

**ACADEMIA DE STUDII ECONOMICE DIN BUCUREȘTI**  
**Școala doctorală de Administrarea Afacerilor**



# **TEZĂ DE DOCTORAT**

Prezentată și susținută public de către autor:

**GEORG SVEN LAMPE**

Titlul tezei de doctorat:

**CERCETĂRI PRIVIND SECURITATEA INFORMAȚIEI ÎN  
PROCESELE DE AFACERI ÎN RELAȚIE CU RISCURILE  
GLOBALE**

Conducător de doctorat: Prof. Univ. Dr. Marieta Olaru

Comisia de susținere a tezei de doctorat:

Prof. Univ. Dr. Cristinel Vasiliu (președinte) - Academia de Studii Economice din București  
Prof. Univ. Dr. Liliana Nicodim (referent) - Universitatea Ovidius din Constanța  
Prof. Univ. Dr. Elena Cerasela Spătariu (referent) - Universitatea Ovidius din Constanța  
Prof. Univ. Dr. Mihaela Maftai (referent) - Academia de Studii Economice din București  
Prof. Univ. Dr. Marieta Olaru (conducător de doctorat) - Academia de Studii Economice din București

București, 2024

## a) Cuprins

### LISTA CUPRINS

<b>LISTA CUPRINS</b>	<b>5</b>
<b>LISTA ABREVIERILOR</b>	<b>11</b>
<b>LISTA FIGURILOR</b>	<b>12</b>
<b>LISTA TABELELOR</b>	<b>13</b>
<b>INTRODUCERE</b>	<b>15</b>
<b>PARTEA I: STADIUL ACTUAL AL CUNOȘTINȚELOR ȘTIINȚIFICE ÎN DOMENIUL CERCETĂRII</b>	<b>26</b>
<b>1. PRINCIPIILE SECURITĂȚII INFORMAȚIILOR ÎN CONTEXTUL RISCURILOR GLOBALE</b>	<b>26</b>
<b>1.1. Principalele obiective ale organizației care vizează construirea performanței organizaționale și crearea unui avantaj competitiv</b>	<b>27</b>
1.1.1. Istoria și definirea managementului securității informatice și cibernetice, continuitatea afacerii și managementul riscurilor	27
1.1.2. Principii și elemente definitorii ale securității informațiilor, confidențialității datelor și obiectivelor de protecție	31
1.1.3. Standarde de risc și elemente de gestionare a riscurilor	34
1.1.4. Elemente și legătura dintre continuitatea afacerii și managementul crizelor	39
<b>1.2. Dependentele și legătura dintre managementul riscurilor și managementul informațiilor și securității cibernetice pentru evaluarea performanței</b>	<b>44</b>
1.2.1. Sistemul de management al securității informaționale și cibernetice în contextul confidențialității, securității, siguranței	44
1.2.2. Cadre strategice la nivelul UE, standarde de securitate informatică și cibernetică, audit și revizuire internă	48
1.2.3. Metode de evaluare a performanței pentru un nivel comun ridicat de gestionare a informațiilor și a securității cibernetice	52
<b>1.3. Stadiul managementului proceselor de afaceri, metode agile</b>	<b>61</b>
1.3.1. Managementul proceselor de afaceri	61

1.3.2. Dependente între managementul proceselor de afaceri și metodologiile agile aplicate la nivel de industrie	66
<b>2. CONECTAREA MANAGEMENTULUI RISCURILOR ÎN SECURITATEA INFORMAȚIEI CU CONTEXTUL MANAGEMENTULUI CONTINUITĂȚII ACTIVITĂȚII</b>	<b>71</b>
<b>2.1. Relevanța evaluării riscurilor infrastructurii tehnologiei informației pentru organizații</b>	<b>72</b>
2.1.1. Factori de risc în securitatea informațiilor și managementul continuității afacerii prin digitalizarea globală	72
2.1.2. Abordări internaționale privind cadrele tradiționale de management al riscurilor pentru securitatea informațiilor, continuitatea afacerii	76
2.1.3. Cadre operaționale aplicate pentru managementul riscurilor în cadrul organizațiilor	87
2.1.4. Rezumat privind utilizarea și limitarea cadrelor de gestionare a riscurilor	92
<b>2.2. Măsurarea maturității eficacității și eficienței în cadrul cadrelor de gestionare a riscurilor</b>	<b>94</b>
2.2.1. Măsurarea eficacității și eficienței gestionării riscurilor	94
2.2.2. Indicatori cheie de performanță în managementul riscurilor	97
2.2.3. Discutarea problemelor de măsurare a riscurilor și a performanței în cadrul cadrelor de gestionare a riscurilor	99
2.2.4. Tendințe actuale în cadrul teoriei și practicii managementului riscului	100
<b>3. INFLUENȚA SISTEMULUI DE MANAGEMENT AL SECURITĂȚII INFORMAȚIEI ÎN CONTEXTUL MANAGEMENTULUI CONTINUITĂȚII AFACERII ASUPRA PROCESULUI DE AFACERI</b>	<b>102</b>
<b>3.1. Relația dintre procesele de afaceri și influența cerințelor de securitate a informațiilor și continuitatea afacerii</b>	<b>103</b>
3.1.1. Prezentare generală a sistemelor de management	103
3.1.2. Tendințe specifice sistemelor de management și rolul normelor internaționale în sistemele de management integrat	105
3.1.3. Cuprinzând studiul proceselor de afaceri și influența cerințelor de securitate a informațiilor și continuitatea afacerii	110
<b>3.2. Factori de influență pentru performanța maturității în sistemele de management neintegrate și integrate</b>	<b>113</b>
3.2.1. Contribuția factorilor de influență, leadership, culturii organizaționale și influenței angajaților	113

3.2.2. Problema măsurării succesului în contextul sistemelor de management	117
3.2.3. Diferențele dintre segmentele industriale și poziția geografică a acestora	120
3.2.4. Rezumatul factorilor de influență pentru performanța sistemelor de management integrat	121
<b>3.3. Subiecte actuale de interes și discuții despre eforturile de evaluare a sistemelor de management în contextul sustenabilității</b>	<b>122</b>
3.3.1. Conectarea dintre procesele de afaceri și sistemele de management folosind	122
3.3.2. Sisteme de management și principii de management al riscului către un management durabil al riscului	123
3.3.3. Tendințe actuale și discuții în ceea ce privește eforturile de evaluare a sistemelor de management în contextul constatărilor de certificare și audit	125
<b>PARTEA II: CONTRIBUȚII PROPRII ÎN DOMENIUL CERCETĂRII</b>	<b>127</b>
<b>4. ANALIZE ALE MATURITĂȚII PROCESELOR DE AFACERI ÎN CONTEXTUL CUNOȘTINȚELOR, SECURITĂȚII INFORMAȚIILOR ȘI MANAGEMENTULUI CONTINUITĂȚII AFACERII, MANAGEMENTULUI RISCURILOR ȘI AGILITĂȚII</b>	<b>127</b>
<b>4.1. Analiza serviciilor gestionate și a factorilor de sustenabilitate, învățarea organizațională și managementul cunoștințelor privind maturitatea firmelor</b>	<b>128</b>
4.1.1. Principalele obiective ale cercetării	128
4.1.2. Metodologia de cercetare și baza de date	128
4.1.3. Rezultatele cercetării serviciilor gestionate și a factorilor de securitate, sustenabilitate, indicatori de performanță pentru învățarea organizațională privind maturitatea firmelor	129
<b>4.2. Cercetarea dependențelor managementului securității informației legate de continuitatea afacerii, caracterizarea impactului afacerii în contextul crizei globale</b>	<b>133</b>
4.2.1. Cercetarea obiectivului principal	133
4.2.2. Metodologia de cercetare și baza de date	135
4.2.3. Rezultatele cercetării dependențelor managementului securității informației legate de continuitatea afacerii, impactul afacerii caracterizându-se în contextul crizei globale	137

<b>4.3. Studiu la nivel de dependențe și perspective strategice în contextul digitalizării, metoda de agilitate adaptată</b>	<b>144</b>
4.3.1.Principalele obiective ale cercetării	144
4.3.2. Metodologia aplicată de cercetare și baza de date	146
4.3.3. Rezultatele cercetării la nivel de dependențe și perspective strategice în contextul digitalizării, metoda de agilitate adaptată	147
<b>5. ANALIZE PENTRU UN CADRU ORGANIZAȚIONAL DE MANAGEMENT AL SECURITĂȚII INFORMAȚIILOR, MĂSURI CLASIFICATE ȘI FACTOR CRITIC DE SUCCES ÎN CONTEXTUL SUSTENABILITĂȚII ȘI SERVICIILOR GESTIONATE</b>	<b>156</b>
<b>5.1. Analiza obiectivelor de protecție, matricea de risc a FMEA adaptată, clasificarea măsurii și evaluarea</b>	<b>157</b>
5.1.1.Principalele obiective ale cercetării	157
5.1.2. Metodologia de cercetare și baza de date	158
5.1.3. Rezultatele cercetării obiectivelor de protecție, matricea de risc a FMEA, clasificarea măsurii și evaluarea	160
<b>5.2. Studiu privind sistemul de politici structurate, rolurile specifice și elementele registrului de risc cibernetic pentru condiționarea procesului de management al riscurilor de securitate cibernetică</b>	<b>168</b>
5.2.1. Principalele obiective ale cercetării	168
5.2.2. Metodologia de cercetare și baza de date a serviciilor gestionate	169
5.2.3. Rezultate privind sistemul de politici structurate, rolurile specifice și elementele de registru de risc cibernetic pentru condiționarea procesului de management al riscurilor de securitate cibernetică	170
<b>5.3. Analiza factorilor critici de succes pentru integrarea unui model de interacțiune circulară pentru procesele de securitate în transformarea digitală</b>	<b>175</b>
5.3.1. Principalele obiective ale analizei: factori critici de succes	175
5.3.2. Metodologia de cercetare și colectarea datelor	176
5.3.3. Rezultatele cercetării factorilor critici de succes pentru integrarea unui model circular de interacțiune pentru procesele de securitate în transformarea digitală	177
<b>6. CERCETAREA ȘI DEZVOLTAREA UNUI MODEL DE MĂSURARE A EFECTELOR SISTEMELOR DE MANAGEMENT ASUPRA</b>	<b>185</b>

<b>PROCESELOR DE AFACERI LUÂND ÎN CONSIDERARE MANAGEMENTUL RISCULUI</b>	
<b>6.1. O analiză cantitativă a rezultatelor auditului sistemului de management pentru a identifica lacunele de cunoștințe ale evaluării performanței sistemului de management</b>	<b>185</b>
6.1.1. Principalele obiective ale analizei	185
6.1.2. Metoda de cercetare și colectarea datelor	186
6.1.3. Rezultatele cercetării și implicațiile evaluării rezultatelor auditului sistemului de management	188
<b>6.2. Analiza implicațiilor noii directive a UE privind măsurile pentru un nivel comun ridicat de securitate cibernetică</b>	<b>199</b>
6.2.1. Obiectivele investigației pentru un nivel comun ridicat de securitate cibernetică în UE	199
6.2.2. Metodologia de cercetare	200
6.2.3. Rezultatele și concluzia analizei implicațiilor noii directive UE pentru un nivel comun ridicat de securitate cibernetică	203
<b>6.3. Dezvoltarea unui model bazat pe un sistem de analiză și clasificare a modului și efectelor de eșec pentru evaluarea performanței sistemelor de management în contextul securității informațiilor și managementului continuității afacerii</b>	<b>215</b>
6.3.1. Obiectivele cercetării	215
6.3.2. Metodologia cercetării aplicate	216
6.3.3. Dezvoltarea teoriei aplicate pentru evaluarea performanței diferitelor sisteme de management	218
6.3.4. Propunerea unui model holistic de evaluare a performanței sistemelor de management integrat în contextul proceselor de afaceri durabile și al managementului riscurilor	226
<b>6.4. Verificarea unui model dezvoltat pentru evaluarea performanței sistemelor de management integrat în contextul proceselor de afaceri durabile și al managementului riscurilor</b>	<b>231</b>
6.4.1. Evaluarea cantitativă a modelului holistic	231
6.4.2. Efectele utilizării modelului de măsurare sugerat	232
<b>CONCLUZIE FINALĂ</b>	<b>237</b>

<b>BIBLIOGRAFIE</b>	<b>247</b>
<b>APENDICE</b>	<b>273</b>
Anexa A: rezultatele cercetării în implementarea sistemelor de management	<b>273</b>
Anexa B: compararea principiilor agile	<b>276</b>
Anexa C: rezultate anonimizate ale datelor din constatările auditului în organizații critice și necritice	<b>277</b>
<b>ANEXELE</b>	<b>300</b>
ANEXA 1: Lista publicațiilor autorului	<b>300</b>

## **b) Cuvinte cheie**

Standarde ale sistemului de management, norme ISO, Sistem de management integrat, performanță, evaluare, management al riscului, securitate informațională, securitate cibernetică, continuitate afacerii, sustenabilitate, agilitate, procese de afaceri, metodologie agilă, management al riscului întreprinderii, eficiență și eficiență organizațională, management al performanței, Leadership, managementul cunoștințelor, dezvoltare de modele, soluții holistice.

## **c) Rezumat**

Această disertație examinează problemele evaluării sistemelor de management integrate și neintegrate în contextul proceselor de afaceri corporative pentru informații și securitate cibernetică, continuitatea afacerii, sustenabilitate și managementul riscurilor. Pe baza unei analize a literaturii de specialitate, autorul a evaluat tendințele actuale și constatările cunoscute în acest domeniu de cercetare și și-a efectuat propriile studii empirice în ultimii cinci ani. Accentul acestor studii a fost pe mai multe domenii care sunt strâns legate de tema de cercetare. Un aspect este performanța organizației, inclusiv criteriile de măsurare a proceselor de afaceri consacrate și metodele măsurate pentru abordări multidimensionale, care includ, de asemenea, consolidarea dimensiunilor informațiilor și securității cibernetică, continuitatea afacerii și sustenabilitatea cerute de UE. Alte aspecte sunt legătura lor cu managementul riscului și factorii de succes ai sistemelor de management. Conceptele de management al riscului oferă soluții practice pentru sistemele de management la nivel de companie și măsurarea acestora.

O altă atenție este importanța și legătura dintre criteriile strategice și tehnologice pentru consolidarea sistemelor de management și managementul de vârf al acestora. În această disertație, autorul pune un accent deosebit pe problemele din acest domeniu de cercetare pe care le-a identificat în timpul multor audituri ale sistemelor de management consacrate pe care le-a efectuat și pe evaluarea soluțiilor utilizate. La elaborarea unui model de evaluare a sistemelor de management integrate și neintegrate, ținând cont de criteriile de context date, s-a pus accentul pe aplicabilitatea rezultatelor pentru utilizare strategică, organizațională și tehnologică și dependențele acestora. Modelul include utilizarea unui mod de eșec adaptat și a unei analize a efectelor cu o metodologie extinsă și agilă, legată de un proces de cartografiere strategică și de ciclul Plan-Do-Check-Act al sistemelor de management. În plus, reprezintă o abordare pentru oamenii de știință, consultanți și practicieni de a aprofunda, revizui și testa în continuare înțelegerea și experiența existentă a subiectelor conexe într-o manieră orientată spre un scop.



Scopul acestei lucrări a fost de a dezvolta un model informațional adaptat al riscurilor și oportunităților care combină procesele de afaceri, obiectele informaționale, activele de susținere, amenințările) pentru analiza clusterelor, care demonstrează abordarea integrată a organizațiilor pentru evaluarea riscurilor cu criterii multiple în domeniile companiilor de furnizare și generare a energiei și companiilor de informații și telecomunicații. Acest model poate fi aplicat atât diferitelor sisteme de management, cât și pentru a obține o creștere a eficienței procesului de management al riscului.

Autorul și-a bazat munca pe diverse metode de cercetare, prima metodologie implicând o revizuire a literaturii în domeniile relevante. Din identificarea stării actuale a cunoștințelor și a lacunelor de cercetare existente, autorul a derivat probleme, abordări și soluții existente. Autorul acestei lucrări a efectuat, de asemenea, studii științifice personale pentru a identifica aspecte importante pentru această lucrare, care se bazează și pe cunoștințele și cunoștințele dobândite în anii de experiență practică. În acest context, primul pas a fost analizarea abordărilor actuale ale riscurilor globale în securitatea informației în contextul managementului continuității afacerii, îmbunătățirea continuă a securității informațiilor și definirea unui sistem de management al securității informației în contextul managementului continuității afacerii. Autorul este intens implicat în implementarea, dezvoltarea și evaluarea sistemelor de management integrate și neintegrate cu diverse companii din sectoare critice și necritice. El este foarte interesat să dobândească cunoștințe, deoarece este vorba în primul rând despre îmbunătățirea continuă a cunoștințelor existente pentru practică și pentru comunitatea științifică. Prin această cercetare, autorul își propune să rezolve un aspect important al muncii sale de zi cu zi, și anume evaluarea riscurilor și a impactului acestora și nivelul de maturitate al sistemelor de management integrate și neintegrate utilizate de organizații și procesele lor de afaceri la nivel mondial.

Un accent deosebit a fost pus și analizat abordările actuale ale riscurilor globale în securitatea informațiilor în contextul managementului continuității afacerii, îmbunătățirea continuă a securității informațiilor și definirea unui sistem de management al securității informației în contextul managementului continuității afacerii. Aceasta înseamnă definirea, evaluarea și atingerea obiectivelor corporative care nu îndeplinesc doar obiectivele tradiționale. Cu toate acestea, valoarea financiară, care în trecut a fost considerată cel mai important aspect al organizațiilor, nu trebuie pierdută din vedere, deoarece aceasta trebuie realizată și raportată conducerii. De asemenea, se obțin noi perspective în acest domeniu în legătură cu sustenabilitatea.

Un proces de afaceri durabil în contextul securității informațiilor, securității cibernetice și continuității afacerii nu este doar un proces bazat pe o intrare de valoare financiară, ci

generează și rezultate în diverse alte aspecte. Unele dintre aceste aspecte de securitate fac parte din stabilirea unor măsuri în conceptul de durabilitate, de exemplu rezultate mai bune în ceea ce privește perspectiva ecologică și socială.

În funcție de domeniul de activitate din diferitele sectoare (energie, sănătate etc.), pot fi necesare și alte elemente pentru o evaluare a performanței. De exemplu, este necesară nu numai crearea de cunoștințe generale și specifice, ci și schimbul de cunoștințe și transferul de cunoștințe pentru cultura organizațională. Acest lucru face parte și din imaginea companiei de a face față societății și responsabilităților sale pe plan intern și extern și de a-și asuma responsabilitatea socială corporativă.

Este recunoscut faptul că evaluarea riscurilor și a oportunităților asociate ca decizie se realizează parțial în condiții de incertitudine. În plus, următorul text reunește discuția recentă privind extinderea procesului de management al riscului (RMP) existent în cadrul BCM din cauza amenințării riscului epidemic/pandemic la adresa securității informaționale a infrastructurii critice, a utilităților gestionate și a serviciilor de telecomunicații și examinează impactul acestuia asupra măsurilor de management al crizei (CM).

În plus, există perspective diferite asupra importanței proceselor de afaceri și a obiectelor informaționale care trebuie protejate și a riscurilor care trebuie abordate care afectează activul suportat. Performanța, care depinde de părțile interesate și de diverse aspecte (organizaționale, tehnice, tehnologice, de personal etc.), trebuie luată în considerare și atunci când se evaluează performanța oricărui sistem de management. O evaluare a performanței sistemelor de management este necesară deoarece fiecare sistem necesită un proces de îmbunătățire continuă. Acest lucru face posibilă maturizarea în timp. Pentru a atinge acest obiectiv inițial, metodologia prezentată mai jos a fost utilizată în această lucrare.

În prima parte a acestei lucrări, a fost efectuată o revizuire a literaturii pentru a examina datele științifice actuale în domeniul evaluării performanței sistemelor de management și a proceselor de afaceri și managementul riscurilor.

Capitolul unu tratează revizuirea literaturii de specialitate în acest domeniu pentru a analiza abordările actuale legate de riscurile globale de securitate a informațiilor în contextul managementului continuității afacerii, îmbunătățirea continuă a securității informațiilor și definirea unui sistem de management al securității informațiilor în contextul managementului continuității afacerii.

Începe prin a discuta istoria, definiția și starea științifică actuală a securității informațiilor în contextul riscurilor globale și al continuității afacerii și al managementului riscurilor.

Autorul a identificat diverse caracteristici ale organizațiilor și rolurilor, de exemplu nevoia de a opera într-un mediu în schimbare sau Domeniul de aplicabilitate (SoA) cu nevoia de a se adapta la aceste circumstanțe în schimbare. Aceasta include, de asemenea, activitățile digitale distribuite, de la managementul și cunoștințele locale, regionale până la interacțiunea globală și integrarea globală a proceselor de afaceri și cultură de securitate.

Este descris managementul riscurilor pentru obiectivele clasice de protecție, care este un proces iterativ de listare, evaluare și tratare a riscurilor. Prin identificarea cauzelor defecțiunii și cuantificarea probabilității de apariție, este posibil să se determine numerele de prioritate de risc folosind o analiză a modului de eșec și a efectelor (FMEA) (ISO/IEC 31000) și matricea de risc.

Prin identificarea cauzelor defecțiunii și cuantificarea probabilității de apariție, este posibil să se determine numerele de prioritate de risc folosind o analiză a modului de eșec și a efectelor (FMEA) (ISO/IEC 31000) și matricea de risc. În plus, aplicarea procesului BIA/RIA este, de asemenea, preluată pentru a identifica informațiile relevante pentru siguranță de la autorități și asociații, avertismentele și incidentele de siguranță care influențează rezultatele tratamentului riscurilor. BCM este un proces de management holistic care permite companiilor să furnizeze servicii și/sau produse critice la un nivel acceptabil, predefinit după un incident, pentru a minimiza daunele. Strategiile BC conexe sunt incluse în analiză pentru a determina un nivel minim acceptabil și un nivel durabil de funcționare.

În cel de-al doilea studiu, evaluarea performanței este explicată mai detaliat, deoarece joacă un rol important pentru organizații. Definiția de bază aici înseamnă că performanța unei organizații este măsurată prin capacitatea de a îndeplini toate sarcinile necesare pentru a-și atinge obiectivele organizaționale și financiare. Atât factorii de influență interni, cât și cei externi trebuie luați în considerare la evaluarea performanței. Orientarea către proces este un aspect obligatoriu al BPM. Capacitatea de a se schimba cât de repede este necesară este o cerință de bază a companiilor de astăzi și, prin urmare, un aspect important în cadrul unui proces de evaluare a unui sistem de management pentru măsurarea performanței, care este explicat mai detaliat.

În cea de-a treia analiză, sunt preluate metodele agile, deoarece au câștigat popularitate în ultimii ani, cu accent pe flexibilitate și adaptabilitate în managementul proiectelor, cum ar fi SCRUM. Acest lucru este, de asemenea, preluat în analiză, deoarece în mediul de afaceri dinamic de astăzi, agilitatea și capacitatea de reacție adecvată sunt de mare importanță.

În capitolul 2, aspectele managementului riscului au fost examinate ca o parte esențială a unei organizații care trebuie pregătită pentru evenimente vizibile și invizibile în cadrul digitalizării. În peisajul actual al afacerilor digitale, caracterizat de un mediu foarte VUCA,

companiile se confruntă cu provocări fără precedent care necesită o nouă abordare a structurii organizaționale și a conducerii.

În plus față de managementul clasic al riscului, care se bazează pe fundamentele managementului riscului și pe metodologia de management al riscului (de exemplu, încorporarea abordărilor de identificare a riscurilor, măsurarea riscurilor, monitorizarea riscurilor, atenuarea riscurilor etc.), se desfășoară o discuție despre managementul tradițional al riscurilor în conformitate cu COSO ERM, ISO 31000 și ISO/IEC27001 pentru a oferi o bază pentru o mai bună înțelegere a cadrului.

Acest studiu evidențiază importanța luării în considerare a factorilor de risc, a puterii de calcul și a proceselor decizionale multicriteriale pentru a îmbunătăți performanța generală și rezultatele în contextul managementului riscului. Prin analize ulterioare, se evidențiază importanța măsurării eficacității și eficienței practicilor de gestionare a riscurilor, în special în ceea ce privește indicatorii-cheie de performanță (KPI). Prin utilizarea cadrelor, metodelor și instrumentelor precum RMI, mecanismele de control intern, companiile își pot îmbunătăți strategiile de gestionare a riscurilor și pot obține rezultate mai bune în diferite sectoare. Acest lucru înseamnă, de asemenea, că evaluarea maturității managementului riscului este o metodă importantă de îmbunătățire a managementului riscului și de adaptare a acestuia la obiectivele strategice și operaționale ale companiei.

În revizuirea literaturii de specialitate din capitolul 3, relația dintre procesele de afaceri și influența cerințelor de securitate a informațiilor și de continuitate a afacerii (de exemplu, pe baza ciclului Plan-Do-Check-Act) este evidențiată de autor, deoarece acesta este un aspect esențial al managementului organizațional. Prin urmare, sunt enumerate cele mai relevante sisteme de management și structura la nivel înalt este examinată mai detaliat pentru a identifica tendințele organizaționale, a le analiza mai detaliat și a arăta diferența față de o structură armonizată. Aceasta implică o examinare amănunțită a statelor membre în ansamblul său și în toate aspectele sale la sediile societății respective.

Pentru ca sistemele de management să-și dezvolte efectul deplin și să conducă la rezultatele dorite, interacțiunea diferiților factori de succes este crucială, care sunt specificați în următorul studiu. Pe lângă aspectele structurale și procedurale, factorii de leadership și angajament față de angajați și cultura organizațională joacă un rol important. Aspectele cu factori precum transparența, încrederea și o cultură a îmbunătățirii continue sunt cuvinte cheie importante aici și formează baza unui sistem de management funcțional. În funcție de cerințele de protecție implementate, acestea pot fi împărțite în măsuri independente, clasificate, grupuri sau niveluri de maturitate în conformitate cu Capability Maturity Model Integration (CMMI).

Prin urmare, autorul sugerează analizarea principiului CMMI și a aplicației pentru înregistrarea și măsurarea maturității sistemului CMS.

A treia analiză specifică faptul că procesele de afaceri (BP) eficiente și fiabile sunt esențiale în raport cu informațiile care trebuie protejate (obiecte informaționale – IO) și sistemele/serviciile lor susținute de tehnologia informației și comunicațiilor (TIC). Numai în acest fel pot fi depășite provocările operaționale complexe ale companiei. Aceasta include, de asemenea, certificarea conform standardului recunoscut la nivel internațional pentru sistemele de management al securității informațiilor conform ISO/IEC 27001 în toate industriile cu infrastructură critică și non-critică.

Partea a II-a a acestei lucrări este contribuția personală a autorului acestei lucrări la domeniul de studiu. Conține studii empirice care extind rezultatele altor studii menționate în partea I pentru a deriva un model de evaluare.

În capitolul 4, autorul a analizat relația dintre procesele de afaceri și nivelul de cunoștințe intelectuale în contextul proceselor ce trebuie securizate și nivelul de maturitate asociat performanței companiei care urmează să fie asigurat, pentru a demonstra importanța integrării cerințelor de securitate pentru impactul performanței. Scopul cercetării a fost de a identifica posibile relații între obiectivele definite, natura acestora și performanța organizațională raportată.

Primul studiu s-a concentrat pe măsurarea performanței mai multor audituri externe în patru organizații care oferă servicii IT gestionate clienților lor. Autorii au verificat nivelul de conformitate cu sistemul de management al serviciilor descris în standardul de cerințe ISO/IEC 20000-1. Accentul se pune pe integrarea cerințelor de securitate bazate pe o analiză a riscurilor în serviciile IT furnizate. Mutarea accentului pe îndeplinirea indicatorilor cheie de performanță din acordurile de nivel de servicii poate ajuta furnizorii de servicii IT, printre altele, să evite incidentele de securitate, dar poate pune în pericol obligațiile contractuale cu clienții.

La ajustarea nivelului de securitate și a măsurilor pentru serviciile informatice furnizate, ar trebui luate în considerare aspecte specifice, cum ar fi activele și serviciile critice care trebuie securizate. Autorii acestui studiu concluzionează că există o legătură clară între securitatea informațiilor și managementul serviciilor. De asemenea, se subliniază că cele două concepte pot fi integrate cu succes. Dacă este bine implementată, securitatea informațiilor are un efect pozitiv asupra managementului serviciilor. În plus, s-a recunoscut că introducerea unui sistem integrat de management al securității informațiilor poate ajuta furnizorul de servicii IT să abordeze măsurile de securitate specifice mult mai detaliat. Acest lucru confirmă abordarea unui sistem de management integrat.

În analiza ulterioară, au fost abordate subiectele de cercetare a dependențelor managementului securității informației în legătură cu continuitatea afacerii și caracterizarea impactului asupra afacerii în contextul crizei globale. Se specifică faptul că ISMS poate atinge multe obiective de protecție care asigură integritatea informațiilor în cadrul unei organizații. În plus, continuitatea activității, împreună cu adăugirile asociate la controale și obiectivele de control, pot fi bine cartografiate într-un cadru general de management. Trebuie luate în considerare completările care abordează subiecte specifice, cum ar fi politica, organizația, personalul, inventarul, operațiunile IT și comunicarea IT, precum și managementul continuității activității din perspectiva SGSI. Dacă există deja un sistem conform ISO 27001, acesta se poate baza pe rezultatele sale, iar extinderea către BCM creează valoare adăugată pentru organizație. Aceasta înseamnă că procedurile esențiale de management sunt încercate și testate.

Se confirmă că amenințările de securitate ale atacurilor cibernetice în structurile inteligente de automatizare și digitalizare sunt în creștere, iar probabilitatea unor întreruperi grave, cum ar fi epidemii/pandemii, este în creștere. Prin urmare, este necesară dezvoltarea continuă a managementului securității informațiilor și a riscurilor de securitate a informațiilor în timpul transformării digitale. Numai în acest fel poate fi identificată mai eficient apariția influențelor grave globale și pot fi reduse la minimum perturbările asociate în managementul proceselor de afaceri și ale continuității afacerii.

Cea de-a treia cercetare a analizat potențialul strategic de gestionare a unui model de maturitate independent în legătură cu digitalizarea proceselor, respectând în același timp obiectivele de protecție pentru securitatea informațiilor și protecția datelor. În acest context, a fost dezvoltată o abordare conceptuală pentru etapele de digitalizare în mai multe etape pentru a arăta că crearea de procese modelate este un pas important în automatizarea proceselor standard. Această extensie arată direcția unei organizații agile de informații și securitate cibernetică și creează valoare adăugată pentru organizații.

Acest lucru creează oportunitatea de a încerca și testa procesele esențiale de afaceri. Prin comparație cu elementele specifice SCRUM, se stabilesc operațiuni concentrate și sigure pentru cerințele de securitate informatică și cibernetică. Procesul de management al riscului nu se mai bazează pe o evaluare unică a riscurilor și pe cataloage statice de amenințări, ci procesele organizaționale și tehnice se adaptează cerințelor de securitate și evoluează continuu. În consecință, evaluările evaluării riscurilor sunt obținute într-o manieră mai agilă și puse în aplicare într-o manieră suficient de detaliată și agilă. Prin urmare, trebuie depuse eforturi la nivelul întregii companii pentru a proteja datele critice, rețelele IT, aplicațiile (software) și sistemele asociate ca parte a sistemului de management integrat.

Modelul propus a fost evaluat folosind o abordare de studiu de caz în cadrul companiei de consultanță. Se poate concluziona că modelul propus poate fi utilizat practic pentru o evaluare a managementului riscurilor companiilor.

Concluzia ultimei părți a capitolului al patrulea a arătat că abordările moderne de management, cum ar fi principiile agile ale industriei cu valoare adăugată, sunt benefice pentru eficiența și eficacitatea organizațiilor. Acest lucru subliniază importanța adaptării rapide pe o piață în schimbare rapidă și importanța acestor principii și tactici operaționale ca factori de influență pentru performanță.

Capitolul 5 tratează cercetarea în domeniul sistemelor de management al securității informațiilor și influența asupra performanței proceselor de afaceri prin cadre asociate pentru a permite măsuri clasificate și pentru a identifica factorii critici de succes în contextul sustenabilității și al serviciilor gestionate.

Pentru domeniul proceselor susținute de TIC, cerințele bazate pe ISO/IEC 27005 sunt utilizate pentru a evalua nevoia de protecție a activelor de susținere. Nevoia de protecție este un activ moștenit al obiectelor de informații care trebuie protejate și care sunt utilizate pentru tranzacții și procese de afaceri conexe. Obiectele de informații sunt atribuite locurilor de utilizare și furnizorilor de servicii. Catalogele de amenințări sunt create pe baza potențialului de deteriorare al informațiilor procesate. Cerința de protecție se calculează conform principiului maxim. În acest scop, a fost analizat un cadru organizațional, orientat spre procese și legal care definește managementul securității informațiilor și al protecției datelor în contextul digitalizării și, în același timp, îndeplinește diferitele obiective de protecție.

În a doua parte a cercetării, s-a arătat că, luând în considerare obiectivele de protecție, este posibil să se implementeze o metodă agilă și să se dezvolte o matrice de risc adaptată bazată pe analiza efectului modului de eșec (FMEA). Ca urmare, cerințele organizaționale ale SGSI ar putea fi examinate în cadrul unui cadru organizațional și orientat spre procese.

În plus, s-a confirmat că SGSI joacă un rol central pentru infrastructurile critice și necritice. Ca parte a analizei, s-a constatat că SGSI poate fi extins prin integrarea proceselor de management al securității informațiilor. Prin urmare, măsurile ar putea fi clasificate, combinate și îmbunătățite, ceea ce afectează în cele din urmă nivelul de maturitate.

Prin adaptarea procesului și specificarea unui registru specific al riscurilor cibernetice, s-a demonstrat că este posibilă gestionarea proactivă a riscurilor de securitate cibernetică. Acest lucru duce la o mai bună implementare a activităților de management, ceea ce crește eficiența procesului de management al riscurilor.

În acest context, a fost dezvoltat un model de interacțiune a proceselor care poate fi utilizat ca model de maturitate independent de industrie pentru evaluarea proceselor de afaceri

pentru actori. Modelul conține mai multe dimensiuni care operaționalizează procesele la nivel de proces prin criteriile de risc evaluate pentru calitate, securitatea și protecția datelor și asigură transparența corespunzătoare a procesului pentru toți cei implicați.

A treia parte a cercetării se referă la dependențele cerințelor de management existente și a obiectelor informaționale care trebuie protejate în organizații, care sunt specificate de obiectivele de protecție. Procesele de securitate a informațiilor asociate trebuie să fie clar definite, astfel încât să poată fi împărțite sau clasificate în securitate informațională strategică și operațională în domeniile de responsabilitate ale celor responsabili din organizația de securitate.

Categoriile orientate spre proces sunt discipline individuale care sunt stabilite și clasificate într-o manieră orientată spre obiective pentru a le gestiona eficient, eficient și durabil. Acest lucru necesită adaptarea activităților de management, ceea ce duce la măsuri sigure și durabile prin clasificarea informațiilor și consolidarea și prioritizarea specifică grupului. Creșterea eficienței procesului de management al riscurilor (RMP) nu este doar posibilă, ci este previzibilă prin consolidarea legată de grup și prioritizarea măsurilor.

Capitolul 6 se referă la dezvoltarea modelelor de măsurare și evaluarea sistemelor de management integrate și neintegrate în diferite sectoare. Acest lucru s-a realizat ca urmare a studiilor desfășurate în cadrul programului de doctorat. Acest lucru a fost realizat prin completarea rezultatelor studiilor menționate în capitolele anterioare cu rezultate suplimentare de cercetare personală și apoi elaborarea posibilelor soluții la problemele descoperite.

Autorul este implicat personal într-o serie de audituri ale sistemelor de management integrate și neintegrate din diferite sectoare și, prin urmare, are date valoroase care pot fi utilizate pentru a aprofunda acest subiect. Rezultatele analizei cantitative au arătat că în anumite domenii există mai multe neconformități și recomandări cu cerințele pentru sistemele de management decât în altele.

Prima parte de cercetare evidențiază problemele în implementarea și aplicarea sistemelor de management al securității informației pe baza experienței profesionale a autorului în consultanță și audit al sistemelor de management. Începe cu prezentarea studiilor care includ dependențe și motive importante și se concentrează pe criteriile cheie în infrastructurile critice și necritice pentru această cercetare. Aceasta se bazează pe o analiză empirică rezultată din rezultatele auditurilor externe efectuate de auditorul N3I (neutru, independent, imparțial, integritate) și din constatările auditului rezultate.

Auditurile efectuate demonstrează verificarea specifică a conformității măsurilor organizatorice, tehnice, de personal și fizice. Procesul de certificare efectuat de auditor sau echipa de auditori este documentat în conformitate cu cerințele normative. Dacă există abateri



de la conformitatea standardului, acest lucru este specificat și înregistrat în mod verificabil ca constatare. Scopul acestor recomandări este de a optimiza eficiența, eficacitatea și conformitatea sistemului de management cu standardele și cele mai bune practici relevante.

În plus, cerințele actuale ale UE pentru noile directive ale UE privind măsurile pentru un nivel comun ridicat de securitate cibernetică sunt abordate și explicate mai detaliat. De asemenea, este discutat potențialul strategic pentru gestionarea durabilă a conformității cerințelor legale și de reglementare pentru o cultură a cerințelor și a riscurilor serviciilor critice și necritice.

În a treia parte, autorul dezvoltă un sistem de evaluare și clasificare bazat pe analiza modului de eșec și a efectelor pentru a evalua performanța sistemelor de management în contextul managementului securității informațiilor și al continuității afacerii și verifică-l pentru utilizare practică.

Pe scurt, munca de cercetare conținută în această teză evidențiază următoarele puncte fundamentale:

- Complexitatea evaluării performanței: Evaluarea performanței sistemelor de management este o provocare atât pentru practică, cât și pentru cercetare. Acest lucru se datorează în principal unei înțelegeri inconsecvente a conceptului de performanță și lipsei de metode standardizate.
- Înțelegerea multidimensională a performanței: Performanța organizațiilor este adesea redusă la indicatori financiari. Disertația susține o înțelegere mai cuprinzătoare a performanței, care include și alte dimensiuni, cum ar fi excelența operațională, eficiența și eficacitatea proceselor.
- Diverse metode de evaluare: Există diverse modele și metode de evaluare multidimensională a performanței. O abordare promițătoare este combinația metodologiei FMEA cu procese agile, cum ar fi SCRUM. SCRUM a fost dezvoltat inițial pentru dezvoltarea de software, dar poate fi adaptat pentru evaluarea holistică a performanței prin integrarea perspectivelor de sustenabilitate și management al riscului.
- Factori de succes pentru integrare și funcționare: Implementarea și certificarea cu succes a sistemelor de management depinde în mare măsură de patru factori: angajamentul managementului, stiluri de conducere adecvate, metode de evaluare adecvate și un proces de îmbunătățire continuă.

Disertația oferă astfel informații valoroase pentru practică și cercetare pentru a surprinde și optimiza performanța sistemelor de management într-o manieră mai holistică. Modelul

dezvoltat de autor își propune evaluarea performanței pe baza unor indicatori de diverse dimensiuni.

Pe lângă indicatorii identificați care decurg din temele securității informaționale și cibernetice, continuității afacerii și sustenabilității, eficiența și eficacitatea proceselor operaționale și strategice reprezintă o perspectivă convingătoare care trebuie evaluată. În acest context, trebuie luate în considerare și aspectele care sunt relevante pentru un anumit subiect al sistemului de management și pentru obiectivele specifice industriei companiei.

Modelele au inclus, de asemenea, măsurarea nivelurilor de maturitate, inclusiv performanța generică a sistemelor de management integrate și neintegrate.

Ultimul pas a fost verificarea modelului propus folosind o analiză cantitativă bazată pe audituri interne și interviuri conexe. În acest fel, autorul a evaluat și comparat abordări și metode, cum ar fi modelul de evaluare propus.

Rezultatele au arătat că modelul BIST propus este o metodă validă de evaluare a performanței sistemelor de management în companii, în special datorită următoarelor puncte:

1. Modelul conectează evaluarea sistemelor de management integrat testate în diferite sectoare cu obiectivul strategic, deoarece poate fi utilizat pentru a testa abordarea agilă promițătoare, combinând metodologia FMEA cu procese agile precum SCRUM și folosind metodologia agilă pentru a raporta rezultatele evaluărilor într-o manieră agregată către managementul de top.
2. Modelul este legat de dezvoltarea proceselor operaționale de afaceri bazate pe strategia definită a organizației.
3. Modelul poate fi utilizat pentru a măsura valorile din toate dimensiunile relevante, inclusiv metodele și KPI-urile utilizate, sustenabilitatea și evaluarea managementului riscurilor companiilor. Modelul BIST propune metode bine cunoscute și consacrate.

Cu aceste cunoștințe, se poate concluziona că modelul propus identifică și rezolvă probleme concrete descoperite de alți autori și oameni de știință în timpul muncii zilnice și cercetării științifice a autorului tezei de doctorat. Prin aplicarea diferitelor abordări de cercetare, a fost derivat și testat empiric un cadru de măsurare holistică pentru evaluarea performanței sistemelor de management integrat examinate. În această lucrare, a fost identificată relevanța strategică a sistemelor de management integrat și evaluarea acestora, deoarece sistemele de management combină o varietate de subiecte de la nivel operațional la nivel strategic.

## d) Curriculum Vitae

PERSONAL  
INFORMATION

LAMPE, Georg Sven



📍 Kerkower Dorfstraße 47, 16278 Angermünde, Germany

☎ +49 173 866 49 15

✉ [lampe@compliance-docs-group.com](mailto:lampe@compliance-docs-group.com)

Sex Masculin | Data nașterii 30.07.1976 | Naționalitate : germană

Sunt inginer foarte motivat, pe de o parte, cu câțiva ani de experiență în sectoarele energiei și telecomunicațiilor și, pe de altă parte, cu abilități organizaționale excelente și abilități de gândire strategică și de afaceri.

Sunt obișnuit în proiectul complex prin experiența mea de a focaliza direcționarea și rezolvarea ordonată a strategiilor companiei, organizarea, implementarea și dezvoltarea eficientă a strategiilor companiei. Prin abilitățile mele profesionale și personale de conducere sunt obișnuit să iau decizii independente, precum și să acționez orientat spre echipă și spre un comportament antreprenorial.

Sunt un muncitor în echipă de conștiință, căruia îi place să iau inițiativă și pot lucra foarte eficient pe cont propriu.

Sunt foarte interesat să studiez noile îmbunătățiri ale performanței sistemelor de management în comparație cu implementarea unui sistem de management integrat (calitate, mediu, securitate, responsabilitate socială) pentru o mai bună înțelegere a noilor sisteme organizaționale și strategice de comunicare în afaceri.

Învăț foarte repede, care salută noi provocări și este deschis la noi experiențe.

## EXPERIENȚĂ PROFESIONALĂ

oct. 2021 –  
prezent

### Director executiv (CEO), manager, lider de echipă management de proiect

Compliance Docs Group Verwaltungs GmbH, Angermünde

- Auditor de certificare ISO 27001 / Partener al TÜV Süd Management Services
- Status: Auditor cu performanță de audit din 10.2015: aprox. 350 d
- Focus: Securitatea informațiilor
- Planificarea și implementarea proiectelor de certificare transnaționale cu standarde multiple și coordonarea echipelor internaționale
- Consolidarea rezultatelor echipelor de audit, compararea cu businesscase-ul, strategia și riscurile, precum și prezentarea către IMM-uri și corporații
- Autor și coautor: diverse conferințe internaționale în domeniul securității informației, securității cibernetice și protecției datelor, BMC etc.
- Unitate de afaceri Rețele de Aprovizionare și Telecomunicații (E/TK/LST) pentru ITIL / ISO 20000, ISO 27001 Securitatea informațiilor, ISO 27019 Infrastructuri critice, (B3S), ISO 22301 Continuitatea afacerii, ISO 50001 Energie, ISO 9001 Calitate, Regulamentul general privind protecția datelor, Risc economic MMS
- Servicii Naționale de Gestionare a Serviciilor IT Proiecte și SOC
- Ofițer de digitalizare
- Implementarea proceselor de securitate a informațiilor (ISO 27001 ff.)
- Pregătirea analizei riscurilor, planificării de urgență și a conceptului de recuperare în caz de dezastru
- Implementarea și optimizarea proceselor IT operaționale pentru creșterea eficienței
- Măsurile de îmbunătățire a proceselor și de creștere a maturității
- Modelarea proceselor ITIL pentru managementul centrelor de date și aplicațiilor etc.
- Sincronizare cu echipele de software, inginerie și asistență din Singapore și Malta/N.Y.
- Coordonarea, managementul unei echipe de furnizori offshore cu 30+ membri
- Managementul contractelor cu furnizorii, planificarea bugetului anual

**Afaceri sau sector** Tehnologia informației, Consultanță

oct. 2021 –  
prezent

## Director executiv (CEO)

Compliance Docs Group GmbH & Co. KG, Angermünde

- Mentalitate de fondator cu un nivel extrem de ridicat de orientare către client
- Experiență în înființarea/dezvoltarea de noi activități de afaceri, de exemplu în mediul industriei IT, cu o puternică voință creativă pentru securitatea informațională și cibernetică, protecția datelor, calitate etc., cu un accent necondiționat pe succes și obiective, precum și o gândire vizionară
- Experiență în înființarea cu succes a unei distribuții multinaționale B2B/B2C (analogică și digitală)
- Înțelegere tehnică IT extinsă (arhitectură, concepție, implementare etc.)
- Responsabilitatea pentru alinierea strategică, organizațională și tehnică completă și execuția proiectelor folosind metodele de management al proiectelor strategice de afaceri și coordonarea proceselor conform ITIL, PMboK în comparație cu BSI, ISO/IEC 27001, ISO/IEC 27019, ISO 9001, ISO/IEC 27701, ISO/IEC 50001, ISO/IEC 55001, Smart Market etc.
- Responsabilitatea pentru activitatea operațională (planificare, dezvoltare și implementare) în conformitate cu legislația, precum și cu reglementările și liniile directoare interne
- Stabilirea canalelor de vânzare; Serviciu clienți; Obligații de relații publice și reprezentare, precum și raportarea periodică către acționari
- Stabilirea gradului de pregătire al companiilor pentru piața de capital
- Coordonarea comerțelor conexe până la redactarea contractelor pentru întreaga conducere externă a companiei
- Responsabilitatea pentru toate subiectele de afaceri și tehnice, precum și asumarea întregii responsabilități bugetare
- Dezvoltarea/implementarea și responsabilitatea măsurilor pentru condițiile-cadru și cerințele legale în industria energetică, de exemplu, bazele tehnice ale furnizării de energie electrică și gaze, elementele de bază pentru operarea rețelei, controlul și dispecerizarea rețelei, infrastructurile IT critice pentru operarea rețelei, domeniul de aplicare al SGSI conform catalogului de securitate IT § 11 alin. 1a EnWG
- Elaborarea/implementarea și responsabilitatea măsurilor privind condițiile cadru legale și reglementările relevante pentru industria energetică (în special separarea), precum și pentru generarea de energie electrică și producția de gaze (proiect hidrogen – centrală electrică hibridă), expertiză tehnică în generare, baze de exploatare și control al instalației, expertiză tehnică privind diferitele categorii de instalații energetice și caracteristicile lor speciale, infrastructuri IT critice pentru operarea instalațiilor – domeniul de aplicare al SGSI conform IT catalog de valori mobiliare § 11 alin. 1b EnWG
- Manager pentru o echipă de ingineri software care dezvoltă soluții pentru sistemele de control din fabrică în jurul IBM SiView MES și interfețele echipamentelor
- Responsabil pentru dialogurile de stabilire a obiectivelor, evaluări anuale ale performanței, planificarea resurselor, interviuri de angajare, organizarea de evenimente de team building
- Sincronizare cu echipele de software, inginerie și asistență din Singapore și Malta/N.Y.
- Coordonarea, managementul unei echipe de furnizori offshore cu 30+ membri
- Managementul contractelor cu furnizorii, planificarea bugetului anual

Afaceri sau sector Consulting and Auditing

Jan 2020 –  
Nov 2022

## Manager principal pentru sisteme de management, Managing Partner

Stadtwerke Schwedt, Schwedt/Oder

- Șef Digitalizare și Sisteme de Management în Divizia Rețele de Aprovizionare și Telecomunicații (E/TK/LST) în unitatea organizațională
- Responsabilitatea pentru gestionarea strategică, organizatorică, tehnică și bugetară completă a proiectelor de digitalizare și a serviciilor IT folosind metodele de management de proiect ITIL, PMboK, Scrum
- Responsabilitatea pentru proiectarea, implementarea și operarea operațiunilor de securitate a controlului energiei electrice, gazelor și încălzirii centralizate în conformitate cu legislația, precum și cu reglementările și liniile directoare interne (ISO/IEC 27001 Securitatea informațiilor, ISO/IEC 27019 Infrastructuri critice (B3S), ISO/IEC 22301 Continuitatea afacerii, ISO/IEC 50001 Energie, ISO 9001 Calitate, Regulamentul general privind protecția datelor) până la proiectarea proceselor de afaceri și stabilirea nivelului de funcționare a serviciului (SLA, OLA) din gestionarea incidentelor (întreruperi operaționale, incidente de securitate, situații de urgență/crize)
- Dezvoltarea, punerea în aplicare și responsabilitatea pentru măsurile privind cadrul legal și cerințele aprovizionării cu energie în rețea în industria energetică, de exemplu, expertiză tehnică în furnizarea de energie electrică și gaze, exploatarea rețelei, controlul și dispecerizarea rețelei, infrastructuri informatice critice pentru operarea rețelei, domeniul de aplicare al SGSI conform catalogului de securitate informatică §§ 11 alin. 1a
- Responsabilitatea pentru pregătirea recomandărilor de acțiune și coordonarea meseriilor conexe

- până la redactarea contractelor de securitate IT și managementul cerințelor, precum și coordonarea proceselor strategice IT Business cu top managementul și șefii de departament
- Îndrumare (personal, profesioniști) angajați

**Afaceri sau sector** și producție de energie, Energie regenerabilă, Tehnologie, Consultanță

Martie 2017 -  
prezent

### Chief Executive Officer (CEO)

Bürgerwind Schönfeld GmbH & Co. KG, Kerkow

- domeniul de afaceri pentru energii regenerabile și responsabilitatea pentru întregul management organizațional, inclusiv dezvoltarea proceselor de afaceri adecvate în cadrul metodologiilor de management de proiect ITIL, PMBOK, precum și managementul calității, securității și confidențialității datelor
- Coordonarea tranzacțiilor până la redactarea contractelor
- Manager (calitate, securitate) și lider (grupuri IT și proiecte) în sistemul de afaceri, precum și în dezvoltarea serviciilor (tele-/comunicații de date) / managementul datelor energetice
- Responsabilitatea pentru întregul management organizațional și tehnic al proiectului, inclusiv dezvoltarea proceselor de afaceri adecvate și a interfețelor de date folosind metodologiile de management de proiect ITIL, PMBOK, Scrum
- Planificarea, dezvoltarea și implementarea sistemului de energie regenerabilă cu specificații prin ajustarea afacerii și a interfeței, gestionarea cererilor și comenzilor, coordonarea tranzacțiilor până la redactarea contractelor
- Instrucțiuni (tehnic, personal) până la 5 angajați și stagiar
- Auditor principal de certificare în calitate de partener al TÜV Süd Management Service GmbH, DEKRA
- Servicii de consultanță pentru audituri de securitate a informațiilor (ISO27001, BSIG §8a, IT-SiKat), TISAX VDA-ISA, ISMS
- Management de proiect (software, automatizare, ITSM), Scrum Master
- **Afaceri sau sector** Energie regenerabilă, Tehnologie, Consultanță

Martie 2009 –  
prezent

### Manager principal pentru sisteme de management, Managing Partner

ENERTRAG AG, Dauerthal/Berlin

- Manager (calitate, securitate) și lider (grupuri IT și proiecte) în sistemul de afaceri, precum și în dezvoltarea serviciilor (tele-/comunicații de date) / managementul datelor energetice
- Responsabilitatea pentru întregul management organizațional și tehnic al proiectului, inclusiv dezvoltarea proceselor de afaceri adecvate și a interfețelor de date folosind metodologiile de management de proiect ITIL, PMBOK, Scrum
- Planificarea, dezvoltarea și implementarea sistemului de energie regenerabilă cu specificații prin ajustarea afacerii și a interfeței, gestionarea cererilor și comenzilor, coordonarea tranzacțiilor până la redactarea contractelor
- Strategie/Procese BSI, Securitate IT, Protecția datelor, Securitate cibernetică, Calitate, ITIL și B3S
- proiecte internaționale de servicii IT, precum și bazate pe SOC
- Controlul proceselor și operațiunilor operaționale de management al serviciilor IT (SLA internațional, OLA pentru clienții majori)
- Managementul echipei de criză pentru IT și NON-IT a tuturor liniilor de vânzări pentru controlul energiei regenerabile (până la 8 GW)
- Management de proiect în proiecte IT internaționale (Franța etc.)
- Dezvoltarea/implementarea sistemului de management al riscului (ISO 31000, ISO 27005)
- Formator de auditori interni
- Instrucțiuni (tehnic, personal) până la 5 angajați și stagiar
- Auditor principal de certificare în calitate de partener al TÜV Süd Management Service GmbH, DEKRA
- Servicii de consultanță pentru audituri de securitate a informațiilor (ISO27001, BSIG §8a, IT-SiKat), TISAX VDA-ISA, ISMS
- Management de proiect (software, automatizare, ITSM), Scrum Master
- Consultanță de proces, traininguri, management interimar

**Afaceri sau sector** Energie regenerabilă, Tehnologia informației, Consultanță

EDUCAȚIE

2019 – 2024

### Studii de doctorat la

The Bucharest University of Economic Studies, Bucharest

Cercetare privind securitatea informațiilor în procesele de afaceri legate de riscurile globale

Cuvinte cheie:

Standarde de Sistem de Management, Norme ISO, Sistem de Management Integrat, Performanță, Evaluare, Managementul Riscurilor, Securitatea Informațiilor, Securitate Cibernetă, Continuitatea Afacerii, Sustenabilitate, Agilitate, Procese de Afaceri, Metodologie Agile, Managementul Riscului Întreprinderii, Eficacitate și Eficiență Organizațională, Managementul Performanței, Managementul Cunoștințelor, Dezvoltare de modele, soluții holistice

2011 – 2014 **Studii la Hochschule für Telekommunikation Leipzig de la Deutsche Telekom**

Universitatea de Telecomunicații Leipzig, Germania,

Master în Inginerie domeniul Tehnologiei Informației și Comunicațiilor

studii profesionale: securitate IT, internetworking, IT-Law și administrarea afacerilor, management de proiect (PMBOK, Scrum)

2003 – 2007 **Studii la Hochschule für Telekommunikation Leipzig de la Deutsche Telekom**

Universitatea de Telecomunicații Leipzig, Germania

Diplomă - inginerie telecomunicații în domeniul Științei Electronice și Ingineria Telecomunicațiilor

Priorități: Managementul conturilor de afaceri IT, inclusiv marketing, management de proiect

2000 – 2003 **Gimnaziu (școală de gramatică)**

Schwedt, Germania

Absolvirea cu fracțiune de normă a diplomei de admitere la universitate

2001 – 2003 **Apprenticeship as an IT systems electronics technician in Angermünde**

Schwedt, Germania

Absolvirea cu fracțiune de normă a diplomei de admitere la universitate

1983 – 1993 **Polytechnische Oberschule (școală elementară/secundară)**

Greiffenberg, Germany

cu dreptul de a frecventa învățământul secundar superior

FORMAR

E

- 2018 PMP, Profesionist în management de proiect (PMI)
- 2017 Auditor certificat de securitate a informațiilor acc. ISO 27001 (TÜV Süd), DEKRA
- 2016 Fundația PRINCE2 (Axelos)
- 2016 Scrum Master profesionist (Scrum.org)
- 2006 Fundația ITIL V2 (HFTL)

ABILITĂȚI  
PERSONALE

Limba maternă

German

Alte limbi

	UNDERSTANDING		SPEAKING		VORBIND
	VORBIND	Reading	Spoken interaction	Interacțiune vorbită	
English	C1	C1	C1	C1	C1

**Abilități și  
competențe  
sociale**

- profesionist cu peste 20 de ani de experiență ca manager, lider de proiect și expert în diferite roluri și industrii
- Reinteracțiune vorbită alization din punctul de vedere al managementului afacerii și al proceselor de risc
- (Planificare, sprijin, dezvoltare, planificare proiect, evaluare, cadru de reglementare - linii directoare, standarde, reglementări)
- Implementarea sistemelor de aplicații, - funcții sau - soluții
- Participarea la toate procesele și fazele de luare a deciziilor tehnice și de vânzare
- Executarea evaluărilor angajaților, inclusiv determinarea sarcinilor și obiectivelor, precum și evaluarea realizărilor, punctelor forte, punctelor slabe ale angajatului
- Motivarea angajaților prin vizualizarea nevoilor și prezentarea modalităților în combinație cu setarea dozată a stimulentele (de exemplu, alocarea responsabilităților, delegarea proceselor)
- Sprijinirea, însoțirea și furnizarea de abilități și competențe organizaționale și tehnice folosind managementul inovativ al formării

**Abilități  
organizaționale**

- Conducerea echipelor internaționale, distribuite, inclusiv modele offshore, nearshore
- Acționând ca profesionist în management de proiect în proiecte clasice sau agile cu accent tehnic sau de coordonare
- Lucrând mulți ani în medii, cu accent pe dezvoltarea, proiectarea și operarea sistemelor de producție 24/7
- Dezvoltarea de servicii recomandabile în lanțul de aprovizionare digital, în conformitate cu obiectivele de protecție (confidențialitate, integritate, disponibilitate, autenticitate), construirea de relații de încredere cu clienții sau partenerii
- Analiza proceselor de afaceri și de suport (interne, externe), precum și măsurile necesare, inclusiv evaluarea riscurilor pentru managementul siguranței și calității în conformitate cu regulamentul privind protecția datelor
- Analiza proceselor și măsurilor clienților

Proiecte:

- comercializarea directă și reglementarea primelor de piață pentru energiile regenerabile (Lege-EEG),
- Întreținerea punctelor de măsurare și operarea contoarelor (rețea inteligentă, contor inteligent și operațiuni),
- certificare conform ISO 27001 (sistem de management al securității informațiilor), ISO 9001 (sistem de management al calității) și sistem de management al protecției datelor
- planificarea, proiectarea conform standardelor/liniilor directoare a proiectelor complexe system-on-chip, IT, siguranța și specifice instalației bazate pe servicii ITIL, PMBOK și Scrum,
- Rețele Wi-Fi/LAN, soluții de telecomunicații, dezvoltare de aplicații software (OPC DA, OPC XML DA, SCADA systems, IEC 60870-5-101 și 104, DIN 61400-25), .Net

Tutore:

- Responsabilitate în domeniul ingineriei energetice și în domeniul materialelor și componentelor
- Pregătirea și desfășurarea cursurilor pentru studenții de licență
- Coaching, instruire și sprijin al elevilor în exerciții

Membrii consiliului elevilor:

- Responsabilitatea Unității de tehnică și sport

**Abilități de  
calculator**

- Certificări în dezvoltarea software JAVA, Scrum, ServiceNow, ITIL, securitatea informației și managementul proiectelor
- Know-how în întregul ciclu de viață al dezvoltării software
- Administrare, experiență de utilizator competentă pentru mai multe sisteme IT
- Tehnologii: Energie regenerabilă, inginerie de sisteme, telecomunicații, managementul datelor energetice, sisteme de aplicații, sisteme IT simple / în rețea, tehnologie de securitate
- Limbaje de programare: C#, C/C++, SPS, HTML, Assembler, JAVA; VHDL(Xilinx, Quartus), Vultur
- Software de sistem, aplicație și simulare: cunoștințe aprofundate în arhitectura fiecărui sistem de operare (DOS, Windows), precum și software de aplicație Office și baze de date, cunoștințe extinse de editare a imaginilor cu Adobe Photoshop, MatLab, LabView, PSpice

Date: 22.08.2024 .....

Signature: .....