

ACADEMIA DE STUDII ECONOMICE DIN BUCUREȘTI

Școala Doctorală Administrarea Afacerilor I



TEZĂ DE DOCTORAT

Prezentată și susținută public de către autor:

Michael Matthias Naumann

Titlul tezei de doctorat:

**CERCETARE PRIVIND ÎMBUNĂTĂȚIREA
EVALUĂRII MATURITĂȚII MANAGEMENTULUI
SECURITĂȚII INFORMAȚIILOR ÎN RAPORT CU
RISCURILE DE SUSTENABILITATE ÎN
PROCESELE DE AFACERI**

**Conducător științific: Prof. univ. Dr. Doru Alexandru
Plesea**

Comisia de susținere a tezei de doctorat:

București, April 2026

a) Cuprins

LISTA CUPRINS

ABSTRACT	3
REZUMAT.....	4
DEDICARE.....	5
CUPRINS	6
LISTA ABREVIERILOR	10
LISTA FIGURILOR	13
LISTA TABELELOR	14
INTRODUCERE.....	16
1 ABORDĂRI ACTUALE ALE SISTEMULUI DE MANAGEMENT AL SECURITĂȚII INFORMAȚIEI ȘI CERINȚELE ÎN CONTEXTUL PROCESELOR DE AFACERI DURABILE	21
1.1 Considerarea istorică a sistemelor de management al securității informațiilor	21
1.1.1 Sisteme de Management al Securității Informațiilor.....	23
1.1.2 Standardizarea securității informațiilor	25
1.2 Securitatea Informației, Inteligența Artificială și Reziliența	26
1.2.1 Inteligență artificială	27
1.3 Securitatea informațiilor în contextul Industriei 4.0.....	36
2 SISTEME DE MANAGEMENT AL SECURITĂȚII INFORMAȚIEI ȘI SUSTENABILITATE	41
2.1 Sustenabilitate și economie circulară	41
2.1.1 Sustenabilitatea ca parte a afacerii	41
2.1.2 Conceptul economiei circulare.....	44
2.2 Riscuri de sustenabilitate în procesele de afaceri	46
2.3 Dezvoltări actuale în domeniul integrării sustenabilității cu sistemele de management al securității informațiilor.....	53
3 MĂSURAREA MATURITĂȚII ÎN SISTEMELE DE MANAGEMENT AL SECURITĂȚII INFORMAȚIILOR.....	63
3.1 Modele de maturitate și niveluri pentru măsurarea maturității.....	63
3.2 Standarde pentru măsurarea securității informațiilor	68

3.3	Metrici și metrici ale Sistemului de Management al Securității Informației..	73
3.3.1	Standarde pentru Metrici de Securitate	73
3.3.2	Standarde pentru măsurarea maturității în securitatea informațiilor	78
4	ANALIZA SISTEMELOR DE MANAGEMENT AL SECURITĂȚII INFORMAȚIEI ÎN CONTEXTUL ECONOMIEI CIRCULARE, SUSTENABILITĂȚII ȘI RESPONSABILITĂȚII SOCIALE CORPORATIVE.....	80
4.1	Analiza securității informațiilor în procesele de afaceri în contextul economiei circulare	80
4.1.1	Contextul analizei, cadrul de cercetare	80
4.1.2	Obiectivele Metodei de Cercetare și Cercetare	80
4.1.3	Rezultatele analizei	82
4.2	Analiza securității informațiilor în procesele de afaceri în contextul Industriei 5.0	88
4.2.1	Contextul analizei, cadrul de cercetare	88
4.2.2	Obiectivele metodei de cercetare	89
4.2.3	Rezultatele studiului	92
4.3	Analiza securității informațiilor în procesele de afaceri în termeni de sustenabilitate și responsabilitate pentru mediu.....	96
4.3.1	Contextul cadrului de analiză și cercetare	96
4.3.2	Obiectivele metodei de cercetare	96
4.3.3	Rezultate și analiză	102
5	ANALIZA MATURITĂȚII PROCESELOR, CONFORMITĂȚII ȘI RISCURILOR ÎN SISTEMELE DE MANAGEMENT AL SECURITĂȚII INFORMAȚIEI	105
5.1	Analiza maturității proceselor și conformității sistemelor de management al informațiilor	105
5.1.1	Contextul analizei.....	105
5.1.2	Obiectivele cercetării și metodei de cercetare	107
5.1.3	Rezultatele analizei maturității proceselor și conformității sistemelor de management al informațiilor.....	108
5.2	Evaluarea conformității sistemelor de management al securității informației cu cerințele standardelor internaționale	120
5.2.1	Contextul cercetării	120
5.2.2	Obiectivele cercetării și metodei de cercetare	123
5.2.3	Rezultatele evaluării conformității sistemelor de management al securității informațiilor cu cerințele standardelor internaționale	126
5.3	Analiza riscurilor în sistemele de management al securității informațiilor..	135

5.3.1	Contextul analizei.....	135
5.3.2	Obiectivele cercetării și metodei de cercetare.....	138
5.3.3	Rezultatele analizei riscurilor în sistemele de management al securității informației	141
6	EVALUAREA SECURITĂȚII INFORMAȚIILOR ȘI A MATURITĂȚII PROCESELOR ÎN SISTEMELE DE MANAGEMENT AL SECURITĂȚII INFORMAȚIEI ÎN COMPANII	151
6.1	Analiza abordărilor actuale pentru evaluarea securității informațiilor în companii	151
6.1.1	Contextul analizei.....	151
6.1.2	Obiective de cercetare și metodă de cercetare	152
6.1.3	Rezultatele analizei abordărilor actuale pentru evaluarea securității informațiilor	153
6.2	Evaluarea maturității proceselor în sistemele de management al securității informației în cadru companiilor.....	161
6.2.1	Contextul cercetării	161
6.2.2	Obiective de cercetare și metodă de cercetare	163
6.2.3	Rezultate și măsuri recomandate.....	169
7	POSSIBILITĂȚI DE ÎMBUNĂTĂȚIRE PENTRU MĂSURAREA MATURITĂȚII SISTEMELOR DE MANAGEMENT AL SECURITĂȚII INFORMAȚIEI ȚINÂND CONT DE SUSTENABILITATE	171
7.1	Principii și aspecte generale ale potențialelor îmbunătățiri în măsurarea maturității	171
7.2	Dezvoltarea unei noi cifre cheie, "Indicele de Securitate a Informațiilor și Sustenabilitate", pentru măsurarea maturității sistemelor de management al securității informațiilor.	173
7.2.1	Determinarea nivelurilor de maturitate	187
7.3	Evaluarea efectelor figurii-cheie propuse pentru procesele de afaceri în sistemele de management al securității informațiilor	188
7.3.1	Implementarea matricei de evaluare	190
	CONCLUZII	196
	BIBLIOGRAFIE	206
	ANEXA.....	227
	Anexa 1: Intervievarea companiilor privind riscurile sistemului de management și constatările auditului.....	228
	Anexa 2: Rezultate anonimizate cu detalii despre sistemele de management ale companiilor auditate	230
	Anexa 3: Feedback-ul sondajului pentru noua metrică ISSI în companie	231

Anexa 4: Exemplu de matrice de calcul într-o companie selectată.....	232
Anexa 5: Matricea de calcul pentru 20 de companii auditate	244
ANEXE	249
Anexa 1: Lista publicațiilor autorului	249

b) Cuvinte cheie

sisteme de management al securității informației, riscuri de sustenabilitate, maturitatea sistemelor de management al securității informației, responsabilitate socială corporativă, procese de afaceri.

c) Rezumat

Teza de doctorat abordează posibilitățile de îmbunătățire a evaluării maturității sistemului de management al securității informației în ceea ce privește riscurile de sustenabilitate în procesele de afaceri. Punctul de plecare îl reprezintă analiza abordărilor actuale ale sistemelor și cerințelor de management al securității informației în contextul proceselor de afaceri sustenabile. Pe această bază, sistemele de management al securității informației și sustenabilitatea, precum și măsurarea maturității sistemelor de management al securității informației sunt cercetate în detaliu.

Cercetarea doctorală se concentrează în continuare pe analiza sistemelor de management al securității informației în contextul economiei circulare, sustenabilității și responsabilității sociale corporative, precum și pe analiza maturității proceselor, conformității și riscurilor în sistemele de management al securității informației. Evaluarea securității informațiilor și a maturității proceselor în sistemele de management al securității informației din companii a fost, de asemenea, studiată. Pe baza rezultatelor cercetării și a experienței în domeniu a doctorandului, accentul este pus pe îmbunătățirea maturității sistemelor de management al securității informațiilor, în special în ceea ce privește sustenabilitatea ca element strategic pentru îmbunătățirea performanței corporative.

În acest scop se dezvoltă o metodă originală de măsurare cu o nouă metrică pentru a identifica oportunități de îmbunătățire în măsurarea maturității sistemelor de management al securității informației, cu accent pe sustenabilitate. Metoda de măsurare propusă a fost testată în practică, cu date colectate din rezultatele auditurilor efectuate și prin aplicarea metodei la o companie selectată.

Ca urmare a cercetării, doctorandul oferă soluții pentru implementarea unui nou indicator, bazat pe cerințele standardelor de securitate a informațiilor, combinate cu cerințele de mediu, sociale și de guvernare. Sunt evidențiate avantajele, limitările și restricțiile aplicării abordării propuse, împreună cu

potențialele oportunități de dezvoltare viitoare.

O prezentare transparentă a stării actuale de securitate a informațiilor din procesele de afaceri, luând în considerare cele mai noi cerințe și tehnologii noi, facilitată de colectarea și utilizarea datelor în toate domeniile de afaceri și de viață, este esențială atât pentru competitivitate, cât și pentru nevoile de cercetare ale modelelor de afaceri actuale. Pentru a îndeplini atât cerințele de reglementare, cât și cele economice, trebuie luate în considerare subiecte suplimentare dincolo de operațiunile IT pure. Acestea includ, în contextul actual, problema sustenabilității, care cuprinde aspecte de mediu, sociale și de guvernare. Combinarea acestor două subiecte ca factori centrali a fost abordată treptat.

Pentru a răspunde la întrebarea de cercetare și a obține perspective empirice, au fost aplicate diverse abordări de cercetare. Acest aspect a fost examinat suplimentar prin evaluarea maturității proceselor și a conformității în cadrul sistemului de management al securității informațiilor, confirmând astfel conformitatea cu cerințele definite. Au fost realizate studii, iar o cifră cheie pentru evaluare a fost dezvoltată. Această cercetare doctorală a analizat inițial partea teoretică, incluzând cercetări privind implementările actuale ale securității IT în raport cu sustenabilitatea, identificarea riscurilor, integrarea sustenabilității în Sistemele de Management al Securității Informației și măsurarea maturității în cadrul Sistemelor de Management al Securității Informaționale. Contribuțiile proprii la cercetare au fost analiza securității informației în ceea ce privește economia circulară, sustenabilitatea și aspectele etice, urmată de o analiză a maturității proceselor, conformității și riscurilor în Sistemele de Management al Securității Informațiilor, precum și o evaluare a securității informațiilor și maturității în companii. Obiectivul final al acestei teze doctorale a fost atins prin dezvoltarea unei măsurători îmbunătățite folosind o figură cheie pentru maturitatea proceselor, cu accent pe securitatea informațiilor și sustenabilitate. Secțiunile următoare oferă un rezumat detaliat al punctelor cheie și rezultatelor pentru fiecare subiect.

Analiza abordărilor actuale ale sistemelor și cerințelor de management al securității informațiilor în contextul proceselor de afaceri durabile a oferit o privire de ansamblu asupra standardelor actuale de securitate a informațiilor și a integrării acestora în sistemele de management. A arătat cum cerințele în schimbare și creșterea obiectivelor de protecție pentru informații sunt determinate de evoluțiile tehnologice. Aceasta evidențiază faptul că atât inovația, cât și amenințările emergente legate de date subliniază importanța lor strategică pentru companii. Mai mult, a explicat necesitatea adaptării proceselor de afaceri și standardelor internaționale pentru a îndeplini cerințele minime, asigurând că măsurile de securitate a informațiilor sunt comparabile și conforme din punct de vedere legal. Cercetarea a arătat că noile subiecte legate de procesarea datelor și inteligența artificială trebuie să fie aliniate cu reglementările și cadrele legale relevante pentru a ajuta companiile să respecte standardele etice, legale și tehnice. Mai mult, a examinat relația dintre reziliența proceselor de afaceri și sistemele IT, având în vedere securitatea

informațiilor și inteligența artificială. Discuția a abordat, de asemenea, Industria 4.0 și rețelistica sistemelor și mașinilor prin Internetul Lucrurilor (IoT) ca principal factor tehnic. În acest context, relația dintre securitatea informației, inteligența artificială și menținerea lanțurilor de aprovizionare în producție și industrie a fost discutată în detaliu.

Pentru *Sistemele de Management al Securității Informațiilor și Sustenabilitate*, au fost analizate și identificate care dependențe și abordări actuale de implementare pentru securitatea IT în raport cu sustenabilitatea. Pentru aceasta, analiza sustenabilității și a economiei circulare a evidențiat importanța pentru companii în termeni de eficiență economică, etică, responsabilitate socială și competitivitate. Au fost abordate și prezentate subiecte critice precum IT verde și securitate cibernetică durabilă. Tehnologia informației a fost analizată în raport cu influența economiei circulare asupra proceselor digitale ale companiilor moderne. Acest cadru evidențiază reînnoirea resurselor, schimbul extins de date, comunicarea securizată și utilizarea eficientă a roboticii și AI. Un alt segment discută riscurile de sustenabilitate și respectarea standardelor UE precum Standardul European de Raportare a Durabilității (ESR), examinând modul în care sustenabilitatea este integrată în proiectele IT.

S-a demonstrat că progresele recente în integrarea sustenabilității cu sistemele de management al securității informațiilor sunt subiecte cruciale care necesită schimbări organizaționale. În plus, utilizarea tehnologiei blockchain în sectorul sustenabilității a fost analizată, iar relevanța aici pentru sustenabilitate a fost demonstrată. Per ansamblu, s-a prezentat că beneficiile combinării eforturilor de sustenabilitate cu sistemele de management al securității informației aduc o eficiență îmbunătățită a resurselor, riscuri reduse, reduceri de costuri și integrarea protocoalelor de securitate.

Măsurarea maturității în sistemele de management al securității informației implică determinarea nivelurilor de maturitate și a caracteristicilor corespunzătoare. S-a analizat că, pe lângă modele și standarde pentru evaluarea maturității generale a proceselor, există și modele specifice pentru evaluarea maturității în securitatea informației. Analiza a relevat că maturitatea poate fi evaluată în cadrul tendințelor emergente precum Industria 4.0, inteligența artificială sau cerințele economiei circulare. Mai mult, au fost prezentate standarde legate de măsurarea securității informațiilor, evidențiind atât asemănările, cât și diferențele. Cercetarea doctorală a identificat care standarde existente și figuri-cheie în domeniul securității informațiilor abordează distincția dintre procese și nivelurile de maturitate. Se poate demonstra că diferite implementări, cerințe și standardizări depind de reglementări din industrie sau generale. Această revizuire a abordărilor actuale oferă o bază pentru cercetări ulterioare.

Cercetarea privind propriile contribuții pentru această cercetare doctorală a fost inițiată prin *Analiza Sistemelor de Management al Securității Informației în contextul Economiei Circulare, Sustenabilității și Responsabilității Sociale Corporative*. Economia circulară și relația sa cu digitalizarea și securitatea

informației influențează și vor continua să influențeze aplicarea economiei circulare în procesele de afaceri. A fost realizată o analiză pentru a identifica care factori sunt în general importanți pentru o economie circulară. Folosind metode de regresie, s-a determinat ce aspecte și perspective economice ar trebui luate în considerare în cazul unei posibile adaptări la nivel național. Pe baza unor exemple de economii circulare existente în țările europene, s-a analizat că se poate atinge un nivel ridicat de reutilizare a resurselor, dar eficiența energetică rămâne îmbunătățibilă. Integrarea IT-ului în cadrul digitalizării lanțurilor de producție, inclusiv automatizarea Industriilor 4.0 și 5.0, a condus la concluzia că există un potențial semnificativ în cadrul companiilor pentru sustenabilitate și economie circulară. Analizele și sondajele realizate de Comisia Europeană au demonstrat că majoritatea companiilor au o atitudine pozitivă față de tehnologia digitală în ceea ce privește impactul său asupra mediului.

Se poate concluziona, de asemenea, că practicile eficiente ale economiei circulare în întreprinderile mici și mijlocii pot fi realizate, spre deosebire de companiile mari în contextul transformării digitale, și modul în care acest lucru poate fi evaluat în diverse industrii. Pe baza acestui lucru, subiectul Industriei 5.0 a fost luat în considerare ca parte a transformării industriale. Din perspectiva Uniunii Europene, accentul este pus pe sustenabilitatea oamenilor, a planetei și reziliență. Distincția dintre Industria 4.0, care pune accent pe fabricile inteligente, tehnologia senzorilor și sistemele flexibile de producție, și dezvoltarea către Industria 5.0, care implică interacțiunea directă între oameni, mașini și robotică prin inteligență artificială, a fost evidențiată. Pe măsură ce utilizarea resurselor și eficiența costurilor devin tot mai importante în acest context, luarea în considerare a sustenabilității și a economiei circulare este crucială. Tehnologiile noi precum Modelarea Informațiilor pentru Clădiri (BIM) iau în considerare atât factorii de securitate a informațiilor, cât și alte subiecte nefuncționale, cum ar fi impactul climatic și al mediului. Aceasta include aspecte precum durabilitatea și siguranța în industria construcțiilor, care sunt considerate elemente ale sustenabilității. Din această perspectivă, Industria 5.0 își propune să susțină întregul ciclu de viață al clădirilor, luând în considerare consumul de resurse și reutilizarea materialelor de construcție. Fără o digitalizare suplimentară în sectorul construcțiilor, susținută de conceptele modelului Industry 5.0, o cale sustenabilă către economia circulară și optimizarea reciclării poate fi realizată doar într-o măsură limitată.

Ca un domeniu suplimentar de cercetare, integrarea subiectelor de sustenabilitate în industrii definite, cum ar fi sectorul imobiliar, a arătat că aceste sectoare trebuie să susțină și cerințele ecologice și sociale în evoluție prin progrese tehnologice. Așa-numita dezvoltare imobiliară durabilă trebuie să ia în considerare eficiența energetică, reducerea deșeurilor și conservarea diversității biologice. Mai mult, aspectele economice precum reducerea costurilor și competitivitatea trebuie echilibrate. Tema securității informației va juca un rol din ce în ce mai important în domenii precum construcțiile, calculul resurselor și în etapele

ulterioare ale managementului și automatizării clădirilor. Atingerea obiectivelor de sustenabilitate și reducerea costurilor prin utilizarea tehnologiilor avansate precum inteligența artificială sau Industria 5.0 poate avea succes doar cu o protecție tot mai mare a datelor și informațiilor digitale.

Prin *Analiza Maturității Proceselor, Conformității și Riscurilor în Sistemele de Management al Securității Informațiilor* s-a demonstrat unde apar lacune în cadrul companiilor chiar și după câțiva ani de implementare a Sistemelor de Management al Securității Informației (ISMS), și de ce acestea nu pot fi închise sau care sunt obstacolele. S-a constatat că atât executarea sarcinilor regulate, de exemplu anuale de rutină, cum ar fi urmărirea sarcinilor, corectarea constatărilor auditului, cât și instruirea angajaților sunt domenii în care pot apărea lacune în timp din cauza planificării manuale sau a lipsei de supraveghere. Se poate demonstra, de asemenea, că numărul de subiecte scade după primii ani de audituri de certificare, apoi atinge un anumit platou și rămâne acolo. Chiar și după mai bine de zece ani, neconformitățile erau încă identificate în domenii care ar trebui gestionate pe deplin în cadrul companiilor examinate. Cauzele pentru aceasta au inclus probleme tehnice de implementare, necesitatea unei documentări îmbunătățite a noilor procese și schimbări organizaționale. O problemă centrală este și interacțiunea umană, deoarece lipsa de conștientizare a angajaților conduce la riscuri semnificative pentru securitatea informațiilor despre date. S-a constatat că și dimensiunea companiei joacă un rol. Companiile mici și mari gestionează sarcinile sistemului de management mult mai eficient decât companiile de dimensiuni mijlocii. Ca concluzie, a fost definit un set de măsuri care urmăresc creșterea revizuirilor interne ale sistemelor de management al securității informației (ISMS), implementarea planificării sistematice a măsurilor, îmbunătățirea gradului de conștientizare și realizarea unei supravegheri mai bune a obiectivelor de securitate a informațiilor prin cifre-cheie și niveluri de maturitate. Cercetările suplimentare au analizat subiectul riscurilor și implementarea securității informațiilor în așa-numitele infrastructuri critice, cum ar fi gestionarea energiei sau companiile din industria apei. Aici, o defecțiune a infrastructurii controlate de IT ar duce la probleme serioase în aprovizionarea companiilor și gospodăriilor. În Germania, aceste companii sunt, prin urmare, supuse cerințelor de dovadă sau certificare. Aceste verificări regulate sunt efectuate prin audituri realizate de organisme externe de certificare. Evaluările rezultate, sub forma constatărilor auditului, oferă perspective atât asupra implementării eficiente a cerințelor, cât și asupra comparației cu companiile din sectorul privat în ceea ce privește infrastructura critică reglementată.

În timpul auditurilor, angajații companiei sunt intervievați, iar concluziile privind implementarea se trag pe baza documentelor și inspecțiilor la fața locului. De asemenea, aici trebuie luată în considerare o evaluare a diferitelor domenii ale standardelor internaționale, cum ar fi ISO/IEC 27001. Faptul că acestea constau în principal în cerințe de nivel înalt din sistemul dumneavoastră de management este considerat mai important decât măsurile ulterioare, care abordează cerințele tehnice, organizaționale, de personal și

de securitate fizică și specifică proceduri mai concrete. În plus, operatorii de infrastructură critică trebuie să îndeplinească cerințe suplimentare, de exemplu pentru alimentarea cu energie, conform ISO/IEC 27019. De asemenea, s-a constatat că majoritatea neconformităților atât în companiile critice, cât și în cele necritice se încadrează în cerințele tehnice, organizaționale sau de personal ale cadrului ISO 27001. Mai mult, a fost identificat un număr mai mare de neconformități la toate companiile examinate din operatorii necritici și, prin urmare, mai puțin reglementați. O analiză detaliată a relevat că principalele motive includ o conștientizare mai ridicată a riscului în sectorul infrastructurii critice în rolul de furnizor, o presiune publică mai mare, cadrul de reglementare și, în consecință, o conștientizare îmbunătățită a securității.

Cercetări suplimentare privind analiza conformității și maturității în sistemele existente de management al securității informațiilor au fost efectuate în ceea ce privește managementul riscurilor ca componentă centrală în gestionarea securității informaționale. În acest scop, un număr definit de companii au fost chestionate cu privire la practicile lor de management al riscului. Pe lângă metodele sau cadrele folosite, au fost examinate în detaliu procedurile de identificare, evaluare și tratare a riscurilor identificate. Mai mult, documentarea sistemelor utilizate și principalele riscuri identificate la final au servit ca bază pentru colectarea datelor. În cadrul companiilor, mai mult de jumătate au adoptat o abordare de management al riscului bazată pe un standard. În plus, s-ar putea face o distincție între o metodologie standardizată a riscului și una bazată pe active, diferența constând în faptul dacă riscurile sunt luate în considerare pentru procesele de afaceri sau în evaluarea detaliată a riscurilor pentru activele companiei. Au existat, de asemenea, diferențe în investigații privind analizele calitative sau cantitative ale riscului, companiile chestionate folosind predominant o strategie calitativă în funcție de dimensiunea lor și de sistemele și resursele disponibile. Următoarele probleme și provocări în managementul riscurilor au fost identificate în companiile chestionate. O problemă centrală este selecția metodologiei de risc sau adaptarea acesteia la cerințele modelelor de afaceri ale companiilor. Un alt aspect esențial este lipsa unei abordări structurate pentru identificarea riscului.

Odată ce riscurile sunt identificate, următorul pas este evaluarea și evaluarea criticității acestora. Cercetarea a arătat că companiile chestionate aplică adesea abordări incorecte sau inadecvate din cauza lipsei unor cerințe specifice în cadrul standardelor de securitate a informațiilor, cum ar fi ISO 27001. Din cauza absenței standardizării, a fost stabilită și propusă o procedură structurată în cercetare. Deoarece analiza riscurilor, așa cum a fost identificată în rezultatele cercetărilor anterioare, reprezintă un punct principal de referință pentru abateri și neconformități în timpul auditurilor, este necesară o concentrare pe această zonă în cadrul sistemului de management al securității informaționale.

Evaluarea securității informațiilor și a maturității proceselor în sistemele de management al securității informației din companii a arătat că, după analiza cu succes a neconformităților și riscurilor din

procesele de afaceri ale sistemelor de management al securității informației (ISMS) și pentru a obține o perspectivă holistică asupra proceselor generale în legătură cu securitatea informațională, se obțin detalii suplimentare privind maturitatea proceselor în ISMS. Aceasta a implicat o investigație asupra unor companii selectate privind rezultatele auditului, modul în care sunt determinate metricile și cifrele cheie și care sunt măsurate și folosite ca indicatori pentru atingerea obiectivelor de securitate a informațiilor. Au fost identificate criterii pentru colectarea acestor cifre cheie, precum frecvența utilizării standard, suportul sistemului și abaterile din audituri legate de monitorizarea lipsă prin cifrele cheie. Figurile cheie din sistemele de management sunt fundamental importante deoarece permit măsurarea și controlul procesului continuu de îmbunătățire din cadrul ciclului PDCA.

În cadrul sistemelor de management al securității informațiilor (ISMS), este necesar să se definească obiective pentru atingerea obiectivelor de protecție — confidențialitatea, disponibilitatea și integritatea informațiilor și datelor — și să se monitorizeze atingerea acestora folosind cifre cheie. O cifră cheie larg utilizată este rata de participare a angajaților la trainingul de conștientizare, un indicator care este revizuit anual în revizuirea managementului împreună cu conducerea executivă. Investigația a determinat câte cifre-cheie sunt folosite în general în cadrul companiei și cât de frecvent sunt măsurate. Mai mult, s-a constatat că majoritatea sistemelor de management au colectarea manuală definită a figurilor cheie. O problemă semnificativă a fost selecția adecvată a figurilor cheie care reflectă cu acuratețe realitatea procesului de afaceri și asigură securitatea informației. Rezultatul studiului a fost că, în absența unor abordări structurate și fără utilizarea unor cifre cheie determinate automat, raportarea este limitată doar în capacitatea sa de a oferi o imagine de ansamblu cuprinzătoare a stării generale a securității informațiilor. Sunt necesare abordări suplimentare, care sunt subiectul unor întrebări suplimentare de cercetare.

Ca parte a unor investigații suplimentare pe această temă, s-a demonstrat că există evaluări de nivel de maturitate în cadrul organizațiilor. Pentru a face acest lucru, structura ISO27001 a fost analizată mai întâi în raport cu o aplicație potențială. Pe baza standardelor pentru evaluarea maturității, cum ar fi modelul CMMI cu cele șase niveluri ale sale sau alte standarde din industrie, a fost identificat și proiectat un model de procedură pentru evaluarea maturității. Așa cum s-a discutat inițial, a trebuit stabilit un regulament pentru ponderarea ariilor individuale ale ISO/IEC 27001, deoarece concluziile din capitolele de audit ale standardului sunt evaluate mai critic decât cele din Anexa A a standardului. Scopul a fost să se dezvolte un calcul pentru un nivel general de maturitate și să se stabilească o valoare minimă pentru acesta, din care să devină clar pentru organizații dacă au atins o conformitate definită cu cerințele și se pot aștepta la mai puține rezultate în audituri. Măsurile recomandate pentru utilizarea unei astfel de evaluări și implementarea ei continuă în cadrul proceselor de îmbunătățire continuă au inclus revizuri regulate și autoevaluări. Modificări ulterioare în această cercetare au dus la rezultate suplimentare și la o

aplicabilitate îmbunătățită în cadrul organizațiilor.

În final, prin această teză de doctorat, s-ar putea sublinia că subiectele legate de securitatea informației prezintă provocări semnificative din cauza includerii tot mai frecvente a unor subiecte precum problemele de sustenabilitate, deoarece complexitatea tot mai mare a sistemelor necesită mai multe date și informații pentru a fi gestionate în siguranță. Diferența existentă constă în prezentarea insuficientă a stării actuale a securității informaționale, combinată cu riscurile legate de sustenabilitate în urmărirea obiectivelor corporative. *Posibilitățile de îmbunătățire pentru măsurarea maturității sistemelor de management al securității informației în considerare* sustenabilitatea sunt rezultatul acestei cercetări doctorale.

Din acest motiv, a fost dezvoltată o mapare a cerințelor din ISO 27001 pentru un Sistem de Management al Securității Informației (ISMS) și cerințele de sustenabilitate ca parte a implementării. Accentul a fost pus pe măsurabilitatea îndeplinirii acestor cerințe prin cifre cheie realizabile și, într-un pas ulterior, pe evaluarea maturității procesului în cadrul cerințelor. Acuratețea dorită a măsurărilor și evaluarea subiectivă a faptului dacă cerințele sunt complet sau doar parțial îndeplinite reprezintă o provocare. Din cauza criticității variabile a cerințelor dintr-un ISMS privind subiectele și problemele capitolelor principale din domeniile tehnice, organizaționale, personale și de securitate fizică ale Anexei A, au fost stabilite criterii diferite de importanță, pe baza cărora au fost calculate ulterior nivelurile de maturitate. Ca concept fundamental pentru evaluarea nivelurilor de maturitate, modelul CMMI a fost utilizat aici. Această abordare face posibilă evaluarea unor domenii individuale ale sistemului de management al securității informațiilor și documentarea separată a evaluării sustenabilității și a nivelului de securitate a informațiilor. Noua figură cheie ISSI analizează cuprinzător relația dintre securitatea informațiilor și implementarea durabilă a cerințelor în domeniile mediului, problemelor sociale și guvernantei. Acest lucru asigură o perspectivă holistică din perspectiva conducerii de top în perioadele regulate de raportare, cum ar fi revizuirea anuală a managementului ISMS. Pentru a testa aplicabilitatea noii abordări și utilitatea noii cifre cheie, a fost realizată o aplicație exemplară într-o companie selectată care operează centre de date în sectorul serviciilor IT, folosind utilizarea durabilă a căldurii reziduale ca unul dintre principalele sale domenii de afaceri. După transmiterea matricei de evaluare, cifrele cheie au fost stabilite, iar nivelurile de maturitate au fost evaluate.

Cifra cheie ISSI calculată a fost discutată cu conducerea pentru perioada curentă de raportare. În plus, compania a examinat evaluarea securității informațiilor folosind criteriile definite și cifrele cheie legate de adaptarea și ajustarea proceselor de afaceri existente. Într-un formular de sondaj de rezumat, au fost oferite contribuții privind îmbunătățirile și dezvoltarea ulterioară a abordării ca feedback. S-au obținut răspunsuri clare și pozitive în ceea ce privește cifra-cheie și abordarea, pentru a obține un indicator care

oferă o perspectivă cuprinzătoare asupra securității informaționale, stadiul conformității înainte de audituri și certificări, precum și implementarea aspectelor de sustenabilitate ca strategie de afaceri și cerință de conformitate în perioadele de raportare.

Ipoteza că o imagine mai bună a metricilor de proces reprezintă mai precis riscurile asociate implementării cerințelor pentru sustenabilitate și securitatea informației, contribuind astfel semnificativ la evitarea sau gestionarea acestora, a fost dovedită în cadrul cercetării. Companiile au în continuare oportunitatea, printr-o cartografiere clară a cerințelor legate de securitatea informațiilor și sustenabilitate, de a ajusta imediat măsurarea atingerii obiectivelor corporative și de a elimina lacunele și riscurile asociate. Pe baza cercetărilor anterioare legate de această activitate, se știe că colectarea cifrelor cheie și, astfel, optimizarea măsurării și atingerii țintite a obiectivelor poate fi implementată doar dacă duce și la creșterea eficienței operaționale în toate ariile de business. Fără a sublinia explicit acest lucru, trebuie menționat că prevenirea incidentelor de securitate care implică scurgeri, pierderi sau compromisuri de date susține, în general, menținerea operațiunilor de afaceri și competitivitatea generală.

În concluzie, cercetarea amplă a literaturii a permis analiza dezvoltării istorice și a stadiului actual al tehnologiei. Aceasta necesită luarea în considerare a cerințelor suplimentare în domeniile securității informațiilor și sustenabilității. Mai mult, au fost analizate instrumente specifice ca factori de implementare a sustenabilității, în special aspectele economice ale economiei circulare, luând în considerare tehnologia informației și protecția informației. Au fost documentate perspective pe baza studiilor și sondajelor. În plus, s-a demonstrat că există relații între riscuri și implementare inadecvată în cadrul procesului de îmbunătățire continuă în companiile sondate și auditate, evidențiind necesitatea urgentă a unei prezentări consecvente a cifrelor cheie și a maturității proceselor. Folosind aceste constatări, au fost examinate și evaluate modelele de maturitate existente și sistemele cu figure-cheie din sistemele de management. După ce a mapat cerințele de sustenabilitate la cerințele standardului ISO/IEC 27001 privind securitatea informațiilor, a apărut necesitatea unei noi cifre cheie, ISSI (Indicele de Securitate a Informațiilor și Sustenabilitate), oferind o perspectivă unificată. De asemenea, a devenit clar că un sistem central de notare folosind metrica ISSI ar putea susține semnificativ atingerea acestor obiective, bazat pe investigațiile companiilor auditate și aplicațiile detaliate.

Această teză de doctorat a demonstrat clar că companiile au nevoie de o perspectivă holistică atât asupra tendințelor actuale legate de securizarea informațiilor, datelor și, implicit, a fundamentelor lor de afaceri, dar acest lucru trebuie făcut acum în combinație cu luarea în considerare a sustenabilității pentru a rămâne competitive.

Ca pas suplimentar pentru cercetări viitoare bazate pe acest aspect, colectarea datelor și a cifrelor cheie ar putea fi, de asemenea, automatizată, controlată de sistem și vizualizată, pe baza feedback-ului rezultatului

implementării exemplare. Aceasta ar reduce efortul manual și ar permite o prezentare în timp real a schimbărilor din nivelul general de maturitate și a figurii-cheie ISSI. Așa cum a menționat compania chestionată, acest efort inițial este în mare parte împiedicat de măsurători inconsistente, lipsa cifrelor și, în consecință, lipsa unei perspective generale în cadrul sistemului de management.

Un alt pas implică luarea în considerare a aspectelor financiare, cum ar fi economiile de costuri rezultate din subiectele de sustenabilitate acum măsurate în securitatea IT operațională și fizică. Reducerea așteptată a riscurilor de securitate, precum și a riscurilor de sustenabilitate, ar putea duce la extinderea modelului, care va fi subiectul cercetărilor viitoare. Acest lucru ar ajuta, de asemenea, la abordarea riscurilor emergente pentru date și informații și pentru cele mai valoroase proprietăți ale companiilor, precum și la pregătirea pentru noi tendințe în digitalizare sau transformare digitală.