Eliminarea sau reutilizarea securizată a echipamentelor	Definirea politicilor și procedurilor specifice				Politica de eliminare și distrugere (o)
A.11.2.8	Echipamente nesupravegheate	Definirea politicilor și procedurilor specifice				
A.11.2.9	Politica biroului și ecranului clar	Definirea politicilor și procedurilor specifice				Politica clară a biroului și a ecranului clar (o)
A.12	**Securitatea operațiunilor**					
A.12.1.1	Proceduri de operare documentate	Definirea politicilor și procedurilor specifice			7, 8, 12, 13, 14, 15, 16, 18, 19, 21, 22	**Proceduri de operare pentru managementul IT**
A.12.1.2	Managementul schimbării	Definirea politicilor și procedurilor specifice				Politica de management al schimbărilor (o)
A.12.1.3	Managementul capacității	Definirea politicilor și procedurilor specifice				

A.12.1.4	Separarea dezvoltării, testării, și a mediilor operaționale	Definirea politicilor și procedurilor specifice				
A.12.2.1	Controale împotriva programelor malware	Definirea politicilor și procedurilor specifice				
A.12.3.1	Backup	Definirea politicilor și procedurilor specifice			16, 17, 18	Politica de backup (o)
A.12.4.1	Jurnal de evenimente	Definirea politicilor și procedurilor specifice				**Registrul activităților utilizatorilor**
A.12.4.2	Protecția informațiilor jurnalizate	Definirea politicilor și procedurilor specifice				
A.12.4.3	Jurnalele de administrator și operator	Definirea politicilor și procedurilor specifice				**Registrul incidentelor de securitate**
A.12.4.4	Sincronizarea ceasului	Definirea politicilor și procedurilor specifice				
A.12.5.1	Instalarea software-ului pe sisteme operaționale	Definirea politicilor și procedurilor specifice				
A.12.6.1	Gestionarea vulnerabilităților tehnice	Definirea politicilor și procedurilor specifice				
A.12.6.2	Restricție la instalarea software-ului	Definirea politicilor și procedurilor specifice				
A.12.7.1	Controlul auditului sistemului informațional	Definirea politicilor și procedurilor specifice				
A.13	**Securitatea comunicațiilor**					
A.13.1.1	Controale de rețea	Definirea politicilor și procedurilor specifice			20	
A.13.1.2	Securitatea serviciilor de rețea	Definirea politicilor și procedurilor specifice			20	
A.13.1.3	Segregarea în rețele	Definirea politicilor și procedurilor specifice			20	
A.13.2.1	Politici și proceduri pentru transferul de informații	Definirea politicilor și procedurilor specifice			5, 7, 8, 15, 20, 26	Politica privind transferul de informații (o)
A.13.2.2	Acorduri privind transferul de informații	Definirea politicilor și procedurilor specifice			5, 7, 8, 20, 26	Politica privind transferul de informații (o)
A.13.2.3	Mesageriile electronice	Definirea politicilor și procedurilor specifice			5, 7, 8, 20, 26	Politica privind transferul de informații (o)
A.13.2.4	Acorduri de confidențialitate	Definirea politicilor și procedurilor specifice			5, 7, 8, 20, 26	**Definirea rolurilor și a responsabilităților**
A.14	**Achiziționarea, dezvoltarea și întreținerea sistemelor**					
A.14.1.1	Analiza și specificațiile cerințelor de securitate a informațiilor	Definirea politicilor și procedurilor specifice			5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 22	
A.14.1.2	Securizarea serviciilor de aplicații în rețelele publice	Definirea politicilor și procedurilor specifice			14	
A.14.1.3	Protejarea tranzacțiilor de servicii de aplicații	Definirea politicilor și procedurilor specifice			14	
A.14.2.1	Politica de dezvoltare sigură	Definirea politicilor și procedurilor specifice				
A.14.2.2	Proceduri de control al schimbării sistemului	Definirea politicilor și procedurilor specifice				

A.14.2.3	Revizuirea tehnică a aplicațiilor după operarea modificărilor platformei	Definirea politicilor și procedurilor specifice				
A.14.2.4	Restricții la modificările pachetelor software	Definirea politicilor și procedurilor specifice				Politica de management al schimbărilor (o)
A.14.2.5	Principii sigure de inginerie a sistemului	Definirea politicilor și procedurilor specifice				**Proceduri securizate de inginerie a sistemului**
A.14.2.6	Mediu securizat de dezvoltare	Definirea politicilor și procedurilor specifice				
A.14.2.7	Dezvoltare externalizată	Definirea politicilor și procedurilor specifice				
A.14.2.8	Testarea securității sistemului	Definirea politicilor și procedurilor specifice				
A.14.2.9	Testarea acceptării sistemului	Definirea politicilor și procedurilor specifice				
A.14.3.1	Protecția datelor de testare	Definirea politicilor și procedurilor specifice				
A.15	**Relația cu furnizorii**					
A.15.1.1	Politica de securitate a informațiilor pentru relațiile cu furnizorii	Definirea politicilor și procedurilor specifice			27, 28	**Politica de securitate privind furnizorii**
A.15.1.2	Abordarea securității în cadrul acordurilor de furnizare	Definirea politicilor și procedurilor specifice			27, 28	
A.15.1.3	Lanț de furnizare a tehnologiei informației și comunicațiilor	Definirea politicilor și procedurilor specifice			27, 28	
A.15.2.1	Monitorizarea și revizuirea serviciilor furnizorilor	Definirea politicilor și procedurilor specifice			27, 28	
A.15.2.2	Gestionarea modificărilor serviciilor furnizorilor	Definirea politicilor și procedurilor specifice			27, 28	
A.16	**Gestionarea incidentelor de securitate a informațiilor**					
A.16.1.1	Responsabilități și proceduri	Definirea politicilor și procedurilor specifice			12, 13, 14, 18, 19, 21, 22, 26, 33, 34, 48	
A.16.1.2	Raportarea evenimentelor de securitate a informațiilor	Definirea politicilor și procedurilor specifice			12, 13, 14, 18, 19, 21, 22, 26, 33, 34, 48	
A.16.1.3	Raportarea punctelor slabe ale securității informațiilor	Definirea politicilor și procedurilor specifice			12, 13, 14, 18, 19, 21, 22, 26, 33, 34, 48	
A.16.1.4	Evaluarea și decizia privind evenimentele de securitate a informațiilor	Definirea politicilor și procedurilor specifice			12, 13, 14, 18, 19, 21, 22, 26, 33, 34, 48	
A.16.1.5	Răspuns la incidentele de securitate a informațiilor	Definirea politicilor și procedurilor specifice			12, 13, 14, 18, 19, 21, 22, 26, 33, 34, 48	**Procedura de gestionare a incidentelor**

A.16.1.6	Învățarea din incidentele de securitate a informațiilor	Definirea politicilor și procedurilor specifice			12, 13, 14, 18, 19, 21, 22, 26, 33, 34, 48	
A.16.1.7	Colectarea probelor	Definirea politicilor și procedurilor specifice			12, 13, 14, 18, 19, 21, 22, 26, 33, 34, 48	
A.17	**Aspecte privind securitatea informațiilor în managementul continuității afacerii**					
A.17.1.1	Planificarea continuității securității informațiilor	Definirea politicilor și procedurilor specifice			5	Analiza impactului asupra organizației (o)
A.17.1.2	Implementarea continuității securității informațiilor	Definirea politicilor și procedurilor specifice			5	**Procedurile de continuitate**
A.17.1.3	Verificați, revizuiți și evaluați continuitatea securității informațiilor	Definirea politicilor și procedurilor specifice			5	Planul de exerciții și testare (o) Plan de întreținere și revizuire (o)
A.17.2.1	Disponibilitatea facilităților de prelucrare a informațiilor	Definirea politicilor și procedurilor specifice			5	Strategia de continuitate a afacerii (o)
A.18	**Conformitate**					
A.18.1.1	Identificarea legislației aplicabile și a cerințelor contractuale	Definirea politicilor și procedurilor specifice			6, 18, 23, 26, 28, 85, 86, 87, 88, 90, 92 – 99.	**Cerințe legale, de reglementare și contractuale**
A.18.1.2	Drepturi pentru proprietate intelectuala	Definirea politicilor și procedurilor specifice			26	
A.18.1.3	Protecția arhivelor	Definirea politicilor și procedurilor specifice			7, 8, 16, 20, 26, 28	
A.18.1.4	Confidențialitate și protecția informațiilor personale	Definirea politicilor și procedurilor specifice			Integral	
A.18.1.5	Reglementarea controalelor criptografice	Definirea politicilor și procedurilor specifice			26	
Clauze	(clauza 4.3)					**Domeniul de aplicare al ISMS**
	(clauza 5.2)					**Politica de securitate**
	(clauza 5.3)				26, 27, 37, 38, 39, 40, 41, 42, 43,	
	(clauza 6.2)					**Obiectivele de securitate a informațiilor**
	(clauza 6.1.2)				5, 6, 10, 17, 18, 19, 20, 21, 22, 35, 36	**Metodologia de evaluare și de tratare a riscurilor**
	(clauza 6.1.3)					**Declarație de aplicabilitate SoA**

	(clauza 6.1.3, clauza 6.2)					**Planul de tratare a riscurilor**
	(clauza 7.2)					**Registrul formării profesionale, a competențelor, a experienței și a calificărilor**
	(clauza 8.2)				28, 32	**Raportul de evaluare a riscurilor**
	(clauza 9.1)				26, 28,	**Rezultatele monitorizării**
	(clauza 9.2)					**Programul și rezultatele auditului intern**
	(clauza 9.3)					**Rezultatele analizei conducerii**
	(clauza 10.1)					**Rezultatele acțiunilor corective**

Concluzii

Analiza GAP reprezintă un suport pentru companii în identificarea cerințelor care sunt și nu sunt îndeplinite în cadrul unui proiect și măsoară, de asemenea, investiția de timp, bani și resurse umane necesara pentru atingerea scopului propus. Analiza GAP este un instrument sau o tehnică care permite unei organizații să compare performanța reală cu standardele.

Analiză GAP va arată cât de departe este organizația de a fi conformă cu standardul ISO 27001. Analiză GAP pentru ISO 27001 poate aduce beneficii unei organizației, inclusiv:

1) Organizația va obține o imagine de ansamblu a ceea ce trebuie făcut pentru a obține certificarea ISO 27001.

2) Acesta va permite organizației să își extindă parametrii SMSI în toate funcțiile afacerii.

3) Este mai probabil să se obțină angajamentul conducerii organizației.

4) Organizația înțelege ce trebuie să facă în continuare.

5) Certificarea acreditată va fi accesibilă.

Rezultatul evaluării va evidenția date despre starea actuală de securitate a informațiilor în comparație cu starea preconizată în conformitate cu standardul ISO / IEC 27001. Analiza GAP compară situația existentă, dacă controalele ISO / IEC 27001: 2013 au fost realizate bine, inclusiv politici, proceduri, instrucțiuni de lucru, până la documentație.

Analiza GAP în GDPR oferă organizației o înțelegere clară a locului în care organizația se află în legătură cu GDPR și ce este necesar pentru a demonstra conformitatea. Analiza diferenței GDPR se bazează pe cele 6 principii ale GDPR și oferă o analiză transparentă a gradului de compatibilitate cu GDPR.

Rezultatele auditului și analiza GAP ajută la identificarea domeniilor principale de risc și la ceea ce trebuie făcut pentru a reduce decalajul de a deveni conform GDPR. Angajatorii ar trebui să ia în considerare, de asemenea, cum să construiască considerații privind confidențialitatea în sistemele de resurse umane încă de la început și în permanență, pentru a contribui la îndeplinirea standardului GDPR privind confidențialitatea.

O analiză GAP ar trebui întotdeauna să se bazeze pe o strategie de evaluare a riscurilor și să o compare cu cele mai bune practici din cadrul GDPR și securității IT.

CAPITOLUL 6. CERCETARE STATISTICĂ PRIVIND CONFORMITATEA ORGANIZAȚIILOR CU CERINȚELE STANDARDULUI ISO 27001 ȘI ALR REGULAMENTULUI GDPR

Prin prezenta lucrare, s-a urmărit realizarea unei analize calitative privind îndeplinirea de către organizații a cerințelor standardului ISO 27001. În acest sens, a fost elaborat un chestionat, care a fost aplicat unui număr de 192 organizații, atât publice, cât și private. Toate organizațiile activează în România, iar în acest sens sunt relevante și prevederile Regulamentului nr. 679 din 27 aprilie 2016 privind protec ia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circula ie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

Pentru realizarea analizei calitative, a fost efectuată o revizuire a controalelor din Anexa A a standardului ISO 27001. Rezultatele analizei calitative se bazează pe relația dintre situația existentă în organizațiile selectate în scopul prezentei cercetări și posibilitatea certificării conformității cu standardul ISO 27001, într-un termen scurt.

În urma analizării rezultatelor, au fost identificate aspecte care ridică dificultăți organizațiilor interesate să implementeze standardul ISO 27001.

În cadrul procesului de interpretare a rezultatelor, au fost indicați factori alternativi posibili, care pot explica observațiile empirice care nu au fost studiate în prezenta teză.

În final, rezultatele analizei calitative au fost rezumate sub forma unei baze de date pentru cercetări ulterioare, fiind totodată folosite la realizarea unui model de analiză a îndeplinirii cerințelor standardului ISO 27001 în cadrul unei organizații.

În vederea întocmirii chestionarului, au fost selectate o serie de controale din Anexa A a standardului ISO 27001, pe baza cărora a fost analizată conformitatea organizațiilor cu cerințele specifice ale unui Siatem de management al Securității Informațiilor.

În primul rând, s-a urmărit să se verifice dacă organizația a determinat cerințele specifice standardului, inclusiv cerințele legale, de reglementare și contractuale.

Totodată, s-a verificat dacă au fost determinate, în cadrul organizației, limitele și aplicabilitatea unui sistem de management al securității informațiilor, luând în considerare aspectele interne și externe, cerințele părților interesate, interfețele și interacționarea cu beneficiarii și alte organizații.

În etapa următoare, s-a procedat la corelarea întrebărilor cu controalele din Anexa A din Standard. Au fost formulate întrebări specifice. O parte dintre întrebări au fost formulate în legătură directă cu conținutul și cerințele controalelor din Anexa A a Standardului, fiind totodată inserate întrebări care au

avut rolul de a clarifica anumite elemente particulare din cadrul organizațiilor. Pentru fiecare întrebare, au fost oferite două variante de răspuns: Da, sau Nu.

Studiul a scos în evidență un grad redus de conformitate totală cu cerințele standardului ISO 27001: 2013, doar 16% dintre organizații respectând prevederile cuprinse în secțiunile standardului. În același timp, 60% dintre organizațiile din eșantion respectă parțial cerințele impuse pentru implementarea Sistemului de Management al Securității Informațiilor, însă numărul de măsuri care au rămas de îndeplinit, variază.

Majoritatea organizațiilor nu angajează un manager ISMS cu normă întreagă Doar 16% dintre acestea angajează un manager dedicat, iar 19% dintre managerii IT sunt responsabili pentru managementul Sistemului ISMS.

În ceea ce privește existența procedurilor de securitate, acestea sunt integrate în activitatea curentă a 80% dintre organizațiile analizate, însă complexitatea procedurilor variază, fiind influențată cel mai mult de mărimea organizației și de numărul de departamente.

Referitor la utilizarea standardului ISO 27001, pentru îndeplinirea cerințelor Regulamentului european GDPR, doar 28% dintre organizații au luat în considerare corelarea prevederilor din cele două documente. Totuși, conformitatea cu cerințele Regulamentului general privind protecția datelor este atinsă de un număr de peste 70% din organizațiile analizate, iar alte 17% respectă doar parțial cerințele GDPR.

Motivele care au determinat organizațiile să implementeze măsuri privind securitatea informațiilor, fie prin implementarea Sistemului de Management al Securității Informațiilor, fie prin implementarea parțială a unor măsuri specifice, țin în general de: nevoie de a îmbunătăți nivelul de securitate a informațiilor (90% dintre respondenți), respectarea cerințelor legale (87% dintre respondenți), cerințe legate de natura sectorului în care activează organizația (42%), sau pentru a obține un avantaj competitiv (37%).

În prezent, în România se remarcă o creștere a preocupării organizațiilor pentru securitatea informațiilor. Majoritatea aleg să implementeze măsurile în mod independent, în funcție de nevoile specifice. Până la acest moment, atenția entităților s-a îndreptat către conformarea față de cerințele Regulamentului GDPR, în timp ce orientarea către sistemul de certificare ISO este întâlnită în puține cazuri. Nu în ultimul rând, se remarcă un scepticism al managementului organizațiilor față de organismele de certificare locale, precum și o lipsă acută de informații referitoare la procesul de certificare, în cazul oricărui standard.

CONSIDERAȚII FINALE. CONTRIBUȚII ORIGINALE

Considerații finale.

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 și 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).

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.

Implementarea GDPR de către organizații ar trebui privită în contextul atingerii obiectivelor lor specifice. Există o necesitate clară de a sublinia beneficiile sale pentru organizații și valorile adăugate pentru afaceri. Este absolut greșit să înțelegeți GDPR ca o altă restricție la mediul de operare. GDPR este un instrument pentru generarea unui avantaj strategic bazat pe încrederea între organizație, angajații săi, clienți și parteneri.

GDPR încurajează utilizarea certificărilor precum ISO 27001 pentru a arăta că organizația își gestionează activ securitatea datelor în conformitate cu cele mai bune practici internaționale. Rezultatele obținute prin prezenta cercetare ne permit să concluzionăm că orice organizație care a pus deja în aplicare sau este în proces de implementare a ISO / CEI 27001 este relativ bine pregătită pentru a demonstra conformitatea cerințele GDPR. Noua reglementare a protecției datelor introduce o serie de reguli care impun organizațiilor să implementeze controale.

O astfel de analiză poate fi utilizată ca punct de pornire pentru definirea criteriilor de respectare a GDPR. În absența unor reguli și constrângeri clare, identificarea standardelor de securitate care pot fi aplicate protecției datelor pentru a reduce decalajul dintre practicile actuale și cerințele legale viitoare poate spori încrederea DS și poate oferi avantaje competitive. De asemenea, poate facilita trecerea la o nouă abordare consolidată a protecției datelor cu caracter personal.

Prin chestionarul cu privire la măsura în care certificarea sistemului de management al securității informațiilor de către ISO 27001 acordă conformitatea companiilor cu GDPR s-a constatat că implementarea unui sistem de management al securității informațiilor de către o companie trebuie să asigure că toate controalele relevante privind combaterea riscurilor asociate confidențialității, integrității și disponibilității sunt puse în aplicare și menținute funcționale.

Pe lângă controalele tehnice adoptate, documentația structurată, monitorizarea și îmbunătățirea continuă, implementarea ISO 27001 promovează o cultură și conștientizarea incidentelor de securitate în organizații. Angajații acestor organizații sunt mai conștienți și au mai multe cunoștințe pentru a putea detecta și raporta incidentele de securitate. Securitatea informației nu se referă doar la tehnologie. Este vorba și despre oameni și procese.

Primul lucru pe care ar trebui să îl facă o organizație este o analiză GAP a Regulamentului GDPR pentru a determina ce mai rămâne de făcut pentru a răspunde cerințelor GDPR UE, iar aceste cerințe pot fi adăugate cu ușurință prin intermediul sistemului de gestionare a securității informațiilor, care este deja stabilit de ISO 27001.

Contribuții originale

Contribuțiile originale aduse de această cercetare constă în

1. Elaborarea matricei de mapare GDPR – ISO 27001: elemente de corespondență pentru 58 de articole GDPR

   Matricea de mapare contribuie la analiza oportunității implementării unui Sistem de Management al Securității Informației în cadrul organizațiilor, oferind posibilitatea managementului organizației de a proiecta o viziune de ansamblu asupra conformității cu două documente esențiale pentru securitatea datelor.

   Matricea a identificat puncte de corespondență pentru 58 din cele 99 de articole ale Regulamentului GDPR, fiind un instrument util, care poate sta la baza unor studii ulterioare în domeniul arhitecturii sistemelor de securitate a datelor.

2. Elaborarea instrumentului de analiză GAP, care permite evaluarea conformității organizației atât pentru cerințele GDPR, cât și pentru cerințele standardului

   Instrumentul de analiză GAP este cea mai importantă contribuție originală, realizată ca urmare a prezentei cercetări. Modelul dezvoltat reprezintă un instrument util atât pentru managementul organizațiilor, cât și pentru departamentele sau lucrătorii responsabili cu implementarea politicilor și a sistemelor de securitate, permițând monitorizarea simultană a gradului de conformitate cu cerințele celor două documente: standardul ISO 27001 și Regulamentul GDPR.

3. Elaborarea și implementarea chestionarului privind nivelul de conformitate al organizațiilor cu cele două documente

   Chestionarul a reflectat nivelul de pregătire al eșantionului de 192 de organizații, în vederea atingerii conformității. Rezultatele sunt relevante pentru direcțiile ulterioare de cercetare, dar și pentru pregătirea unor ghiduri care să faciliteze îndeplinirea cerințelor de conformitate, prin care să fie abordate cu precădere aspectele care au cel mai scăzut grad de îndeplinire, în cadrul eșantionului. Totodată, prin aplicarea chestionarului prin metoda interviului, s-au furnizat respondenților clarificările și informațiile necesare, astfel că informațiile și valorile colectate se prezintă un grad ridicat de precizie.

4. Elaborarea unei platforme online - ghid pentru organizații în domeniul standardului ISO 27001:2013

   Prin intermediul platformei online s-a urmărit oferirea informațiilor din capitolul 3 al tezei, sub forma unui ghid de implementare, în regim de acces deschis. Această platformă reprezintă un instrument facilitator pentru organizațiile preocupate de protejarea securității datelor.

   În prezent, platforma cuprinde informații, analize și interpretări pentru fiecare clauză a Standardului ISO 27001, respectiv pentru fiecare control din Anexa A. Platforma se constituie inclusiv ca o direcție viitoare de cercetare, fiind necesară dezvoltarea acesteia.

Direcții ulterioare de cercetare

1. Testarea platformei online

   Platforma online înglobează, în prezent, conținut referitor la clauzele și controalele standardului. Pe termen mediu, se are în vedere testarea conținutului prin aplicarea unor chestionare utilizatorilor platformei, pentru a se analiza modul în care analizele elaborate contribuie la implementarea sistemelor de securitate în organizații.
2. Actualizarea analizei conținutului, în funcție de modificarea standardului și evoluția cercetărilor din domeniu

   Conținutul platformei va fi analizat în funcție de viitoarele modificări ale Standardului ISO 27001, precum și de evenimente relevante, precum incidente de securitate cu caracteristici specifice.
3. Lansarea unei aplicații de tip Decision-Making, pentru instrumentul GAP

   Instrumentul de analiză GAP, destinat evaluării nivelului de conformitate atât pentru cerințele standardului ISO 27001, cât și ale Regulamentului GDPR, poate fi transpus într-o aplicație informatică, pornind de la algoritmul bazat pe matricea de mapare.

BIBLIOGRAFIE

1. ABUSAAD, Belal; SAEED, Fahad A.; ALGHATHBAR, Khaled; KHAN, Bilal. Implementation of ISO 27001 in Saudi Arabia – obstacles, motivations, outcomes, and lessons learned. In: *Proceedings of the 9th Australian Information Security Management Conference*, Edith Cowan University, Perth Western Australia, 5-7 December, 2011, doi: 10.4225/75/57b52709cd8b2
2. AHMED, B.Si; NIBOUCHE, F. Using survey to estimate the effort of setting up an Information Security Management System: Case ITC Organizations. In: *5th International Conference on Control, Decision and Information Technologies (CoDIT)*, 10-13 April 2018, Thessaloniki, Greece. Thessaloniki: IEEE, 2018, doi: 10.1109/CoDIT.2018.8394907
3. ALSHITRI, Khalid I.; ABANUMY, Abdulmohsen N. Exploring the Reasons Behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia. In: *Proceedings of the International Conference on Information Science & Applications (ICISA),* Seoul, South Korea, 6-9 May 2014. Seoul. IEEE, 2014, doi: 10.1109/ICISA.2014.6847396
4. Apud. ABU-MUSA, Ahmad. Information security governance in Saudi organizations: an empirical study*. Information Management & Computer Security*. 2010, vol. 18, no. 4, pp. 226-276, doi: 10.1108/09685221011079180
5. ARMEANU, Stefan Daniel; VINTILA, Georgeta; GHERGHINA, Stefan Cristian A Cross-Country Empirical Study Towards the Impact of Following ISO Management System Standards on Euro-Area Economic Confidence. *Amfiteatru Economic Journal*. 2017, vol. 19, no. 44, pp. 144-165. Disponibil: http://www.amfiteatrueconomic.ro/temp/Article_2599.pdf
6. ARMERDING, Taylor The 17 biggest data breaches of the 21st century [online]. *Csoonline.com*, 26 Jan. 2018 [citat 8.09.2018]. Disponibil: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html
7. BANILA, Silviu Marian, Analiza: Cele mai importante breșe de securitate din istoria recentă [online]. *Manager.ro*, 18 februarie 2014 [citat 8.09.2018]. Disponibil: http://www.manager.ro/articole/analize-92/analiza-cele-mai-importante-brese-de-securitate-din-istoria-recenta-60867.html
8. BOEHMER, W. Cost-Benefit Trade-Off Analysis of an ISMS Based on ISO 27001. In: *Proceedings of the International Conference on Availability, Reliability, and Security*, Fukuoka, Japan, 16-19 March 2009. Fukuoka: IEEE, 2009 pp. 392-399, doi: 10.1109/ARES.2009.128
9. BOEHMER, Wolfgang. Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. In: *Emerging Security Information, Systems and Technologies*, SECURWARE'08: Second International Conference, Cap Esterel, France, 25-31 Aug. 2008. Cap Esterel: IEEE, 2008, pp. 224-231, doi: 10.1109/SECURWARE.2008.7
10. BRODERICK, J. Stuart. ISMS, security standards and security regulations. *Information Security Technical Report*. 2006, vol. 11, no. 1, pp. 26-31, doi: 10.1016/j.istr.2005.12.001

11. *BS ISO 27001 Information technology – security techniques – information security management systems – requirements*. London: British Standards Institute, 2005.
12. CALDER, Alan; WATKINS, Setve. *IT governance: a manager's guide to data security and ISO 27001/ ISO 27002*. 4th ed. London: Kogan Page Limited, 2008.
13. CANDIWAN. Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia. In: *Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security*, Kuala Lumpur, Malaysia,17-19 Nov., 2014 [citat 8.09.2018]. Disponibil: https://www.researchgate.net/publication/268462706_Analysis_of_ISO27001_Implementation_for_Enterprises_and_SMEs_in_Indonesia
14. CANDRA, Johanes Widhi; BRILIYANT, Obrina Candra; TAMBA, Sion Rebeca. ISMS Planning Based On ISO/IEC 27001:2013 Using Analytical Hierarchy Process at Gap Analysis Phase (Case Study: XYZ Institute). In: *11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, Lombok, Indonesia, 26-27 Oct. 2017. Lombok: IEEE, 2017, doi: 10.1109/TSSA.2017.8272916
15. CĂLINESCU, Mihaela Îmbunătățirea sistemelor de management pentru sistemele informatice. *Buletinul AGIR* [online]. 2003, nr. 3 [citat 8.09.2018]. Disponibil: http://www.agir.ro/buletine/80.pdf
16. *Certification Europe. ISO 27001 Global Survey*: The Facts and the Figures Underlying the Growth of ISO 27001 World-wide, Certification Europe, Dublin, 2008.
17. COJOCARU, Igor; GUZUN, Mihail. Sistemul de management al securită ii informa ionale ISO/IEC 27001:2013. Algoritmul de implementare. In: *Proceeding of the 8th International Conference on Microelectronics and Computer Science*, Chisinau, Republic of Moldova, October 22-25, 2014. Chișinău: Technical University of Moldova, 2014, pp. 362-365.
18. COLES-KEMP, Luzzie; OVERILL, Richard E. The Information Security Ownership Question in ISO/IEC 27001 – an Implementation Perspective. In*: Proceedings of the 4th Australian Information Security Conference*, Perth, Australia, 5 December, 2006, doi: 10.4225/75/57b656ae34767
19. DISTERER, Georg. ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*. 2013, no. 4, pp. 92-100, doi: 10.4236/jis.2013.42011
20. DOBRATZ, Susanne; RÖDIG, Peter; BORGHOFF, Uwe M.; RÄTZKE, Björn; SCHOGER, Astrid. The Use of Quality Management Standards in Trustworthy Digital Archives. *The International Journal of Digital Curation*. 2010, vol. 5, no. 1, pp. 46-63, doi: 10.2218/ijdc.v5i1.143
21. EVANS, Rhys; TSOHOU, Aggeliki; TRYFONAS, Theo; MORGAN, Thea. Engineering secure systems with ISO 26702 and 27001. In: *System of Systems Engineering (SoSE): the 5th International Conference*, Loughborough, UK, 22-24 June 2010, Loughborough,: IEEE, 2010, pp. 1-6, doi: 10.1109/SYSOSE.2010.5544065

22. FOMIN, Vladislav V.; VRIES, Henk J.; BARLETTE, Yves. ISO/IEC 27001 Information Systems Security Management Standard: Exploring the reasons for low adoption. In: *Proceedings of The third European Conference on Management of Technology (EUROMOT)*. Nice, France, September 2008. Disponibil: https://www.researchgate.net/publication/228898807_ISOIEC_27001_Information_Systems_Security_Management_Standard_Exploring_the_reasons_for_low_adoption
23. GILLIES, Alan. Improving the quality of information security management systems with ISO27000. *The TQM Journal.* 2001, vol. 23, no. 4, pp. 367-376, doi: 10.1108/17542731111139455
24. GREAVU-ȘERBAN, Valerică. Prezentare ISO27001: Sistemul de management al securită ii informa ionale. In: *Conferin a Ştiin ifică Na ională cu participare Interna ională „Zilele Academice Ieşene"*, edi ia a XXV-a, Iasi, 16-17 septembrie 2010, vol. 11, doi: 10.13140/RG.2.1.2418.5449
25. HAGEN, Janne Merete; ALBRECHTSEN, Eirik; HOVDEN, Jan.Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*. 2008, vol. 16, no. 4, pp.377-397, doi: 10.1108/09685220810908796
26. HENNING, David. *Tackling ISO 27001: A Project to Build an ISMS. GIAC GCPM Gold Certification* [online]. SANS Institute, 2009 [citat 8.09.2018]. Disponibil: https://www.sans.org/reading-room/whitepapers/leadership/tackling-iso-27001-project-build-isms-33169
27. HONG, Kwo-Shing; CHI, Yen-Ping; CHAO, Louis R.; TANG, Jih-Hsing. An integrated system theory of information security management. *Information Management & Computer Security*. 2003, vol. 11, no. 5, pp. 243-248, doi: 10.1108/09685220310500153
28. HSU, C. W. Frame Misalignment: Interpreting the Implementation of Information Systems Security Certification in an Organization. *European Journal of Information Systems.* 2009, vol. 18, no. 2, pp. 140-150, doi: 10.1057/ejis.2009.7
29. HSU, Carol; WANG, Tawei; LU, Ang. The Impact of ISO 27001 Certification on Firm Performance. In: *49th Hawaii International Conference on System Sciences*, Koloa, HI, USA, 5-8 Jan. 2016. Koloa: IEEE, 2016, pp. 4842-4848, doi: 10.1109/HICSS.2016.600
30. *ISO 27001 Global Report 2016* [online]. IT Governance Ltd, Cambridgeshire Business Park, 2016 [citat 10.09.2018]. Disponibil: https://www.itgovernance.co.uk/download/ISO27001-Global-Report-2016.pdf
31. *ISO/IEC 27000-series* [online]. Wikipedia, last edited on 26 August 2018 [citat 8.09.2018]. Disponibil: https://en.wikipedia.org/wiki/ISO/IEC_27000-series
32. Key Components of the Standard: BS 7799 (ISO 17799) [online]. *Information Security Management System*, 2 November 2007 [citat 8.09.2018]. Disponibil: http://isms-guide.blogspot.com/2007/11/key-components-of-standard-bs-7799-iso.html

33. KOPIA, Jan. Study on Integration and Leadership Styles of Management Systems Based on a High Level Structure. In: *Proceedings of the 4th International Conference on Management Leadership and Governance (ICMLG 2016)*, St. Petersburg State, Russia, 14-14 April, 2016. Kidmore End: Academic Conferences International Limited, 2016, pp. 431-441.
34. KOPIA, Jan; KOMPALLA, Andreas; CEAUŞU, Ioana. Theory and Practice of Integrating Management Systems with High Level Structure. *Quality - Access to Success*. 2016, vol. 17, no. 155, pp. 52-59.
35. KU, Cheng-Yuan; CHANG, Yi-Wen;.YEN, David C. National Information Security Policy and its Implementation: A Case Study in Taiwan. *Telecommunications Policy.* 2009, vol. 33, no. 7, pp. 371-384, doi: 10.1016/j.telpol.2009.03.002
36. LI, Shing-Han; YEN, David C.; CHEN, Shih-Chih; CHEN, Patrick S.; LU, Wen-Hui; CHO, Chien-Chuan. Effects of virtualization on information security. *Computer Standards & Interfaces*. 2015, vol. 33, no. 7, pp. 371-384. Disponibil: 10.1016/j.telpol.2009.03.002
37. LOMAS, Elizabeth. Information governance: information security and access within a UK context. *Records Management Journal*. 2010, vol. 20, no. 2, pp. 182-196, doi: 10.1108/09565691011064322
38. MATARACIOGLU, Tolga; OZKAN, Sevgi. Analysis of the User Acceptance for Implementing ISO/IEC 27001:2005 in Turkish Public Organizations. *International Journal of Managing Information Technology*. 2011, vol. 3, no. 1, pp. 1-14, doi: 10.5121/ijmit.2011.3101
39. NABI, Syed Irfan; MIRZA, Abdulrahman A.; ALGHATHBAR, Khaled. Information Assurance in Saudi Organizations – An Empirical Study. In: *Security Technology, Disaster Recovery and Business Continuity. Communications in Computer and Information Science*, vol 122. Berlin, Heidelberg: Springer, 2010, pp. 18-28, doi: 10.1007/978-3-642-17610-4_3
40. NEUBAUER, Thomas; EKELHART, Andreas; FENZ, Stefan. Interactive Selection of ISO 27001 Controls under Multiple Objectives. In: *Proceedings of The Ifip Tc 11 23rd International Information Security Conference*. Boston: Springer, 2008, vol 278, pp. 477-492, doi: 10.1007/978-0-387-09699-5_31
41. POTTER, Chris; BEARD, Andrew. *Information Security Breaches Survey 2010*. London: Price Water House, Coopers Earl's Court, 2010.
42. PURCAREA, A.; TIGANOAIA, B.; PETREA, G., Considerations regarding the implementation and certification within ogranization security management systems. In: *International Conference on Management and Industrial Engineering*, Bucharest, 20-21 Oct., 2011. Bucharest: Niculescu Publishing House, 2011, pp. 106-113.
43. SINGH, Lakhwinder Pal; BHARDWAJ, Arvind; SACHDEVA, Anish. The Impact of ISO Implementation on Output Parameters in SME's in India. In: *Portland International Conference on Management of Engineering and Technology (PICMET 07)*, 5-9 August 2007, Portland, Oregon. Portland: IEEE, 2007, pp. 2031-2037, doi: 10.1109/PICMET.2007.4349532

44. SUSANTO, Heru; ALMUNAWAR, Mohammad Nabil; TUAN, Yong Chee. Information Security Challenge and Breaches*:* Novelty Approach on Measuring ISO 27001 Readiness Level. *International Journal of Engineering and Technology.* 2012, vol. 2, no. 1, pp. 67-75. Disponibil: http://iet-journals.org/archive/2012/jan_vol_2_no_1/36585913256483_abstract.php
45. SUSANTO, Heru; ALMUNAWAR, Mohammad Nabil; TUAN, Yong Chee. Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences.* 2011, vol. 11, no. 5, pp. 23-29.
46. SUSSY, Bayona; WILBER, Chauca; MILAGROS, Lopez; CARLOS, Maldonado. ISO/IEC 27001 Implementation in Public Organizations: A Case Study. In: *10th Iberian Conference on Information Systems and Technologies (CISTI)*, Aveiro, Portugal 17-20 June 2015, Aveiro: IEEE, 2015, doi: 10.1109/CISTI.2015.7170355
47. *The ISO Survey of Management System Standard Certification 2017* [online]. International Organization for Standardization, August 2018 [citat 10.09.2018]. Disponibil: https://www.iso.org/the-iso-survey.html
48. TUDOR, Razvan; BADEA, Dumitru. Operational risk quantification and modelling within Romanian insurance industry. In: *Proceedings of the International Conference on Business Excellence*, Bucharest, 30-31 March 2017. Bucharest, 2017, vol. 11, no. 1, pp. 637-648, doi: 10.1515/picbe-2017-0068
49. ȚIGĂNOAIA, Bogdan. Comparative study regarding international standard on information security management systems in organizations: ISO/IEC 27001:2013 vs ISO/IEC 27001:2005. In: *2nd International Conference on Globalization, Intercultural Dialogue and National Identity*, 29-30 May 2014, Targu Mures, Romania. Targu Mures, 2014, pp. 102-109.
50. ȚIGĂNOAIA, Bogdan. Some Aspects Regarding the Information Security Management System within Organizations – Adopting the ISO/IEC 27001:2013 Standard. *Studies in Informatics and Control*. 2015, vol. 24, no. 2, pp. 201-210.
51. ȚIGĂNOAIA, Bogdan. Theoretical and practical considerations regarding the information security management system within organizations in concordance with the new international standard ISO / IEC 27001: 2013. In: *2nd International Conference on Globalization, Intercultural Dialogue and National Identity*, 29-30 May 2014, Targu Mures, Romania. Targu Mures, 2014, pp. 62-68.
52. AL-MAYAHI, Ibrahim, MANSOOR, Sa'ad P. ISO 27001 Gap Analysis - Case Study. In: *International Conference on Security & Management (SAM' 12)*, Las Vegas, July 16-19, 2012. [citat 16.01.2019]. Disponibil: http://worldcomp-proceedings.com/proc/p2012/SAM9779.pdf
53. ARAFIANDI, Andi. GAP Analysis: Determine the success [online]. *Andi Rafiandi's Blog*, 2015, 14 November [citat 16.01.2019]. Disponibil: https://arafiandi.wordpress.com/2015/11/14/gap-analysis-determine-the-success/

54. ARMERDING, Taylor. The 17 biggest data breaches of the 21st century [online]. *Csoonline.com*, 26 Jan. 2018 [citat 8.09.2018]. Disponibil: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

55. AVRIGEANU, Elena Andreea. GDPR. Stadiul actual și perspective. Soluții Titus. In: *Buletinul AGIR*. 2017, nr. 4, pp. 13-16 [citat 8.09.2018]. Disponibil: http://www.agir.ro/buletine/2904.pdf

56. BARNARD-WILLS, D. The technology foresight activities of European Union data protection authorities. In: *Technological Forecasting & Social Change*. 2017, vol. 116, pp. 142–150 [citat 16.01.2019]. Disponibil: 10.1016/j.techfore.2016.08.032

57. BAUER, Danielle 6 Steps to GDPR Implementation [online]. *RIMS Inc.*, 2018, 2 Aprilie [citat 16.01.2019]. Disponibil: http://www.rmmagazine.com/2018/04/02/6-steps-to-gdpr-implementation/

58. BÉLANGER, France, CROSSLER, Robert E. Privacy in the Digital Age: A Review of Information Privacy Research. In: *Information Systems. MIS Quarterly*. 2011, vol. 35, no. 4, pp. 1017-1041 [citat 16.01.2019]. Disponibil: DOI: 10.2307/41409971

59. BOWMAN, John, GUFFLET, Myriam. Meeting the Challenge of a Global GDPR and BCR Programme. In: *The European Data Protection Law Review (EDPL)*. 2017, vol. 3, no. 2, pp. 257-261 [citat 16.01.2019]. Disponibil: DOI: 10.21552/edpl/2017/2/21

60. BRODERICK, J.S. ISMS, security standards and security regulations. In: *Information Security Technical Report*. 2006, vol. 11, no. 1, pp. 26-31 [citat 14.01.2019]. Disponibil: DOI: 10.1016/j.istr.2005.12.001

61. CANDIWAN. Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia. In: *Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security*, Kuala Lumpur, Malaysia, 2014 [citat 11.01.2019]. Disponibil: https://www.researchgate.net/publication/268462706_Analysis_of_ISO27001_Implementation_for_Enterprises_and_SMEs_in_Indonesia

62. CLARKE, R. Internet Privacy Concerns Confirm the Case for Intervention. In: *Communications of the ACM*. 1999, vol. 42, no. 2, pp. 60–67 [citat 11.01.2019]. Disponibil: DOI: 10.1145/293411.293475

63. CLARKE, Roger. *What's 'Privacy'?* [online]. Version of 7 August 2006. Prepared for a Workshop at the Australian Law Reform Commission on 28 July 2006 [citat 11.01.2019]. Disponibil: http://www.rogerclarke.com/DV/Privacy.html

64. COOPER, Daniel P., MILNER-SMITH, Helena, YOUNG, Mark, MOSS, Ashley. Are You Ready for the European General Data Protection Regulation? In: *Employee Relations Law Journal*. 2017, vol. 43, no. 3, pp. 60-65.

65. Cybersecurity Survey reveals significant GDPR readiness GAP [online]. *© Varonis*, 6 December 2017 [citat 11.01.2019]. Disponibil: http://ir.varonis.com/news-releases/news-release-details/cybersecurity-survey-reveals-significant-gdpr-readiness-gap

66. DELL Secureworks Consulting Services Agreement [online]. *© StudyLib,* 2019 [citat 11.01.2019]. Disponibil: https://studylib.net/doc/9514822/iso-27001-gap-analysis

67. DEY, Manik. Information security management - a practical approach. In: *Proceeding AFRICAN 2007 Conference*, Windhoek, South Africa, 26-28 Sept. 2007. IEEE, 2007 [citat 16.01.2019]. Disponibil: DOI: 10.1109/AFRCON.2007.4401528

68. EDWARDS, Laura. Cybersecurity survey reveals significant GDPR readiness gap [online]. *© GDPR.Report*, 6 December 2017 [citat 11.01.2019]. Disponibil: https://gdpr.report/news/2017/12/06/cybersecurity-survey-reveals-significant-gdpr-readiness-gap/

69. FRANKLIN, Maren. *Performance Gap Analysis: Tips, Tools, and Intelligence for Trainers.* [S.n.]: American Society for Training and Development, 2006. ISBN: 978-1562864279.

70. FROMHOLZ, J.M. The European Union Data Privacy Directive. In: Berkeley Technology Law Journal. 2000, vol. 15, no. 1, pp. 461–484 [citat 11.01.2019]. Disponibil: DOI: 10.15779/Z383D48

71. GAP Analysis [online]. *© GlobalSequr*, 2018 [citat 11.01.2019]. Disponibil: https://globalsequr.com/en/gdpr/gap-analysis/

72. GAP Analysis. In: *Cambridge Business English Dictionary* [online]. © Cambridge University Press [citat 15.01.2019]. Disponibil: https://dictionary.cambridge.org/dictionary/english/gap-analysis

73. GAP Analysis: Determine the Success [online]. *Arafiandi blog*, November 14, 2015 [citat 15.01.2019]. Disponibil: https://arafiandi.wordpress.com/2015/11/14/gap-analysis-determine-the-success/

74. GDPR could see Irish organisations face heavy fines in the future. In: *Sunday Business Post*, Mar 10, 2017 [citat 15.01.2019]. Disponibil. https://search-proquest-com.am.e-nformation.ro/docview/1901470819?accountid=136549

75. GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation. In: *Computer Law & Security Review*, 2018, vol. 34, no. 2, pp. 279-288 [citat 11.01.2019]. Disponibil: DOI: 10.1016/j.clsr.2017.12.003

76. GRIERSON, Jamie, GIBBS, Samuel. NHS cyber-attack causing disruption one week after breach. In: *The Guardian*. 2017, 19 May [citat 11.01.2019]. Disponibil: https://www.theguardian.com/society/2017/may/19/nhs-cyber-attack-ransomware-disruption-breach

77. HERAVI, Alireza, MUBARAK, Sameera, CHOO, Kim-Kwang Raymond. Information privacy in online social networks: Uses and gratification perspective. In. *Computers in Human Behavior*. 2018, vol. 84, pp. 441-459 [citat 15.01.2019]. Disponibil: DOI: 10.1016/j.chb.2018.03.016

78. HRNČIAR, Miroslav. Gap analysis of approaches to implementation of management systems. In: *Proceedings of the Scientific Conference Qualita and Leading Innovation 2014*, Košice, Hradec Králové, September 19-20, 2014, pp. 52-61 [citat 11.01.2019]. ISBN 978-80-553-1815-8. Disponibil: DOI: 10.12776/QALI.V1.#5

79. ISO 27001:2013 Toolkit [online] *Qualsys*, © 2018 [citat 11.01.2019]. Disponibil: https://quality.eqms.co.uk/iso-27001-toolkit-transition?submissionGuid=167386ef-d575-471e-8119-94507e62a890

80. *ISO-27001 Compliance* [online]. Gap Analysis. © Risk Factory, 2019 [citat 11.01.2019]. Disponibil: https://www.riskfactory.com/AllServices/ISO27001ComplianceGapAnalysis/

81. *ITIL Continual Service Improvement: 2011 (Best Management Practices).* The Stationery Office, 2011. ISBN: 978-0113313082

82. KAPLAN, R.S., NORTON, D.P. Mastering the Management System. In: *HBS Centennial. Harvard Business Review.* 2008, vol. 86, no. 1, pp. 62-77 [citat 15.01.2019]. Disponibil: https://hbr.org/2008/01/mastering-the-management-system

83. KARABACAK, Bilge, Sogukpinar, Ibrahim. A quantitative method for ISO 17799 GAP analysis. In: *Computers and Security Journal*. 2006, vol. 25(6), pp. 413–419. [citat 15.01.2019]. Disponibil: DOI: 10.1016/j.cose.2006.05.001

84. KLAHR, Rebecca et al. *Cyber Security Breaches Survey: Main report. Department for Digital, Culture, Media & Sport*, 19 April 2017. [citat 15.01.2019]. Disponibil: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

85. KURNIANTO, Ari, ISNANTO, Rizal, PUJI WIDODO, Aris. Assessment of Information Security Management System based on ISO/IEC 27001:2013 On Subdirectorate of Data Center and Data Recovery Center in Ministry of Internal Affairs. In: *The 2nd International Conference on Energy, Environmental and Information System (ICENIS 2017)*. E3S Web of Conferences, 2018, vol. 31, art. no. 11013 [citat 15.01.2019]. Disponibil: DOI: 10.1051/e3sconf/20183111013

86. LACHAUD, Eric. Why the certification process defined in the General Data Protection Regulation cannot be successful. In: *Computer Law & Security Review*. 2016, vol. 32, no. 6, pp. 814–826 [citat 15.01.2019]. Disponibil: DOI: 10.1016/j.clsr.2016.07.001

87. LAMB, Christopher Charles, HEILEMAN, Gregory L. Content-centric Information Protection in Cloud Computing. In: *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*. 2012, vol.: 2, no. 1, pp. 28-39 [citat 15.01.2019]. Disponibil: DOI: 10.11591/closer.v2i1.1615

88. NANDA, V. *Quality Management System Handbook for Product Development Companies*. Boca Raton: CRC Press Book, 2005. eISBN: 978-1420025309

89. NYKÄNEN, Riku, HAKULI, Mikko. Information Security Management System Standards: A gap Analysis of the Risk Management in ISO 27001 and KATAKRI. In: *European Conference on Information Warfare and Security*: *ECIW 2013*. Academic Conferences Limited, 2013, pp. 344-350. ISBN: 978-1-909507-34-0.

90. Parlamentul European. Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (Text cu relevanță pentru SEE). In: *Jurnalul Oficial al Uniunii Europene*, 2016, L 119, vol. 59, pp. 1-88 [citat 15.01.2019]. ISSN 1977-0782. Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32016R0679

91. PAVLOU, Paul A. State of the Information Privacy Literature: Where Are We Now and Where Should We Go? In: *MIS Quarterly*. 2011, vol. 35, no. 4, pp. 977-988 [citat 15.01.2019]. Disponibil: DOI: 10.2307/41409969

92. PICARD, M., RENAULT, A., BARAFORT, B., CORTINA, S. Measuring readiness for compliance: a gap analysis tool to complete the TIPA process assessment framework. In: KREINER, C., O'CONNOR, R.V., POTH, A., MESSNARZ, R. (eds.) *EuroSPI 2016. CCIS*.Cham: Springer, 2016, vol. 633, pp. 106-116 [citat 15.01.2019]. Disponibil: DOI: 10.1007/978-3-319-44817-6_9

93. POULLET, Yves. Is the general data protection regulation the solution? In: *Computer Law & Security Review*. 2018, vol. 34, no. 4, pp. 773-778 [citat 15.01.2019]. Disponibil: DOI: 10.1016/j.clsr.2018.05.021

94. REID, R. D. Benefit Without a Doubt. In: *Quality Progress*. 2010, no. 11 [citat 15.01.2019]. Disponibil: http://asq.org/quality-progress/2010/11/benefit-without-a-doubt.html

95. RODRIGUES, R., BARNARD-WILLS, D., de HERT, P., PAPAKONSTANTINOU, V. The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR", In: *International Review of Law, Computers & Technology, Taylor & Francis*. 2016, vol. 30, no. 3, pp. 248–270 [citat 15.01.2019]. Disponibil: DOI: 10.1080/13600869.2016.1189737

96. SALBU, Steven R. The European Union Data Privacy Directive and International Relations. In: *William Davidson Working Paper*. 2001, no. 418 [citat 15.01.2019]. Disponibil: https://core.ac.uk/download/pdf/3103205.pdf

97. SCHNEIDER, Jennifer, Romanowski,Carol, Mishra, Sumita,. Raj, Rajendra K., Dobie, Sarah. Building robust risk management as a method of situational awareness at the local level. In: *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, 23-24 Oct. 2018, Woburn, MA, USA. Woburn: IEEE, 2018 [citat 15.01.2019]. eISBN: 978-1-5386-3443-1. Disponibil: DOI: 10.1109/THS.2018.8574167

98. Security firm hijacks high-profile Twitter accounts [online]. In: *BBC News*. 2018, 28 December [citat 15.01.2019]. Disponibil: https://www.bbc.com/news/technology-46700995?intlink_from_url=https://www.bbc.com/news/topics/cp3mvpdp1r2t/cyber-attacks&link_location=live-reporting-story

99. SEERDEN, Xander, SALMELA, Hannu, RUTKOWSKI, Anne-Françoise. Privacy Governance and the GDPR: How Are Organizations Taking Action to Comply with the New Privacy Regulations in Europe? In: de WAAL, Benny M.E, RAVESTEIJN, Pascal (eds). *Proceedings of the 14th Conference on Management, Leadership and Governance*, HU University of Applied Sciences, Utrecht, Netherlands 18 - 19 October 2018. Reading: Academic Conferences and publishing limited, 2018, pp. 371-378. ISBN: 978-1-912764-02-0.

100. SHAH, Bhaumik. ISO 27001 Gap Assessment and Risk Assessment: What's the Difference? [online]. *Pivot Point Security*, Jan 12, 2016 [citat 15.01.2019]. Disponibil: https://www.pivotpointsecurity.com/blog/difference-between-iso-27001-gap-assessment-risk-assessment/

101. SIPONEN, M., WILLISON, R. Information security management standards: Problems and solutions. In: *Information & Management*. 2009, vol. 46, no. 5, pp. 267-270 [citat 15.01.2019]. Disponibil: DOI: 10.1016/j.im.2008.12.007

102. SMITH, H. Jeff, DINEV, Tamara, XU, Heng. Information Privacy Research: An Interdisciplinary Review. In: *MIS Quarterly*. 2011, vol. 35, no. 4, pp. 989-1015 [citat 15.01.2019]. Disponibil: DOI: 10.2307/41409970

103. Step Plan GDPR Implementation [online]. *Taylor Wessing,* 17 February 2017 [citat 15.01.2019]. Disponibil: https://deutschland.taylorwessing.com/en/step-plan-gdpr-implementation

104. VALDEVIT, Thierry, Mayer, Nicolas, Barafort, Béatrix. Tailoring ISO/IEC 27001 for SMEs: A Guide to Implement an Information Security Management System in Small Settings. In: O'Connor R.V., Baddoo N., Cuadrago Gallego J., Rejas Muslera R., Smolander K., Messnarz R. (eds) *Software Process Improvement. EuroSPI 2009*. Communications in Computer and Information Science, vol 42. Berlin, Heidelberg: Springer, 2009, pp 201-212 [citat 15.01.2019]. eISBN 978-3-642-04133-4. Disponibil: DOI: 10.1007/978-3-642-04133-4_17

105. VALDEVIT, Thierry, MAYER, Nicolas. A Gap Analysis Tool for SMEs Targeting ISO/IEC 27001 Compliance. In: *Proceedings of the 12th International Conference on Enterprise Information Systems*, ISAS, Funchal, Madeira, Portugal, June 8 - 12, 2010, vol. 3 [citat 16.01.2019]. Disponibil: http://www.nmayer.eu/publis/ICEIS10%20-%20Gap%20analysis%20tool%20for%20SMEs.pdf

106. VOSS, W. Gregory. European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield and the Right to Delisting. In: *Business Lawyer*. 2016, vol. 72, pp. 221–234 [citat 15.01.2019]. Disponibil: https://ssrn.com/abstract=2894571

107. WALCZUCH, Rita M., STEEGHS, Lizette. Implications of the new EU Directive on data protection for multinational corporations. In: *Information Technology & People*. 2001, vol. 14, no. 2, pp. 142-162 [citat 15.01.2019]. Disponibil: DOI: 10.1108/09593840110695730

108. What is an ISO 27001 gap analysis? [online]. *Noticebored*, Jul 7, 2016. Disponibil: https://blog.noticebored.com/2016/07/what-is-iso-27001-gap-analysis.html

109. Wonga data breach 'affects 245,000 UK customers' [online]. In: *BBC News*, 2017, 9 Aprilie [citat 15.01.2019]. Disponibil: https://www.bbc.com/news/business-39544762

110. WOOLLVEN, Camden. 5 key benefits of an ISO 27001 gap analysis [online]. *IT Governance Blog,* 10th August 2018 [citat 15.01.2019]. Disponibil: https://www.itgovernance.co.uk/blog/5-key-benefits-of-an-iso-27001-gap-analysis

111. ZEADALLY, Sherali, BADRA, Mohamad. *Privacy in a Digital, Networked World: Technologies, Implications and Solutions.* New York: Springer, 2015 [citat 15.01.2019]. eISBN 978-3-319-08470-1 Disponibil: DOI: https://doi-org.am.e-nformation.ro/10.1007/978-3-319-08470-1

REZUMAT

Teza de doctorat Cercetări privind implementarea Sistemelor de Management al Securității Informațiilor în arhivele digitale își propune să analizeze metodele și mijloacele de implementare a unui Sistem de Management al Securității Informațiilor (ISMS) în organizații, indiferent dacă acestea sunt publice sau private, precum și de mediul în care evoluează. În acest sens, prin prezenta lucrare se vor analiza atât standardul internațional de securitate a informației, ISO/IEC 27001:2013, cât și prevederile Regulamentului nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (GDPR).

Lucrarea este structurată în șase capitole și evidențiază avantajele implementării unui Sistem de Management al Securității Informațiilor în organizații, prezentând totodată principalele proceduri pe care le implică procesul de implementare și certificare. Necesitatea acestora a fost evidențiată atât prin analiza stadiului actual al cercetării, cât și prin rezultatele cercetării statistice. Totodată, cercetarea actuală prezintă elemente de originalitate, în raport cu obiectivele asumate, dintre acestea cel mai important fiind instrumentul de analiză GAP pentru verificarea simultană a conformității, atât cu ISO 27001, cât și cu GDPR.

ABSTRACT

The doctoral thesis "Research on the implementation of Information Security Management Systems in digital archives" aims to analyze the methods and means of implementing an Information Security Management System (ISMS) in organizations, whether they are public or private, or by the environment in which they evolve. In this sense, this paper will analyze both the international standard of information security, ISO / IEC 27001: 2013, and the provisions of Regulation no. 679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR).

The paper is structured in six chapters and highlights the advantages of implementing an Information Security Management System in organizations, while presenting the main procedures involved in the implementation and certification process. Their need was highlighted both by the analysis of the current state of research and by the results of statistical research. At the same time, the current research proposes a series of original contributions, in relation to the assumed objectives, of these the most important being the GAP analysis tool for the simultaneous verification of compliance, both with ISO 27001 and with GDPR.