UNIVERSITATEA DE STAT DIN MOLDOVA

ȘCOALA DOCTORALĂ ȘTIINȚE ALE NATURII

Cu titlu de manuscris
C.Z.U. 004.056:336.71(478)(043)

BRICEAG VALENTIN

ANALIZA ȘI CREȘTEREA NIVELULUI DE MATURITATE A SISTEMULUI DE MANAGEMENT AL SECURITĂȚII INFORMAȚIEI PENTRU ENTITĂȚI DIN REPUBLICA MOLDOVA

(pe exemplul băncilor comerciale)

232.02 Tehnologii, produse și sisteme informaționale

Teză de doctor în Informatică

Autor: _____
(semnătura)

Conducător de doctorat: _____ Bragaru Tudor, dr. în ec., prof. univ.
(semnătura)

Comisia de îndrumare: _____ Paladi Florentin, dr. hab., prof. univ.
semnătura)

_____ Cerbu Olga, dr. în șt. f.m., conf. univ.
(semnătura)

_____ Cojocaru Igor, dr. în inf., conf. univ.
(semnătura)

Chișinău, 2024

CUPRINS

ADNOTARE

BRICEAG Valentin: „Analiza și creșterea nivelului de maturitate a sistemului de management al securității informației pentru entități din Republica Moldova (pe exemplul băncilor comerciale)”.

Teză de doctor în informatică, Chișinău, 2024.

Structura tezei: teza este scrisă în limba română și constă din introducere, trei capitole, concluzii generale și recomandări, bibliografie 93 de titluri și 4 anexe. Teza conține 141 de pagini cu text de bază, 54 figuri și 10 tabele. Rezultatele obținute sunt publicate în 8 lucrări științifice cu volum total de circa 7 coli de autor.

Cuvinte-cheie: Securitatea Informației (SecInf), Securitatea cibernetică (SC), Sistem de Management al Securității Informației (SMSI), Model Multiprofil de Maturitate a Securității Informației (M^3SI), Baza generică de date M^3SI, Profil de securitate a informației tipic unei industrii (PSITI), Profil individual de securitate a informației (PISI) pentru o entitate concretă.

Scop: elaborarea unui model multiprofil de maturitate a securității informației cu suport informatic pentru evaluarea și creșterea nivelului de maturitate.

Obiective: Crearea unei baze generice de date M^3SI privind cunoștințele despre cadrele de abordare, cerințe, amenințări, riscuri și controale de securitate a informației; Elaborarea aplicației instrumentale de suport a modelului multiprofil M^3SI, a profilurilor tipice unor industrii PSITI și a profilurilor PISI pentru entități concrete; Generarea, aprobarea și validarea unui profil tipic PSITI pentru activitatea bancară, stabilirea valorilor țintă ale criteriilor de măsurare și evaluarea conform PISI.

Noutatea și originalitatea științifică: modelul generic M^3SI, profilul tipic PSITI și profilurile particulare PISI cu controale, criterii și metrici specifice, instrumentul software de suport pentru M^3SI și procesul de evaluare sunt originale și potrivite pentru diferite entități și contexte diferite de utilizare.

Rezultatul obținut care contribuie la soluționarea unei probleme științifice importante îl constituie baza de cunoștințe despre cadrele de abordare și controalele de securitate a informației și generarea modelelor multiprofil conforme unor cerințe tipice comune și specifice individuale, pentru cazuri particulare, concrete.

Semnificația teoretică este determinată de sintezarea bazei de cunoștințe, a modelelor, profilurilor, controalelor de securitate a informației, a criteriilor de evaluare și măsurare a maturității conform cerințelor tipice și particulare.

Valoarea aplicativă constă în aportul substanțial al modelelor, profilurilor generate și a aplicației de suport pentru măsurarea și evaluarea nivelului de maturitate a securității informației, aplicabile pentru un cerc larg de organizații și utilizatori evaluatori, auditori ai securității informației.

Implementarea rezultatelor: modelele M^3SI, PSITI, PISI și aplicația de suport au fost implementate în BNM pentru activitățile de supraveghere și evaluare a SecInf a BC din Moldova.

ANNOTATION

BRICEAG Valentin: "Analysis and Enhancement of the Information Security Management System Maturity Level for the Republic of Moldova Entities (Case Study - Commercial Banks)".

PhD thesis in computer science, Chisinau, 2024.

Thesis structure: the thesis is written in Romanian and consists of an introduction, three chapters, general conclusions and recommendations, a bibliography of 93 titles and 4 appendices. The thesis contains 141 pages of basic text, 54 figures and 10 tables. The obtained results were published in 8 papers with a volume of over 7 sheets of author.

Keywords: Information Security (IS), Cyber Security (CS), Information Security Management System (ISMS), Multiprofile Information Security Maturity Model (M^3SI), Generic Database M^3SI, Information Security Profile Typical of an Industry (PSITI), Individual Information Security Profile (PISI) for a specific entity.

Research purpose: the development of a multi-profile information security maturity model with TI support for evaluating and increasing the maturity level of information security.

Research objectives: Create a generic M^3SI database of knowledge about IS approach frameworks, requirements, threats, risks and controls; Development of the instrumental support application of the M^3SI multi-profile model, of the typical for an industry profile PSITI and of the individual PISI profile for concrete entity; Generating, approving and validating a typical PSITI profile for banking activity, establishing the target values of the measurement criteria and evaluation according to PISI.

Scientific novelty and originality: The generic M^3SI model, the typical PSITI profile and the particular PISI profiles with specific controls, criteria and metrics, the software tool supporting the model M^3SI and the evaluation process are original and suitable for different entities and different contexts of use.

The obtained result, which contributes to solving of an important scientific problem, is the database with the knowledges about the information security approach frameworks and controls and the generation of multi-profile models conforming to typical common and specific individual requirements, for particular, concrete cases.

The theoretical significance it is determined by the synthesis of the knowledges base, information security models, profiles, controls and their evaluation and measurement of the criteria for evaluating and measuring their maturity according to typical and particular requirements.

The applicative value: it consists in the substantial contribution of the generated models, profiles and the supporting application in the measurement and evaluation of the maturity level of IS, applicable to a wide area of organizations and user's evaluator-auditors of IS.

Implementation of the results: the M^3SI, PSITI, PISI models and the auxiliary application were implemented in the NBM for supervisory activities and assessment of information security of banks in Moldova.

АННОТАЦИЯ

Бричаг Валентин: «Анализ и повышение уровня зрелости системы управления информационной безопасностью для предприятий Республики Молдова (на примере коммерческих банков)».

Докторская диссертация по информатике, Кишинёв, 2024.

Структура диссертации: диссертация написана на румынском языке и состоит из введения, трех глав, общих выводов и рекомендаций, библиографии из 93 названий и 4-ёх приложений. Диссертация содержит 141 страниц основного текста 54 рисунков и 10 таблиц. Полученные результаты опубликованы в 8-и научных работах с общим объёмом около 7 авторских листов.

Ключевые слова: информационная безопасность (ИБ), кибербезопасность (КБ), система управления информационной безопасностью (СУИБ), многопрофильная модель зрелости информационной безопасности (M^3SI), универсальная база данных M^3SI, типичный для отрасли профиль информационной безопасности (PSITI), Индивидуальный профиль информационной безопасности (PISI) для конкретной организации.

Цель: разработка многопрофильной модели зрелости ИБ с ИТ-поддержкой для оценки и повышения уровня зрелости.

Подцели: создание базы данных M^3SI, содержащее обобщённые знания о подходах к ИБ, о требованиях, угрозах, рисках и средствах контроля ИБ; разработка инструментального приложения для поддержки многопрофильной модели M^3SI, типовых отраслевых профилей PSITI и индивидуальных профилей PISI для конкретных объектов; разработка, утверждение и валидация типового профиля PSITI для банковской деятельности, установление целевых значений критериев и оценка согласно PISI.

Научная новизна и оригинальность: генерирующая модель M^3SI, типичный для отрасли профиль PSITI и индивидуальные профили PISI для конкретных объектов со специфическим контролями ИБ, критериями и показателями, программный инструмент, для поддержки модели M^3SI и процесса оценки – являются оригинальными и подходят для различных объектов и различных конкретных контекстов использования.

Полученный результат, способствующий решению важной научной задачи, является обобщённая база знаний по основным общепризнанным подходам и управлению ИБ и построение на их основе многоуровневых моделей, соответствующих типовым отраслевым и конкретным индивидуальным требованиям, для конкретных частных случаев.

Теоретическая значимость: определяется синтезом базы знаний, критериев оценки зрелости и их измерения в соответствии с типовыми и специфическими/частными требованиями.

Прикладная ценность: заключается в существенном вкладе моделей, профилей и вспомогательного приложения для измерения и оценки уровня зрелости ИБ, применимого к широкому кругу организаций и пользователей оценщиков и аудиторов ИБ.

Внедрение результатов: модели M^3SI, PSITI, PISI и вспомогательное приложение были внедрены в НБМ для надзорной деятельности и оценки ИБ банков Молдовы.

LISTA ABREVIERILOR

BC	*Bancă comercială*
BD	*Bază de date*
(ISC)²	*The International Information System Security Certification Consortium*
BNM	*Banca Națională a Moldovei*
BSC	*Balanced Scorecard, o metrică de performanță a managementului strategic*
CAATs	*Computer Assisted Audit Techniques, tehnici de audit asistate de computer*
CEN	*The European Committee for Standardization*
CENELEC	*European Electrotechnical Committee for Standardization*
CGEIT	*Certification / Certified in Governance of Enterprise IT*
CIA	*Confidențialitate, Integritate Accesibilitate (Disponibilitate)*
CIS	*Centru de securitate internet (din engl.)*
CIS CSAT	*CIS Controls Self-Assessment Tool*
CISA	*Certified Information Systems Auditor*
CISM	*Certified Information Security Manager*
CMMC	*Cybersecurity Maturity Model Certification*
CMMI	*Capability Maturity Model Integration*
COBIT	*Control Objectives for Information Technologies*
CRISC	*Certified in Risk and Information Systems Control*
CVE	*Common Vulnerabilities and Exposures*
e.g.	*De exemplu, provine din latinescul „exempli gratia”*
DoS, DDoS	*Atac de blocare a serviciilor (engl. Denial of Service, Distributed DoS)*
ENISA	*European Network and Information Security Agency*
ETSI	*European Telecommunications Standards Institute*
GDPR	*Regulamentul general al UE privind protecția datelor cu caracter personal*
HCE	*Hotărârea Comitetului Executiv*
HIPAA	*Legea privind mobilitatea și responsabilitatea în asigurări de sănătate (engl. Health Insurance Portability and Accountability Act, S.U.A.)*
IDS	*Sistem (software) de detecție a intruziunilor (din engl.)*
IEC	*Comisia internațională pentru electrotehnică (din engl.)*
IoB	*Internetul afacerilor (din engl. Internet of Business)*
IoT	*Internetul lucrurilor sau Lucruri Internet (din engl. Internet of Things)*
IPS	*Sistem (software) de prevenție a intruziunilor (din engl.)*
ISACA	*Asociația profesională internațională axată pe guvernarea tehnologilor și sistemelor informaționale (Information Systems Audit and Control Association)*
ISO	*Organizația Internațională de Standardizare (din engl.)*
ISO27k	*Familia de standarde ISO/IEC 27000 privind securitatea informației*

ITIL	*Bibliotecă de infrastructură TI (din engl. TI Infrastructure Library)*
ITU	*Uniunea Internațională a Telecomunicațiilor (din engl.)*
KBS	*Societate Informațională Bazată pe Cunoaștere (Knowledge Based Society)*
M^{3}SI	*Model multiprofil de maturitate a securității informației*
MM	*Model de maturitate*
MSAT	*Din engl. Microsoft Security Assessment Tool*
NIST	*Institutului Național de Standardizare și Tehnologie (din engl.)*
NM	*Nivel de maturitate*
OCEG	*Open Compliance and Ethics Group*
O-ISM3	*The Open Group Information Security Management Maturity Model*
OSI	*Ofițer pentru securitatea informației*
OWASP	*Din engl. Open Web Application Security Project, o metodologie stabilită la nivel mondial pentru evaluarea vulnerabilităților aplicațiilor web*
PCI DSS	*Standard pentru securitatea industriei plăților cu carduri bancare (din engl. Payment Card Industry Data Security Standards)*
PDCA	*Ciclul îmbunătățirii continue a lui Deming (din engl. Plan-Do-Check-Act)*
PISI	*Profil individual/particular de securitate a informației (profil individual)*
PSITI	*Profil de securitate a informației tipic unei industrii (profil tipic)*
RM	*Republica Moldova*
SADD	*Sistem/servicii automatizate de deservire la distanță*
SANS	*Institutul SysAdmin Network Security*
SC	*Securitate cibernetică*
SecInf	*Securitatea Informației*
SGBD	*Sistem de gestiune a bazelor de date*
SI	*Sistem informațional, și/sau/inclusiv sistem informatic (engl. Information System)*
SIEM	*Managementul securității informațiilor și evenimentelor (din engl.)*
SM	*Sistem de management*
SMB	*Small and Medium Business*
SMSI	*Sistem de Management al Securității Informației*
SO	*Sistem de operare*
SoA	*Declarația (sferei, ariei) de aplicabilitate a SMSI și/sau a auditului SMSI*
TI	*Tehnologii Informaționale (engl. Information Technology, TI)*
TIC	*Tehnologii Informaționale și comunicaționale (engl. I&CT)*

INTRODUCERE

Actualitatea și importanța temei abordate. Succesul unei organizații moderne, indiferent de sfera sa de activitate, de dimensiune, forma de proprietate etc., depinde de înțelegerea rolului pe care informațiile îl joacă în viața sa și de gestionarea eficientă a acestor informații, inclusiv de asigurarea securității informației. SecInf este un proces desfășurat, de regulă, într-un mediu aflat în continuă schimbare, care **se maturizează** *(crește, se îmbunătățește)* de-a lungul timpului în funcție de cerințe, cultură, scop urmărit, investiții, personal implicat etc.

Astăzi **securitatea informației este un subiect fierbinte**, prezent pe agenda majorității conferințelor internaționale și naționale. De exemplu: *Conferința OSCE „Oameni, încredere, reziliență: construirea securității cibernetice pentru toți”*, octombrie 2023; Con*ferința internațională de securitate cibernetică „CyberCon”,* Romania, mai, 2023; *Conferința Internațională cu genericul „Securitatea Cibernetică în Republica Moldova: Provocări, Tendințe și Soluții”*, octombrie 2023. Anual în lume și în UE sunt desfășurate diverse *campanii tematice de sensibilizare în domeniul SecInf* precum *„Luna europeană a securității cibernetice”,* susținute și promovate de toate țările membre ale UE, inclusiv de RM și nu numai.

Întreprinderea publică „Serviciul Tehnologia Informației și Securitate Cibernetică” (STISC) oferă sistematic noutăți privind SecInf, e.g. *https://stisc.gov.md/ro/comunicate-de-presa/noutati-din-domeniul-securitatii-cibernetice-2022024/*, diverse **programe de conștientizare a SecInf,** e.g. *https://stisc.gov.md/ro/constientizare/*. Conștientizarea este recunoscută ca cea mai prioritară acțiune de asigurare a SC. **Securitatea Informației a devenit o disciplină** studiată în majoritatea instituțiilor universitare, inclusiv din RM. De exemplu, în cadrul proiectului Erasmus+ LMPI *(https://www.lmpi-erasmus.net)*, patru cele mai mari universități din Moldova (USM, UTM, ASEM, Universitatea Alecu Russo din Bălți) începând cu anul 2018 au introdus la ciclul I licență și ciclul II masterat un șir de cursuri speciale, precum:

- Metode criptografice de protecție a informației;
- Securitatea sistemelor informatice;
- Administrarea și securitatea rețelelor de calculatoare;
- Mijloace tehnice de protecție a informației;

- Gestiunea securității informatice/informației;
- Auditul securității informatice/informaționale;
- Securitatea informației întreprinderii;
- Securitatea web aplicațiilor;
- Securitatea tranzacțiilor electronice și altele.

Actualmente majoritatea absolută a persoanelor fizice și juridice, a organizațiilor private, publice, guvernamentale etc. sunt prezente în spațiul digital/virtual global, fără careva frontiere bine definite și clar delimitate. **Prezența masivă a oamenilor și organizațiilor în spațiul virtual constituie o sursă majoră a riscurilor de securitate pentru datele personale și informațiile sensibile** manipulate în spațiul cibernetic, dar care sunt valoroase pentru o persoană fizică, o organizație, o regiune sau un stat.

Pe de altă parte, **există diverse mituri, confuzii** care duc la tratarea eronată a securității informației: confundarea conceptelor de Securitate a Informației, Securitate Cibernetică, Securitate Informatică etc.; iluzia precum că datele, informațiile nu sunt atât de valoroase, încât merită să se cheltuiască bani cu asigurarea lor; alte iluzii precum că SecInf rezidă exclusiv în securitatea TI, SI și este exclusiv grija departamentului TI și că cumpărarea mai multor instrumente poate consolida SC și multe altele.

Conform estimărilor de la ***Statista*** privind perspectiva securității cibernetice, costul global al criminalității cibernetice este de așteptat să crească în următorii cinci ani de circa 3 ori, de la 8,44 trilioane USD în 2022 la 23,84 trilioane USD în 2027 [1]. Alte statistici ce denotă importanța SecInf sunt aduse în compartimentul „*1.3. Importanța, provocări și probleme majore de SecInf în activitatea bancară”*.

Dar ce are comun **Securitatea informației** cu **Securitatea cibernetică**? Anticipând și fără a intra în prea multe detalii, SC este o subcategorie a SecInf [2]. **Securitatea informațiilor** este un domeniu mai larg, ce acoperă mai multe domenii, cum ar fi securitatea fizică, protejarea informațiilor de amenințări precum dezastrele naturale și altele. **Securitatea cibernetică** se referă, în primul rând, la **amenințările legate de tehnologie**, cu practici și instrumente care le pot preveni sau atenua. Cadrul conceptual și definitoriu de Securitate a informației și SC sunt aproximativ aceleași în majoritatea surselor, e.g. ISO/IEC 27000:2018 [3], ISO/IEC 27032:2012. Iar pentru a corespunde modificărilor ISO/IEC 27001:2022, în versiunea ISO/IEC 27032:2023 [4], în clauza 3.6 SC este precizată ca ***„protecția oamenilor, societății, organizațiilor și națiunilor împotriva riscurilor cibernetice”***. În toată familia de standarde ISO27k conceptele SecInf/SC se referă la *„conservarea confidențialității, integrității și disponibilității informației”*, cu diferența că SecInf

se limitează doar la informația în format digital din spațiul cibernetic/sistemele cibernetice și că actualmente informațiile sunt preponderent în format digital. În marea majoritate a cazurilor, securitatea cibernetică acoperă cca 95% din securitatea informației [2] și doar o mică parte a activelor informaționale continuă să circule în format tradițional pe hârtie.

Pentru că există abrevierea general acceptată de SI pentru sisteme informatice/ informaționale, abrevierea pentru Securitatea informațiilor în prezenta lucrare este SecInf. Iar termenii de **SecInf/SC**, în esență puțin diferiți, adesea **vor fi folosiți cu sens interschimbabil.** Sub abrevierea SC, acolo unde este potrivit contextului, se poate subînțelege și ca securitatea informației.

SC și **asigurarea securității informației în spațiul cibernetic devine o preocupare majoră a tuturor** actorilor implicați de la diferite niveluri, pornind de la persoane fizice *(protecția datelor personale),* organizații particulare și publice *(universități, școli, spitale, primării, bănci etc. cu necesitatea de protecție a datelor sensibile),* și terminând cu nivelul organelor guvernamentale de reglementare și supraveghere *(de exemplu Ministerul Educației, Ministerul Sănătății, Ministerul Finanțelor, Banca Națională, Inspectoratul Fiscal de Stat, Serviciul Tehnologia Informației și Securitate Cibernetică etc.),* unde se concentrează responsabilitatea elaborării și aplicării de politici de securitate coerente în domeniul respectiv la nivel de industrie, de stat sau la nivel global pe anumite industrii.

Pierderile, și ca urmare importanța securității informației, au crescut esențial după pandemia COVID-19 (2019-2022), simultan cu migrarea *„peste noapte”* a majorității organizațiilor spre **telelucru, teleeducație** etc. cu accesarea de la distanță a datelor sensibile. Iar procesul de asigurare a securității informațiilor în asemenea condiții nu mai este doar apanajul specialiștilor de TIC, ci și a întreg personalului implicat. SC cere o atenție și o implicare a managementului de vârf și de toate nivelurile, care definesc strategiile, politicile și necesitățile organizației în analiza, evaluarea și tratarea riscurilor de securitate a informațiilor [5, 28].

Încadrarea temei în preocupările internaționale, naționale în context inter-/ și transdisciplinar. Tema cercetată **se încadrează perfect și corelează puternic cu strategiile și bunele practici generate de organizații globale recunoscute.** Printre cele mai importante sunt dezvoltatorii standardelor sistemelor de management *(și audit, ca componentă indispensabilă a oricărui SM)* și organizațiile ce oferă certificări profesionale în domeniul SecInf precum:

- Asociația mondială de Audit și Control a Sistemelor Informaționale *(ISACA, www.isaca.org) cu renumitul său produs COBIT, numeroase publicații și cărți, jurnal periodic (de 6 ori pe an) și certificările specialiștilor recunoscute la nivel global, precum CISA, CISM, CGEIT, CRISC etc.;*

- Institutul Național de Standardizare și Tehnologie din S.U.A. *(NIST, http://nist.gov), cu renumitele serii de Publicații Speciale ce țin de SC (NIST SP 800-53, NIST SP 800-50, NIST SP 800-39, NIST SP 800-37, NIST SP 800-61);*
- Comitetul pentru securitatea datelor din industria cardurilor de plată *(PCI SSC, https://www.pcisecuritystandards.org) cu produsul său de bază PCI DSS;*
- Organizația Internațională pentru Standardizare *(ISO, https://www.iso.org/)* și Comisia internațională pentru Electrotehnică *(IEC, https://www.iec.ch/homepage/)* cu sute de standarde agreate la nivel internațional de experți și care descriu **cel mai bun mod de a face ceva,** inclusiv în domeniul SecInf (familia de standarde ISO27k), managementul riscului (ISO 31000), managementul serviciilor TI (ITIL, ITSM ISO/IEC 20000) etc.;
- Institutul SANS *(Sysadmin Network Security, http://sans.org, S.U.A.),* renumit pentru produsul său comun cu Centrul de Internet Securitate *(https://cissecurity.org) „Top CIS 20 Critical Security Controls"*, ajuns la versiunea 8 și pentru *SANS Security Policy Project (Free Security Policy Templates)* cu zeci de șabloane de politici uzuale în domeniul SC și pentru cele peste 40 de cerificări *GIAC (Global Information Assurance Certification);*
- (ISC)², *The International Information System Security Certification Consortium*, organizație mondială de certificare profesională, înființată în 1989 care a creat și menține actual **corpul comun de cunoștințe CBK** *(Common Body of Knowledge)*, pe care se bazează certificările profesionale recunoscute drept standard global de excelență: *CISSP, SSCP, CCSP, CAP, CSSLP, HCISPP, ISSAP, ISSEP etc*. Pentru detalii privind certificările (ISC)² a se vedea *(https://www.isc2.org/Certifications#/);*
- Institutul European de Standardizare în domeniul Telecomunicațiilor *(ETSI, https://www.etsi.org);*
- OCEG *(Open Compliance and Ethics Group, http://oceg.org),* cu produsul său O-ISM3 *(http://ism3.com);*
- Agenția Uniunii Europene pentru Securitate Cibernetică – *ENISA (https://www.enisa.europa.eu/)*, care se bazează pe activitatea organizațiilor europene de standardizare precum *CEN (The European Committee for Standardization), CENELEC (European Electrotechnical Committee for Standardization, https://www.cencenelec.eu/), ETSI* (*European Telecommunications Standards Institute, https://www.etsi.org/)*, responsabile pentru dezvoltarea și definirea standardelor voluntare la nivel european. **ENISA sprijină dezvoltarea, ratificarea și**

testarea în timp util a standardelor aplicabile la nivel global pentru sistemele, aplicațiile și serviciile TIC și multe altele.

Detalii privind produsele, standardele dezvoltate, instrumentele administrate a se vedea adresele web oficiale ale acestor principale organizații în domeniul SecInf/SC, toate accesate/verificate la data 28.02.2024.

Scop urmărit. Sarcina de implementare și de îmbunătățire continuă a proceselor de gestionare a SecInf/SC într-o entitate concretă trebuie să corespundă obiectivelor afacerii, cerințelor contextului intern și mediului extern de reglementare și de supraveghere *(profil PISI);* să țină cont de specificul industriei *(profil PSITI)* și de starea curentă a SecInf, de riscurile informaționale, de cultura informațională corporativă *(politicile de SecInf)* și cea a personalului implicat în SecInf etc. Ca urmare, pentru a construi, organiza și asigura cu succes SecInf într-o entitate, pornind de la analiza necesității, identificării cerințelor, riscurilor etc., este nevoie de un **model individual simplu, transparent și ușor de adaptat la contexte specifice/concrete,** care să fie utilizat pentru evaluarea stării SecInf, care ar susține nevoile tuturor actorilor implicați de la toate nivelurile, pornind de la managerii de vârf, profesioniștii și experții de securitate etc., până la utilizatorii finali, conectați la rețea de la stații terminale, adesea aflate la distanță și negestionate de entitate.

Realizarea „manuală” a unor asemenea profiluri PSITI/PISI necesită cheltuieli importante de bani și de timp, precum și un personal înalt calificat. **Automatizarea și intelectualizarea** procesului de realizare a profilurilor și a evaluării nivelului de maturitate a SecInf conform PISI ar putea soluționa problema. În acest sens, rezultatele preconizate presupun adoptarea unui c**adru generic unic/model multiprofil de maturitate a SecInf** M^3SI cu o bază de date unică privind cunoștințele de SecInf, din care sunt generate profiluri tipice și particulare ale SecInf, potrivite necesităților concrete de analiză, măsurare și îmbunătățire continuă a SecInf. În rezultatul realizării cercetării modelul M^3SI, profilurile tipice PSITI și profilurile individuale PISI cu controale, criterii și metrici specifice, precum și procesul de evaluare a SecInf au ca suport un instrument software original simplu și intuitiv, potrivit pentru diferite entități și diferite contexte concrete de utilizare.

Pentru atingerea acestui scop au fost realizate următoarele **obiective majore**:

- Studiul diverselor cadre de abordare și de reglementare a SecInf, analiza, și cartografierea relațiilor între ele cu crearea unei baze generice de date M^3SI privind cunoștințele despre **cadre, zone de securitate, cerințe, amenințări, riscuri și controale** de SecInf;

- Studiul, analiza și clasificarea cerințelor de SecInf specifice unor industrii, cu elaborarea unor **profiluri de securitate a informației tipice unei industrii PSITI**, e.g. pentru domeniul bancar și a **profilurilor individuale de securitate a informației PISI**, e.g. pentru o bancă comercială;
- **Elaborarea web aplicației de suport** și administrare a modelului multiprofil M^3SI, a profilurilor tipice PSITI și a profilurilor individuale PISI;
- **Generarea-aprobarea-validarea unui profil PSITI** pentru BNM și a unui profil PISI pentru o bancă comercială ipotetică;
- **Evaluarea nivelului de maturitate** a SecInf a unei entități conform profilului PISI.

Ipoteza de cercetare. Conform lui Peter Drucker, unul dintre cei mai cunoscuți și influenți gânditori și scriitori în domeniul teoriei și practicii managementului, considerat **fondatorul managementului modern,** doar *„Ceea ce se măsoară, se îmbunătățește. Ceea ce se măsoară, se gestionează”*. Prima ipoteză rezultă din acest celebru citat și se referă la necesitatea acută a **unui instrument adecvat pentru a măsura, evalua, compara, gestiona SecInf**. A doua ipoteză este **a simplifică, pe cât este de posibil, abordarea SC** astfel, încât gestiunea să fie inclusiv și pe măsura necesităților și pe măsura puterilor organizațiilor medii/mici referite ca SMB care nu întotdeauna dispun de resurse suficiente, de cadre profesionale cu calificările necesare. Justificarea este legată și de terminologia instabilă, de marea diversitate a unghiurilor de vedere diferite, de multitudinea cadrelor de reglementare și controale de SecInf, de specificul, individualitatea entităților etc., care face abordarea SecInf foarte complexă chiar și pentru profesioniști.

În cadrul tezei de doctorat se propune un model de maturitate și o aplicație-suport de automatizare a gestionării SecInf/SC în baza acestui model. Pornind de la automatizarea operațiilor rutinare privind inventarierea activelor, amenințărilor și riscurilor informaționale, evidenței dispozitivelor mobile și/sau de domiciliu, cu acces la distanță, evidența resurselor informaționale critice/valoroase pentru afacere, care poate spori esențial calitatea gestionării SecInf. Și terminând cu evaluarea maturității proceselor de gestionare a SecInf, susținută de *măsurări, evaluări, raportări, comparări* a nivelului de maturitate [6, 7] ca verigă centrală pentru planificarea-realizarea îmbunătățirea continuă a SecInf a unei organizații și remedierea vulnerabilităților în timp util.

Focusarea cercetării. SecInf poate fi extrem de diferită pentru diferite industrii și întreprinderi de diferite mărimi, în special entități mici-mijlocii/SMB. Problemele, amenințările, riscurile, soluțiile, costurile SecInf sunt diferite pentru diferite organizații, industrii și domenii de activitate *(e.g. educație, medicină, servicii bancare, e-afaceri, e-guvernare),* deoarece cerințele și contextele interne/externe, infrastructurile, produsele utilizate și personalul implicat sunt

diferite. În general, SecInf include: securitatea infrastructurilor critice *(tehnologiile informaționale, sistemele informaționale, rețele private intranet/extranet, Internet etc.)*, securitatea web și securitatea bazelor de date, securitatea tranzacțiilor etc. în toate entitățile subordonate, asociate sau relaționate. În esență, toate acestea rezidă în **probleme de management** și de **factor uman**, care depind, în mare parte, de amploarea entității și de cultura informațională. Subiectul de bază este **proiectarea unui model de maturitate generic**, care să vizeze provocările diferitelor organizații și industrii. Iar ieșirea specifică a cercetării/produsul final este modelul tipic PSITI și profilul individual PISI al SecInf pentru o oarecare organizație sau o parte a acesteia în funcție de formă, apartenență, mărime. Pentru soluționarea acestor probleme umane și de management, cercetarea este focusată pe **diminuarea complexității proceselor de planificare-măsurare-evaluare-îmbunătățire a SecInf** și a influenței factorului uman prin automatizarea operațiilor rutinare de realizare a profilurilor tipice și particulare de SecInf, precum și a activităților de apreciere a riscurilor, inclusiv de colectare a măsurărilor și de evaluare a nivelului de maturitate.

Metodologia utilizată. Pentru dezvoltarea modelului de maturitate M^3SI [7], care ar permite determinarea stării actuale a SecInf/SC, a SMSI și direcțiile prioritare de dezvoltare a acestora a fost utilizat conceptul de „model de maturitate", general acceptat la nivel global, de exemplu standardul O-ISM3 [8], [9], [10].

Modelul de maturitate M^3SI [7] se bazează, în temei, pe **sintezarea metodologiilor și modelelor de securitate** deschise, publice, ținând cont de cerințele principalului standard sistemic ISO/IEC 27001:2022 [11], urmărind simplificarea și automatizarea, pe cât e posibil, a procesului de evaluare a SecInf și de gestiune a SMSI conform principiilor general acceptate de către ISO pentru orice tip de SM. Modelul de maturitate este folosit ca instrument de măsurare a stării unui proces pe baza **unui set de metrici**, care reprezintă caracteristici specifice. Evaluarea acestor metrici permite o mai bună înțelegere a stării actuale a proceselor SMSI, a riscurilor aferente și a direcțiilor de creștere a maturității proceselor de SecInf, SMSI și a organizației în ansamblu. Baza de date a aplicației conține cele mai bune practici de SecInf, inclusiv specifice pentru diferite industrii, este adaptabilă/extensibilă și permite crearea profilurilor particulare pentru entități și misiuni concrete, potrivite pentru măsurarea și evaluarea sistematică a nivelului de maturitate în scopul îmbunătățirii continue.

Rezultatele tezei includ adoptarea unui cadru generic unic – **Model multiprofil de maturitate a SecInf M^3SI**, cu o bază de date unică privind cunoștințele despre cadrele de abordare și controalele de SecInf, din care sunt generate în mod inteligent **profiluri tipice și particulare** de SecInf, potrivite necesităților concrete de analiză, măsurare și îmbunătățire continuă a SecInf.

Modelul M^{3}SI, profilurile tipice industriei PSITI, profilurile particulare PISI în baza controalelor, criteriilor și metricilor prestabilite și procesul de evaluare a SecInf cu cinci niveluri de maturitate de la 1 *(starea inițială)* la 5 (*îmbunătățire continuă)* au ca suport **un instrument software original simplu și intuitiv**, potrivit pentru diferite entități și diferite contexte concrete.

Importanța/valoarea aplicativă a rezultatelor obținute constă în funcționarea mai sigură a organizațiilor. Profilurile tipice PSITI și cele particulare rezultante PISI, simple și transparente, permit diferitelor entități implementarea, gestionarea eficientă și îmbunătățirea continuă a SecInf, ceea ce, la rândul său, conduce la atingerea mai sigură a obiectivelor de afaceri.

Aplicația instrumentală de suport a modelului M^{3}SI simplifică și ușurează esențial gestionarea SecInf , automatizând operațiile rutinare de administrare a bazei de date cu cunoștințele despre riscuri, cerințe și controale specifice, de generare a profilurilor particulare, de evaluare a nivelului de maturitate și urmărire a progresului. Aplicația M^{3}SI este de tip **web cu acces controlat** de către autor, este disponibilă la adresa *https://www.m3-si.eu/.* Toate acestea luate împreună permit diferitelor entități *organizarea, abordarea și gestionarea eficientă a securității informației,* prevenirea și combaterea mai eficientă a riscurilor și amenințărilor în adresa securității informației, urmărirea evoluției maturității în timp și/sau compararea maturității SecInf între entități tipice.

Aprobarea rezultatelor cercetării. Rezultatele științifice obținute de autor în cadrul tezei au fost prezentate **în cinci rapoarte la trei conferințe științifice internaționale** diferite și au fost **publicate în trei reviste diferite**, inclusiv una din România și două în reviste de categoria B incluse în Registrul Național al RM privind revistele de profil. Pentru detalii a se vedea lista publicațiilor autorului la tema tezei.

Volumul și structura tezei. Teza este scrisă în limba română cu titlu de manuscris, este tehnoredactată și imprimată la calculator. Lucrarea este structurată în introducere, 3 capitole, concluzii generale și recomandări, bibliografie și anexe cu un total de 173 pagini.

Sumarul compartimentelor tezei. În „Introducere" este elucidată convingător relevanța și importanța temei de cercetare în baza celor mai actuale surse și statistici despre starea domeniul SC și principalele provocări. Sunt descrise scopul, obiectivele tezei, rezultatele preconizate noutatea științifică a lor, valoarea teoretică și aplicativă a rezultatelor tezei.

Capitolul *„1. Analiza stării actuale a securității informației în sectorul bancar al Republicii Moldova"* realizează o trecere în revistă a stării SecInf, identifică unele **probleme și provocări majore** legate de SecInf și de e-transformarea, schimbarea continuă a valorilor, structurilor, fenomenelor, proceselor, modului de a lucra, învăța, a se distra etc. prin utilizarea

masivă TIC, Internet și Web în toate domeniile activității umane, prin hiper-conectivitatea rețelelor, oamenilor, entităților.

Capitolul *„2. Aspecte teoretice, metodologice și practici de abordare a securității informației prin prisma SMSI”* prezintă succint aspectele teoretice, metodologice și practice de abordare a SecInf; abordări moderne a SecInf bazată pe standarde de bune practici, pe riscuri și pe modele de maturitate, principalele direcții și recomandări de organizare și îmbunătățire continuă a SMSI. Securitatea informației implementată corect în condițiile migrării afacerilor în spațiul cibernetic, a telelucrului în masă și a accesului de la distanță a informațiilor sensibile **presupune o noua abordare, orientată nu doar pe soluții tehnice-tehnologice, pe TIC și pe sisteme informaționale tradiționale**, dar și pe securitatea dispozitivelor mobile, de domiciliu cât și pe securitatea IoT, IoB, cloud etc., inclusiv pe **schimbarea paradigmei** de pe abordarea preponderent tehnică-tehnologică spre abordarea organizațională în cadrul sistemelor de management, care ar permite controlul și monitorizarea eficientă a riscurilor cibernetice.

Capitolul *„3. Model multiprofil de maturitate a securității informației M^3SI”* prezintă esența inovativă a cercetării prin abordarea modernă a SecInf în baza standardelor deschise, modelului de maturitate multinivel cu suport informatic, ce permite generarea modelelor tipice unor industrii PSITI și a modelelor individuale PISI particularizate în acord cu politicile corporative concrete, standardele directoare ale familiei ISO27k, valorile țintă ale criteriilor de evaluare a maturității SecInf.

În *„Concluzii finale și recomandări”* se face o totalizare a sarcinilor propuse spre soluționare și a principalelor rezultate obținute, inclusiv validarea lor teoretică și practică-aplicativă.

Citarea în text este realizată în conformitate cu cerințele SM ISO 690:2022 [12] **în sistemul numeric cu cifre între paranteze pătrate** în ordinea în care sursele sunt referite pentru prima dată. Citările ulterioare ale aceleiași surse de informații păstrează numărul primei ei citări.

Pentru figurile și tabelele împrumutate sau adaptate sunt date referințe la surse. Lipsa referințelor la surse pentru tabele și figuri semnifică implicit că acestea sunt elaborate de autor.

Cunoașterea este prin ea însăși putere.
(Francis Bacon)

1. ANALIZA STĂRII ACTUALE A SECURITĂȚII INFORMAȚIEI ÎN SECTORUL BANCAR AL REPUBLICII MOLDOVA

Cunoașterea este putere îndeosebi în adoptarea deciziilor. Capitolul curent are ca scop cunoașterea cerințelor și stării SecInf în domeniul bancar, **identificarea problemelor majore legate de SecInf** în băncile comerciale din RM și **justificarea actualității SecInf**. Informațiile despre SMSI proprietare constituie secretul firmei și nu pot fi făcute publice. Însă provocările și problemele majore de SecInf în industria bancară sunt comune, cerințele și reglementările sunt aceleași, legate în principal de **accesul de la distanță** la mijloacele aflate în contul clientului în scopul obținerii de informații privind starea contului, efectuarea de plăți, alimentarea contului și alte tranzacții preponderent electronice.

De regulă, tranzacțiile sunt realizate prin soluții informatice, bazate pe utilizarea TIC, SI, pe comunicarea prin Internet/Web și telefonia mobilă, puse de o bancă la dispoziția clientului sub formă de **sisteme/servicii automatizate de deservire la distanță**/SADD fie prin **internet-banking**, fie prin **mobile-banking**. Asemenea aplicații permit clientului prin intermediul unei metode de autentificare și al unui mijloc de comunicație să aibă acces de la distanță la mijloacele aflate în cont în scopul obținerii de informații privind starea contului, efectuării tranzacțiilor în numele și la ordinul clientului etc. Iar identificarea **criteriilor unice comune de creștere a nivelului de maturitate a SecInf,** pornind de la cadrul legal unic al activității băncilor din Republica Moldova, a **principalelor aplicații, instrumente și soluții informatice** precum și a **provocărilor moderne de SecInf** constituie una din principalele sarcini ale tezei**.** Realizarea acestui deziderat, la rândul său, permite conceperea și îmbunătățirea continuă a SMSI pentru băncile din RM în deplin acord cu bunele practici globale de abordare a SecInf, recomandate de diverse organisme internaționale recunoscute prin numeroase standarde, directive și reglementări.

1.1. Cadrul legal și de reglementare al sectorului bancar din Republica Moldova

Sub titlul curent sunt examinate succint conceptul de SecInf/SC și setul de Legi importante ale RM, regulamente ale BNM și regulamente interne ale BC, ce prescriu crearea și îmbunătățirea continuă a SMSI ca mijloc de gestionare și asigurare eficientă a SecInf/SC în domeniul bancar.

Actualmente probabil că nu există organizație care să nu opereze date cu caracter personal, să nu dispună de mijloace hardware-software, TI, SI, de o rețea corporativă, de un Web site, de acces la Internet etc. Există zeci de tipuri de legi și reglementări în vigoare aplicabile într-o măsură mai mare sau mai mică entităților bancare și care pot intra sau nu în sfera SMSI, în funcție de măsura de manipulare cu acestea, mărimea entității, genurile de afaceri. De exemplu:

- *Normele tehnice în domeniul semnăturii electronice avansate calificate*, aprobate prin ordinul directorului Serviciului de Informații și Securitate al Republicii Moldova nr. 69 din 15.07.2016;
- *Legea nr. 467 din 21.11.2003 cu privire la informatizare și la resursele informaționale de stat;*
- *Legea nr. 241 din 15.11.2007 privind comunicațiile electronice;*
- *Cerințele minime obligatorii de securitate cibernetică* aprobate prin Hotărârea Guvernului nr. 201 din 28.03.2017;
- *Legea nr. 20 din 03.02.2009 privind prevenirea și combaterea criminalității informatice* și multe altele, și doar unele dintre cele mai importante pentru contextul tezei vor fi succint examinate în continuare.

Examinarea detaliată a acestora nu intră în sfera tezei, dar pot f utile pentru definirea NM.

1.1.1. Conceptul de securitate a informației/securitate cibernetică

Securitatea ca concept generic reflectă **starea de funcționare normală, durabilă și continuă a oricărei entități**, inclusiv a băncilor comerciale din sistemul bancar al RM. Pentru buna funcționare mecanismele de securitate trebuie să fie capabile să facă față unei game largi de **riscuri, atacuri, amenințări, accidente** sau **calamități,** care trebuie tratate în mod previzibil, simultan și/sau post factum, cu **asumarea conștientă a riscurilor** în limita unor costuri raționale, suportabile. Iar **securitatea informației** semnifică c**onservarea celor trei proprietăți fundamentale** ale informației – CIA în orice formă a sa: *electronică, pe suport de hârtie etc.* Caracteristicile primare ale informației ce constituie obiectul SecInf sunt referite în literatura de specialitate ca **triada CIA** și sunt definite în ISO/IEC 27000:2018 [3]: *Confidentiality/ Confidențialitate (clauza 3.10), Integrity/Integritate (clauza 3.36), Availability/Accesibilitate sau Disponibilitate (clauza 3.7)*. Totodată, SecInf se referă și la alte câteva atribute adiționale secundare, realizate în baza celor fundamentale. Este vorba de **posesia informației** *(cine este stăpânul, posesorul, responsabilul),* **utilitatea informației** *(sau semnificația,* c*u atât mai mare, cu cât informația este mai valoroasă, mai accesibilă),* **autenticitatea informației** *(clauza 3.6), (informațiile neautentice pot constitui dezinformații),* **contabilizarea** *(în engleză accountability,*

de exemplu pentru justificarea achitărilor reciproce), **non-repudierea** *(sau imposibilitatea dezicerii de unele acțiuni efectuate, e.g. plasarea unei comenzi, clauza 3.48)* și **fiabilitatea** *(clauza 3.55)* a standardului referit mai sus. SecInf se referă și la **protejarea tuturor resurselor implicate** în gestiunea informației de-a lungul transformărilor semnale-date-informații *(Fig. 1.1)*.

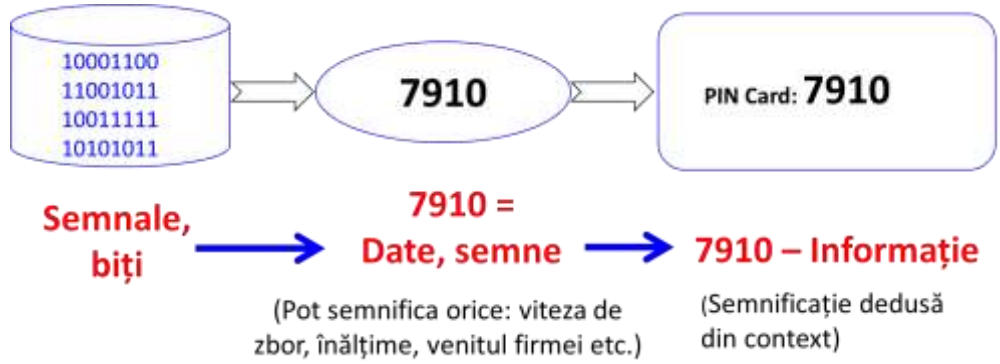


Figura 1.1. Relația semnale-date-informații

SecInf se **referă la toate formele și dispozitivele** electronice de stocare utilizate *(Fig. 1.2)*, fiecare dintre ele fiind însoțite de riscuri specifice e.g. de pierdere, deteriorare etc.

Figura 1.2. Exemple de dispozitive electronice de stocare a datelor/informațiilor

Materializarea informației poate fi sub diferite forme: *Exprimată prin vorbire; Scrisă sau imprimată pe hârtie sau alți purtători solizi; Stocată/procesată electronic; Transmisă/comunicată prin mijloace de comunicație clasice (e.g. poștă) sau electronice (e.g. e-mail, messinger); Înregistrată pe diverse tipuri de suporturi (RAM, CD-rom, format audio/video etc.).* Conform

„*Recomandărilor cu privire la obiectivele de control și măsurile de securitate ale SMSI”* elaborate de BNM pentru BC [13] ***„Resurse informaționale*** *– orice informație utilizată în cadrul proceselor de activitate a entității, sau orice bun material sau nematerial implicat direct sau indirect în crearea, procesarea, stocarea și accesarea informației în cadrul proceselor de activitate (de exemplu: date, aplicații program, soft de sistem, echipamente de calcul, alte elemente de infrastructură).* ***Resursă informațională sensibilă*** *– resursa informațională, compromiterea securității căreia poate implica riscuri majore pentru entitate”.*

Tot acolo este definit cadrul de organizare a *SecInf, e.g. clauza 3.1. Politica de securitate a informației, 3.2. Organizarea SMSI; Responsabilitatea pentru resurse (clauza 4.1); Clasificarea informației (clauza 4.2); Capitolul V. Cerințe de securitate privind resursele umane; Capitolul VI. Securitatea fizică și a mediului de lucru etc.* Pentru alte detalii a se vedea sursa citată.

Confidențialitatea informației implică o ierarhizare a nivelurilor de clasificare a informațiilor, o ierarhizare a drepturilor de acces pe niveluri diferite de încredere, o specificare a modurilor de păstrare și distrugere etc. Informațiile sensibile ale unei entități trebuie grupate și marcate. De exemplu: **informații confidențiale/strict confidențiale** *(secret de stat, secret de firmă)*, care nu pot fi divulgate, dezvăluite decât în anumite situații prevăzute de lege; **informații cu difuzare restricționată**, e.g. pentru anumite roluri, servicii; **informații interne**/de uz intern al entității, a căror accesare sau diseminare neautorizată ar putea produce prejudicii entității; **informații publice**, cu difuzare liberă, nerestricționată, nelimitată.

Informațiile confidențiale sunt esențiale pentru afaceri, cad sub incidența unor legi, reglementări etc. Aceste informații sunt accesibile doar persoanelor autorizate ale entității, de regulă un cerc restrâns și prestabilit de către top-managementul firmei. Accesul, utilizarea și partajarea acestor informații de către persoane neautorizate este considerat ca încălcare a SecInf.

Pentru a indica necesitatea, prioritățile și gradul de protecție, **informațiile trebuie clasificate**. De regulă, informațiile în diferite entități pot fi clasificate în diferite moduri. Încadrarea informațiilor entității în diferite categorii se realizează prin reglementări interne, elaborate și aprobate în conformitate cu reglementările organelor superioare sau de supraveghere și determină nivelul cerințelor de SecInf. Clasificarea informațiilor este un document de uz intern al entității.

De exemplu, **informațiile de uz intern** doar în cadrul entității, ca și informațiile private care sunt accesibile numai anumitor angajați, nu ar trebui să fie accesibile sau vizibile de terțe persoane, altele decât angajații unității. Informațiile partajate între unitățile entității intră în această clasă. Datele cu caracter personal ale angajaților, definite ca **date cu caracter sensibil**, constituie date de uz intern și pot fi stocate și procesate, dezvăluite etc. conform prevederilor Legii RM 133 [14] la nivel național, iar la nivel global al UE – de GDPR [15]. Stocarea și procesarea informațiilor

personale care nu sunt relevante pentru entitate și/sau nu sunt prevăzute de lege constituie deficiențe ale SMSI și/sau încălcarea SecInf, care poate fi sancționată la nivel național mai moale, dar la nivelul UE destul de dur.

Categoria în care este încadrată o informație sensibilă în cadrul entității ar trebui indicată în mod explicit și neechivoc prin marcaje specifice, fie aplicate prin redactare electronică, fie prin etichetare, fie prin notificări succinte și directe privind caracterul informațiilor respective. **Securitatea axată pe confidențialitate** asigură că informația poate circula numai pe același nivel de clasificare/încredere sau la niveluri superioare, **reglementează drepturile și regulile de acces** în funcție de nivelul de încredere al subiecților *(oameni, dispozitive, procese)* și clasificarea obiectelor. De regulă, între nivelurile de încredere și clasificare există o relație de dominare (de sus în jos), cu proprietățile **reflexivă, antisimetrică, tranzitivă.**

1.1.2. Cadrul legal al SMSI ca mod de gestionare a securității informației

Actualmente securitatea informației a devenit **o problemă organizațională acută**, gestionată în mod strategic, tactic și operațional-continuu printr-un sistem de management cu valoare incorporată, bazată pe investiții, abordată în mod procesual și reglementată de numeroase organisme naționale și internaționale de standardizare [7].

De regulă, SecInf/SC este asigurată în cadrul unor **SMSI proprietare**, care variază în funcție de industrie, mărimea și locația entității, domeniul și obiectul de activitate al organizației, strategiile și politicile interne în acord cu reglementările în vigoare și cadrul legal aferent. Iar realizarea SMSI presupune seturi de controale *(preventive, detective, corective)* și proceduri operaționale, ce asigură caracteristicile primare și secundare ale informației, protecția tuturor activelor și resurselor informaționale din cadrul entității, inclusiv personal, tehnologii informaționale și comunicaționale, servicii de suport etc. pentru a ține sub control **riscurile și incidentele de SecInf** la un nivel acceptabil prestabilit. În acest sens, SecInf se referă la diversitatea formelor de manifestare a informației și diversitatea dispozitivelor și tehnologiilor informaționale și comunicaționale în procesele de stocare-procesare-transmitere. SecInf include ca și componente majore securitatea cibernetică, care, la rândul său include **securitatea rețelei corporative, securitatea internet/web și securitatea aplicațiilor informaționale**.

Conceptul de securitate a informației se referă atât la informațiile non-digitale, cât și la informațiile digitale din spațiul cibernetic; atât la persoane fizice, private, cât și la orice organizații publice, de afaceri, guvernamentale etc., în teza numite generic **entități**.

Ca urmare a informatizării principalelor procese operaționale și tranzacționale ale unei bănci și a creșterii continue a costurilor crimelor cibernetice, SecInf a devenit o problemă critică pentru succesul afacerilor bancare și necesită o **abordare transversală, în adâncime**, **aliniată** la standardele globale general acceptate, la strategiile naționale, la strategiile și obiectivele locale specifice organizației.

Băncile comerciale din RM operează cu date și procese complexe, reglementate de o serie de acte normative naționale și internaționale. De regulă, bunele practici și reglementări globale în domeniul securității informației prevalează. Dar multe dintre acestea nu sunt obligatorii. De exemplu, certificarea conform PCI DSS nu este cerută pentru toate băncile, ci doar pentru entitățile-procesatoare de tranzacții cu carduri bancare. O bancă-procesator de tranzacții cu carduri bancare este obligată să-și certifice acest sistem. Certificarea conform COBIT sau conform ISO/IEC 20000 sau ISO/IEC 27001 etc. este benevolă și decizia aparține entității. Totodată, entitățile care au și aplică eficient un SMSI certificat conform ISO/IEC 27001 sau un sistem de plăți cu carduri bancare certificat conform PCI DSS, chiar dacă nu sunt obligate să o facă, au șanse mai mari față de concurenți, inclusiv de participare în granturi, proiecte, concursuri internaționale etc. În același timp, este de menționat că **certificarea nu garantează performanța**. Performanța SecInf depinde de buget, de capacitatea și angajamentul tuturor celor implicați în administrarea și utilizarea TI, SI.

Sectorul bancar în Republica Moldova funcționează pe două niveluri: Banca Națională a Moldovei și 11 bănci comerciale *(https://bnm.md/ro/content/bancile-licentiate-din-republica-moldova/)*. BNM realizează funcțiile de reglementare și supraveghere a activității băncilor și relațiile cu acestea în conformitate cu *Legea cu privire la BNM nr. 548-XIII* din 21.07.1995 cu modificări din 2020 [16]. Legea de bază care reglementează activitatea băncilor este *Legea privind activitatea băncilor nr. 202* din 06 octombrie 2017 [17]. Lichidarea băncilor, reglementarea valutară, activitățile de creditare etc. nu constituie subiectul tezei.

Specificul tezei este axat pe SADD, serviciile TIC, plăți cu carduri, e-banking etc., reglementate la nivel de național de un set de legi și regulamente precum:

- Lege Nr. 105 din 13.03.2003 privind protecția consumatorilor;
- Lege Nr. 299 din 21.12.2017 privind aprobarea Concepției securității informaționale a Republicii Moldova;
- Lege nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic;
- Lege cu privire la serviciile de plată și moneda electronică nr. 114 din 18.05.2012;
- Recomandări cu privire la obiectivele de control și măsurile de securitate ale SMSI, aprobate de Guvernatorul BNM în 2010 cu modificări din 01.07.2015;

- Regulament cu privire la cardurile bancare, aprobat HCE BNM nr 62 din 24.02.2005;
- Regulament cu privire la sistemele de control intern în bănci, aprobat prin HCE al BNM Nr. 96 din 30.04.201;
- Regulament privind cerințe minime pentru Sistemele Informaționale și de Comunicare ale băncilor, aprobat prin HCE al BNM nr. 47 din 14 martie 2018;
- Regulament privind cadrul de administrare a activității băncilor, aprobat prin HCE al BNM nr. 322 din 20.12.2018.

O listă completă a regulamentelor specifice activității BNM și BC a se vedea la adresa *https://www.bnm.md/ro/content/lista-regulamentelor*. Versiunile oficiale, îndeosebi a legilor în vigoare, sunt disponibile la *https://www.legis.md*. Dar examinarea aspectelor de SecInf în cadrul acestor legi specifice, chiar și „pe diagonală", ar necesita prea mult spațiu, incomensurabil cu cel posibil în cadrul unei teze de doctor.

Organizarea SecInf și SMSI în cadrul unei bănci este realizată în baza *Regulamentului cu privire la sistemele de control intern în bănci*, aprobat de BNM prin Hotărârea sa HBN96/2010 din 30.04.2010, cu modificări din 01.07.2017 în baza Hotărârii HBN146 din 07.06.17 [18].

Utilizarea SADD pentru **efectuarea de plăți preponderent în mod electronic cu carduri bancare**, eventual cu bani virtuali (e-/web-many), sisteme de e-banking, Internet/online banking, mobile-banking și/sau **automate bancare/ATM,** și/sau sisteme automate de auto-deservire/**POS terminale** *(Point of Sale)* sau **terminale „Self-service**" constituie grija și partea principală a SecInf. Apropo, conform unui raport al Fondului Monetar Internațional citat de incomemagazine.ro la 14 februarie 2024 *(https://viza.md/category/tags/automate-bancare) RM are cea mai mare concentrație de automate bancare*.

La nivel global activitățile BC sunt reglementate de **standardele-pereche ISO/IEC 27001** [11] **și ISO/IEC 27002** [19] **ediția a III din 2022**, GDPR [15], PCI DSS v4.x din noiembrie 2023 [20]**,** Regulamentul UE 2017/2402 al Parlamentului European și al Consiliului UE din 12 decembrie 2017 de stabilire a unui cadru general pentru securitizare și de creare a unui cadru specific pentru securitizare simplă, transparentă și standardizată și de modificare a Directivelor și Regulamentelor Comisiei Europene (CE): 2009/65/CE din 2009, 138/CE, 2011/61/UE, nr. 1060/2009/CE și nr. 648/2012/UE. Prin acestea și alte directive **UE stabilește standarde tehnice de reglementare**, care precizează informațiile ce trebuie furnizate în conformitate cu cerințele privind notificarea STS *(Securitizare Transparentă și Standardizată),* formularele pentru furnizarea de informații în conformitate cu cerințele privind notificarea STS, terțele părți care verifică respectarea criteriilor STS [21] etc.

1.1.3. Scopul și obiectivele SMSI pentru asigurarea securității informației

Abordarea securității informației corporative în baza SMSI este global recunoscută.

Scopul SMSI pentru o BC este de a oferi o viziune clară referitor la sistemele de protecție și prevenire a atacurilor asupra informației și activelor informaționale sub orice formă. Principalele cerințe de securitate a informației, de stabilire a SMSI, de implementare și funcționare a SMSI, de monitorizare și revizuire a SMSI, de menținere și îmbunătățire a SMSI, de documentare a SMSI sunt expuse în *Regulamentul cu privire la sistemele de control intern în bănci* [18], secțiunea 3, clauzele 33-37 și în secțiunea 4, cerințe privind auditul intern al SMSI și în standardul [11].

Obiectivele de bază ale SMSI pentru o bancă comercială includ:

1. Consolidarea echipei cibernetice și a capacităților pentru desfășurarea de operațiuni bancare inovatoare digitizate, cu carduri bancare și în condiții de siguranță maximală posibilă, asigurate inclusiv prin rolurile de supraveghere ale SMSI, controalele de securitate, măsurarea și evaluarea riscurilor, gestionarea incidentelor de SecInf etc.;
2. Determinarea riscurilor și resurselor necesare pentru asigurarea unui grad înalt de protecție al informației și activelor informaționale în desfășurarea operațiunilor bancare;
3. Reglementarea și promovarea standardelor de securitate cibernetică actuale, formarea continuă a cadrelor băncii.

Principalele elemente arhitecturale și sarcini ale SMSI sunt prezentate în *Figura 1.3* și logica funcționării în *Figura 1.4.*

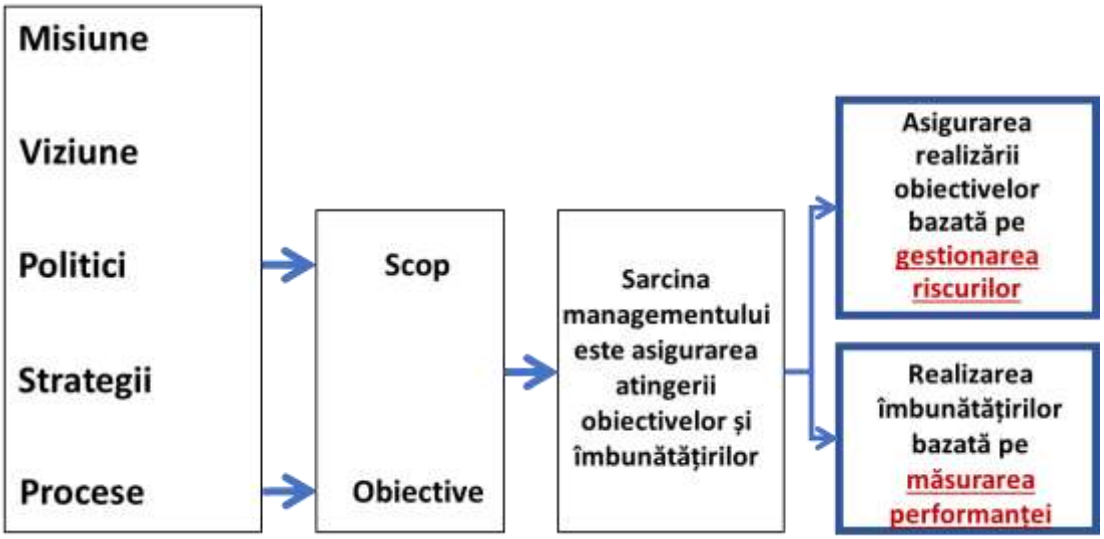


Figura 1.3 Principalele componente ale SMSI

Figurile 1.3 și 1.4, elaborate în baza standardului ISO/IEC 27001:2022, reflectă abordarea procesuală PDCA a SMSI în ciclul de analiză a performanței și îmbunătățire continuă conform

misiunii, strategiei generale de afaceri și a politicilor de securitate. Scopul și obiectivele SMSI rezidă în a asigura că:

- Băncile dispun de o strategie adecvată aferentă tehnologiei informației și comunicațiilor, aliniată la strategia generală de afaceri;
- Procesele de guvernanță internă sunt stabilite adecvat în raport cu sistemele TI, SI ale băncii;
- Cadrul intern de gestionare a riscurilor TI, SI și de control intern protejează în mod adecvat sistemele TI, SI ale băncilor;
- Sistemul de plăți online este conform cu standardul internațional de securitate a datelor din industria cardurilor de plată PCI DSS*;*
- Sunt respectate drepturile privind protecția datelor cu caracter personal conform Legii RM nr. 133 din 2011 și GDPR din 2016 cu aplicare din 2018.

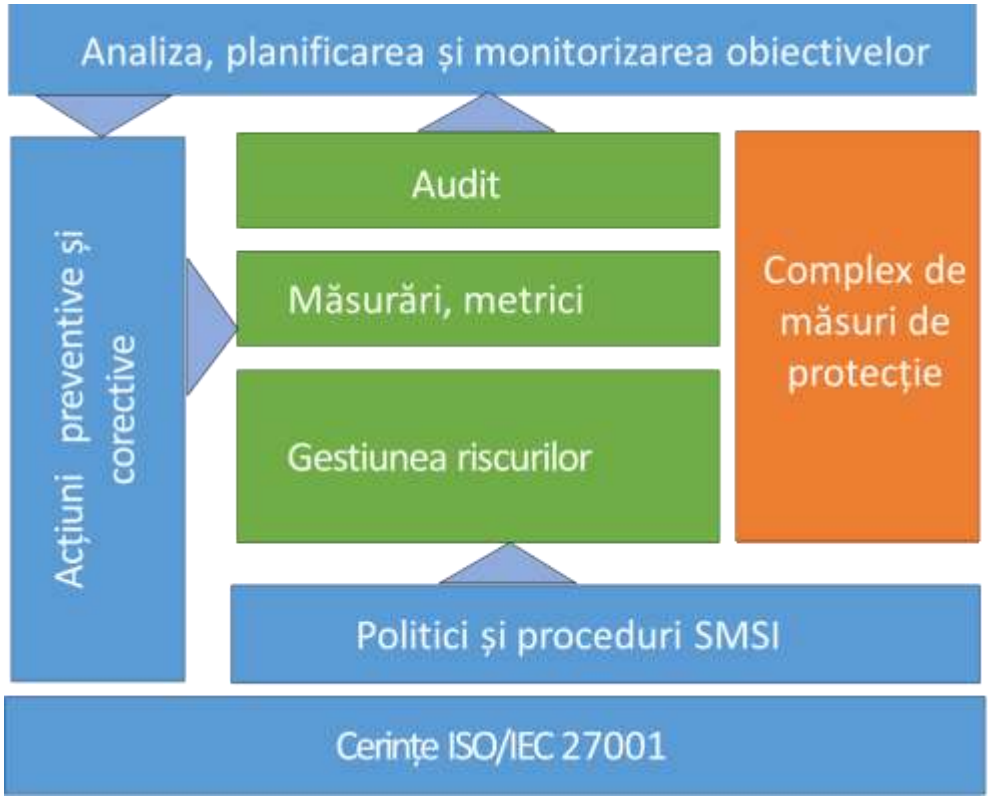


Figura 1.4. Logica funcționării SMSI

1.2. Cerințe de bază față de SMSI

Ca urmare a mediului în continuă schimbare, cerințele față de SecInf și SMSI sunt/trebuie să fie în permanentă îmbunătățire cu scopul asigurării concordanței cu prevederile legislației, cu principiile internaționale general acceptate și cele mai bune practici, inclusiv Directivele Uniunii Europene, Regulamentului BNM cu privire la sistemele de control intern în băncile din RM etc.

Un SMSI veritabil trebuie să posede un set de caracteristici obligatorii, e.g.: *să fie bine documentat/stabilit în scris; să asigure îndeplinirea cerințelor clienților; să asigure atingerea obiectivelor organizației în condiții de siguranță; să fie aplicabil în toate activitățile organizației* și altele.

Detalii privind cerințele, inclusiv de planificare, suport, operare, audit intern sistematic și/sau audit de performanță, controalele/măsurile de securitate, metricile etc. a se vedea [4], [11], [19], [47].

1.2.1. Cerințe generale privind cadrul securității informației

Ținând cont de locul și rolul informației în societatea modernă, de pătrunderea TIC în toate sferele de activitate umană și de amploarea afacerilor electronice, de digitizarea serviciilor bancare, inclusiv de plăți preponderent electronice, de creșterea criminalității informatice, de contextele individuale unice ale entităților etc., un cadru rezonabil de dezvoltare-implementare al SMSI ar trebuie să fie:

- **Scalabil** – să poată fi dezvoltat simultan cu dezvoltarea afacerii, TI, SI, SADD și adaptat la apariția noilor amenințări și riscuri conform valorii activelor informaționale;
- **Repetabil** – susținut de metodologii și procese iterative pe domeniile definite ale procesării informațiilor, cu oferirea de rezultate consistente și comparabile în timp sau între entități;
- **Defensiv** – să permită îmbunătățirea continuă bazată pe analiza riscurilor specifică contextului; utilizarea principiilor și controalelor auditabile; utilizarea proceselor și cadrelor documentate și acceptate pentru gestionarea și controlul riscului;
- **Măsurabil** – să permită măsurarea maturității/capacității SecInf, ce oferă o imagine clară a stării programului de securitate și a capacităților de performanță, a îmbunătățirii continue definite în mod obiectiv de schimbările din mediile de risc sau de afaceri;
- **Durabil** – să fie centrat pe afacere, cu proceduri definite care să sprijine creșterea eficienței proceselor de afaceri și reducerea costurilor de conformitate pe întreg ciclul de viață al informațiilor și adaptării la schimbările în mediile TI, SI și de afaceri.

Tipul controlului/măsurii de securitate conform ISO/IEC 27002:2022 [19] poate fi:

- **Preventiv** – controlul are scopul de a preveni apariția unui incident de securitate a informațiilor;
- **Detectiv** – controlul acționează atunci când are loc un incident de securitate a informațiilor;
- **Corectiv** – controlul acționează după ce are loc un incident de securitate a informațiilor.

SMSI acoperă trei zone largi de resurse, prezentate în *Figura 1.5.*

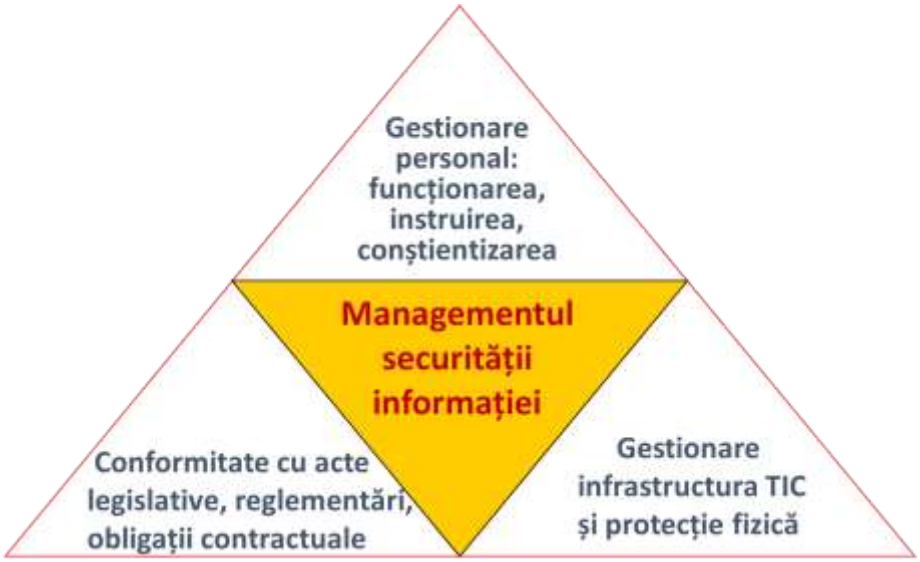


Figura 1.5. Trei zone largi de resurse gestionate în cadrul SMSI

Cele patru domenii de management ale SMSI sunt realizate prin procese, politici, proceduri, structuri organizatorice, software și hardware pentru a proteja activele informaționale *(Fig. 1.6).*

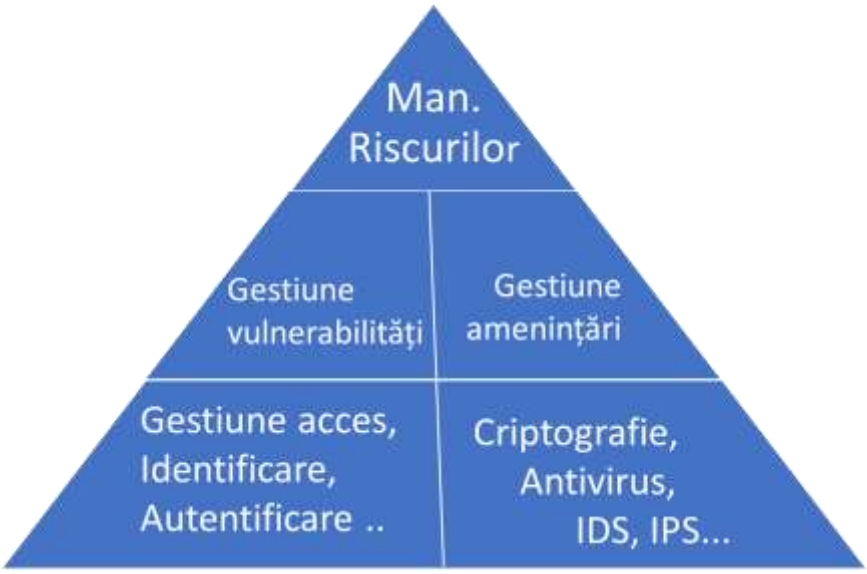


Figura 1.6. Domeniile de management ale SMSI

O viziune de ansamblu a fluxului implementării – certificări SMSI conform suitei de protocoale și forumului ISO27k este prezentat în *Figura 1.7.*

Este de menționat, nici standardul ISO/IEC 27001:2022, nici certificarea de conformitate SMSI standardului nu sunt obligatorii. Deciziile aparțin entității. Dar certificarea este singura dovadă indiscutabilă a implementării SMSI; conferă legalitate – demonstrează autorităților competente că organizația respectă legile și reglementările aplicabile în domeniu; confirmă angajamentul – ajută la asigurarea și demonstrarea obligațiilor organizației la toate nivelurile.

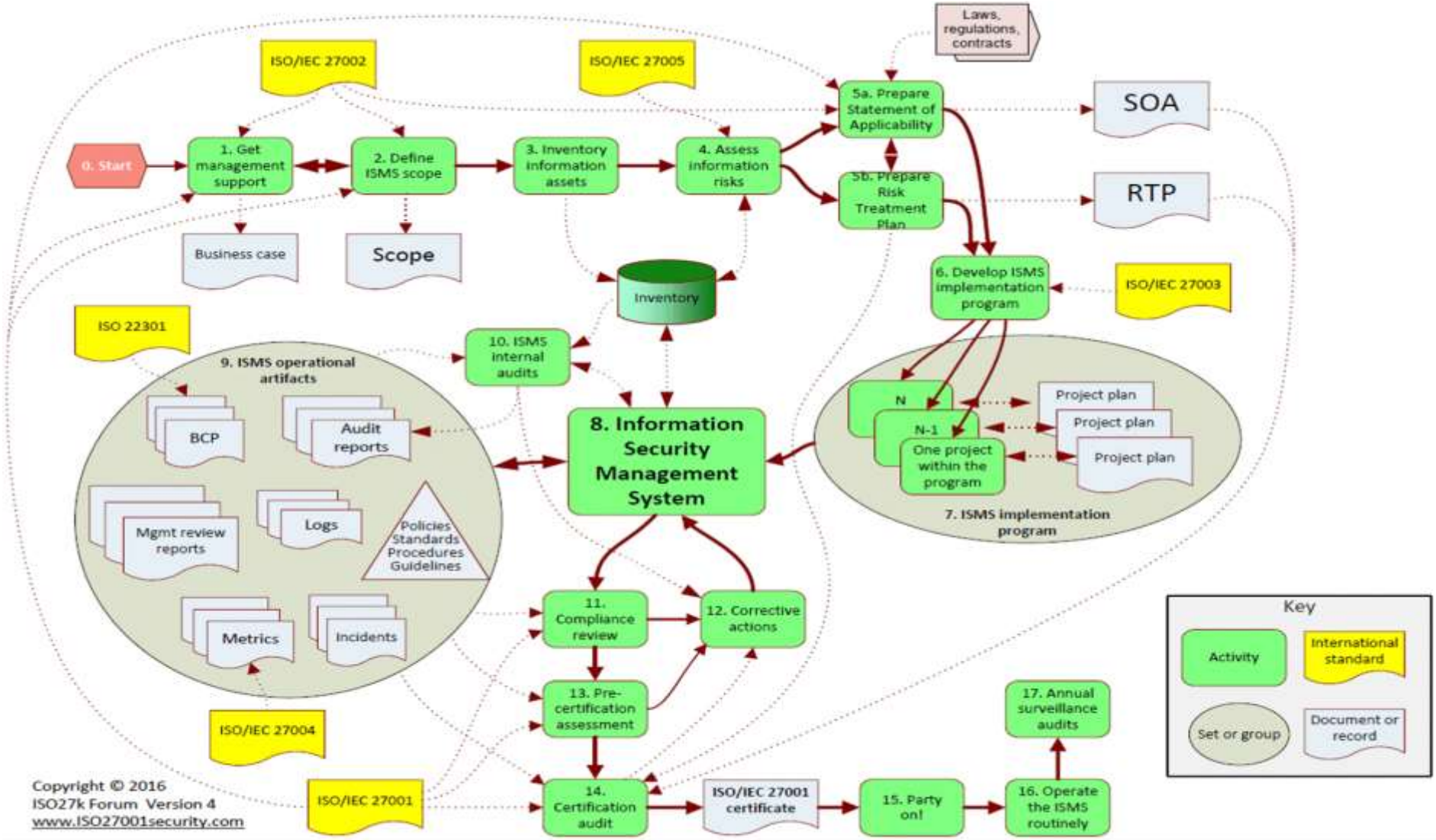


Figura 1.7. Fluxul activităților de dezvoltare-certificare SMSI

Pe de altă parte, certificarea nu garantează performanța. Performanța depinde de buget, de capacitatea și de angajamentul tuturor celor implicați în administrarea SMSI. Certificarea este o acțiune continuă, impune anumite costuri. Certificatul de conformitate valabil, de regulă 3 ani, trebuie reconfirmat în fiecare an. Prezența certificatului nu infirmă și nu confirmă starea de facto a SecInf și SMSI ca atare. Oricum, **dinamica entităților certificate în ultimii ani are o tendință pronunțată de creștere**, din 2014 până în 2022 fiind de peste 300% *(Fig. 1.8, [90])*. Acesta deoarece a crescut și continuă să crească importanța, nivelul de conștientizare, cultura SecInf.

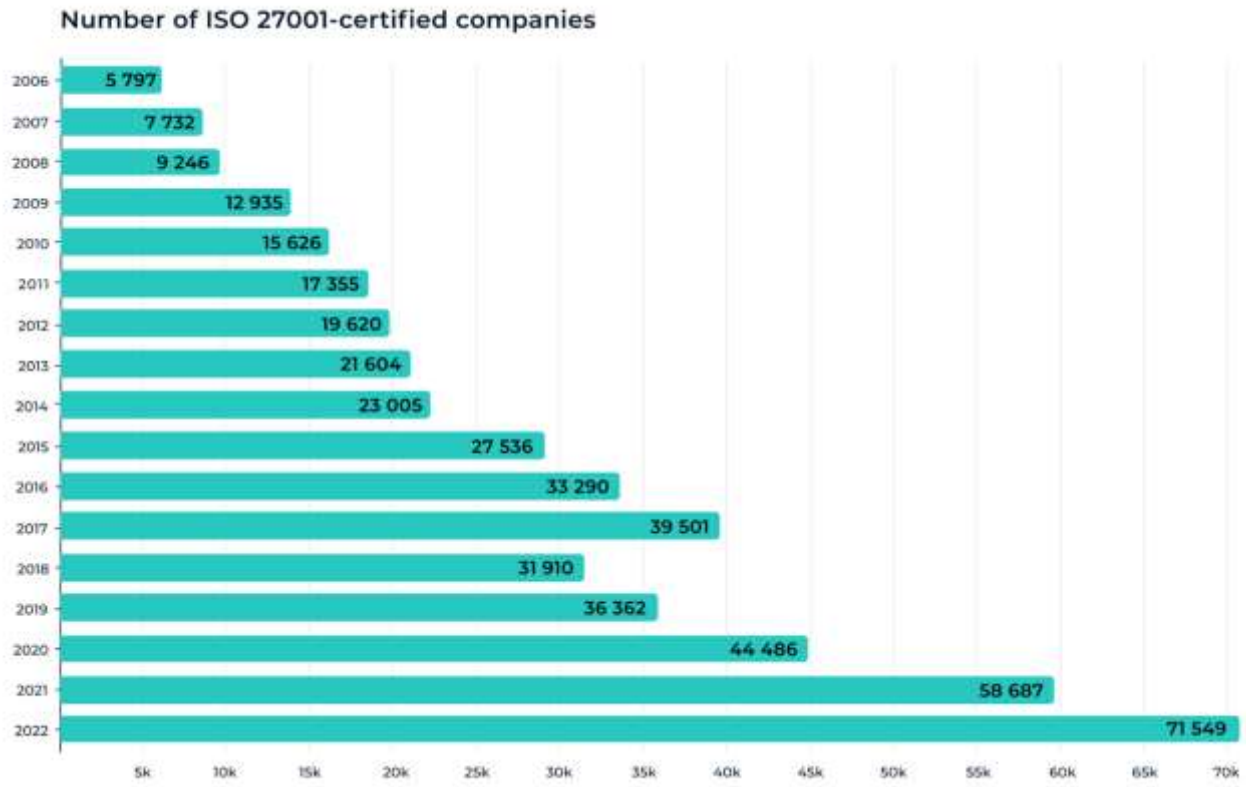


Figura 1.8. Numărul de certificate SMSI de conformitate ISO 27001 [90]

SMSI, conform cerințelor, este un sistem documentat, bazat pe dovezi, înscrisuri, planuri etc. Structurarea documentației SMSI în forma „piramidală" pe niveluri (*Fig. 1.9)* sugerează volumul, conținuturile și personalul implicat. De exemplu, nivelul de siguranță asumat de factorii de decizie este dat în *Declarația de politică a top managementului,* un document de cel mai înalt nivel, de la care pornește SecInf; adesea are un volum de până la o pagină, maximum două și care este aplicată tuturor unităților și angajaților. Documentele de nivelul patru, de la baza piramidei, sunt cele mai numeroase și voluminoase, conțin înregistrări ale proceselor și practicilor operaționale, diverse rapoarte, protocoale, registre și alte dovezi ale activităților de monitorizare, care demonstrează, certifică, validează atingerea sau nu a gradului de SecInf declarat de top

management prin implementarea activităților de SecInf în modul prescris de r*egulamente, ghiduri, manuale, proceduri* de SecInf.

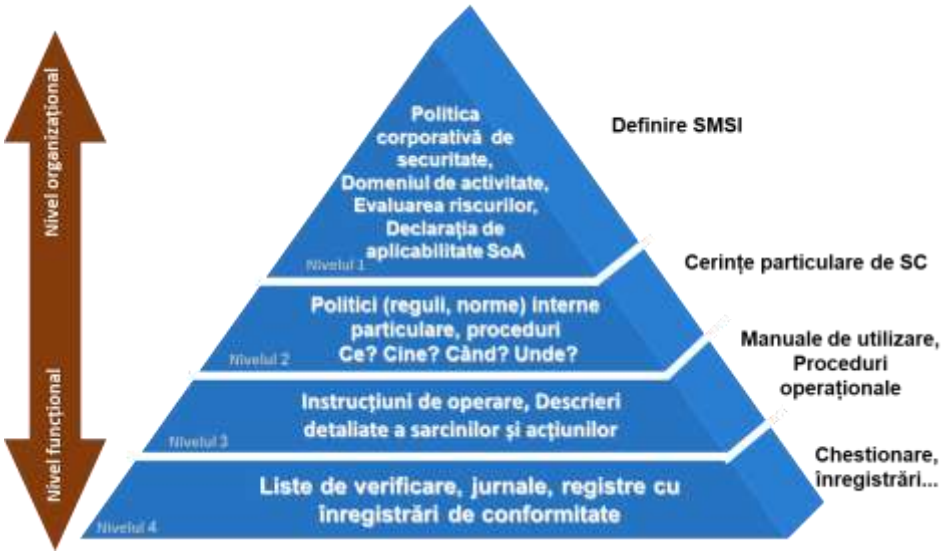


Figura 1.9. Documentele SMSI

Noua redacție a standardelor pereche ISO/IEC 27001↔ ISO/IEC 27002 din 2022 [11, 19] a introdus un **atribut pentru asocierea controalelor de SecInf la conceptele de securitate cibernetică** cu valorile definite de *Identificare; Protejare; Detectare; Răspuns; Recuperare* [75, 76]. Iar standardul de guvernare a securității informațiilor [77] oferă îndrumări responsabililor privind conceptele, obiectivele și procesele de evaluare, direcționare, monitorizare și comunicare a proceselor legate de securitatea informațiilor din cadrul entității.

Sumarul controalelor de securitate enumerate în *Anexa A (normativă)* a standardului ISO/IEC 27001 și detaliate în compartimentele 5-8 ale standardului pereche ISO/IEC 27002 includ 93 de controale grupate în patru categorii:

- Controale organizaționale (37);
- Controlul personalului (8);
- Controale fizice/de securitate fizică (14);
- Controale tehnologice (34).

Pentru detalii a se vedea standardele citate.

1.2.2. Cerințele PCI DSS

PCI SSC *(Payment Card Industry Security Standards Council)* în produsul său de bază/standardul PCI DSS *(Payment Card Industry Data Security Standard),* ajuns în 2023 la versiunea 4.x, formulează 12 cerințe pentru gestionarea datelor deținătorilor de card și menținerea

unei rețele securizate, grupate în șase obiective largi (*Fig. 1.10),* toate fiind necesare pentru ca o întreprindere să devină conformă standardului. Pentru detalii a se vedea [20], [78].

Dar, după cum a fost menționat, nu toate băncile/organizațiile ce operează cu carduri de plată sunt obligate să certifice conformitatea cu standardul, ci doar centrele de procesare a tranzacțiilor cu carduri sau cele care pot influența securitatea tranzacțiilor.

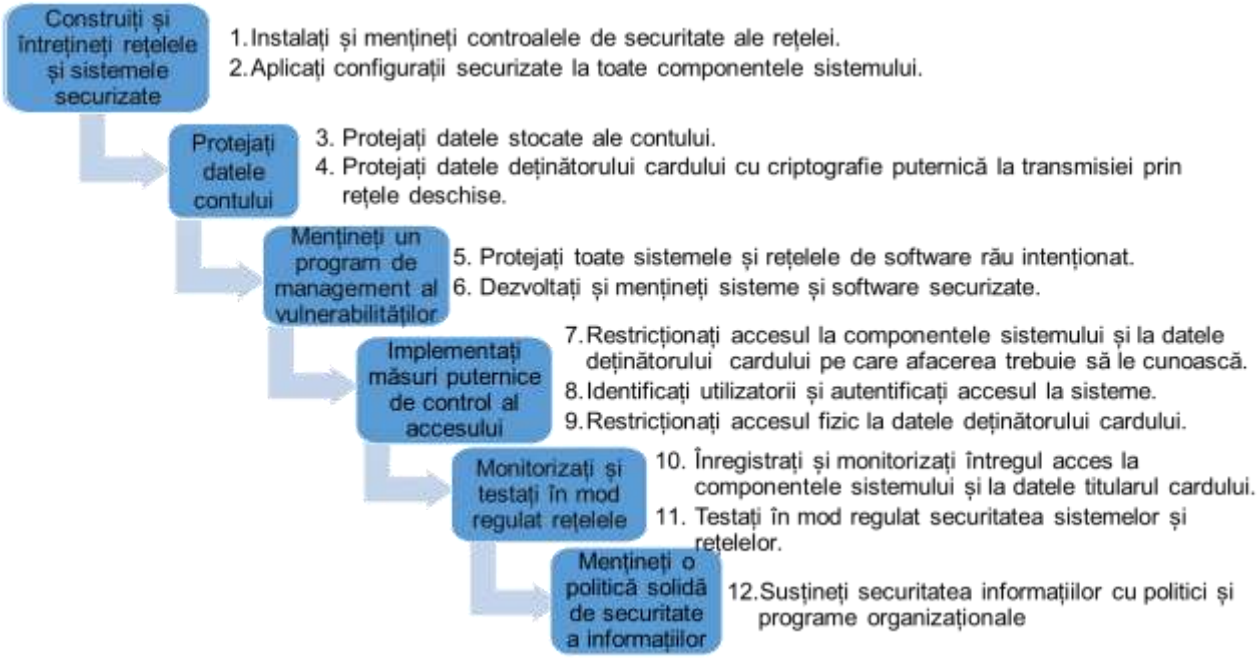


Figura 1.10. Cele 12 cerințe de conformitate PCI DSS grupate în șase arii

Nivelurile de conformitate a entităților cu PCI DSS în funcție de numărul de tranzacții efectuate cu carduri de plată pe an a se vedea *Figura 1.11* și *Tabelul 1.1*.

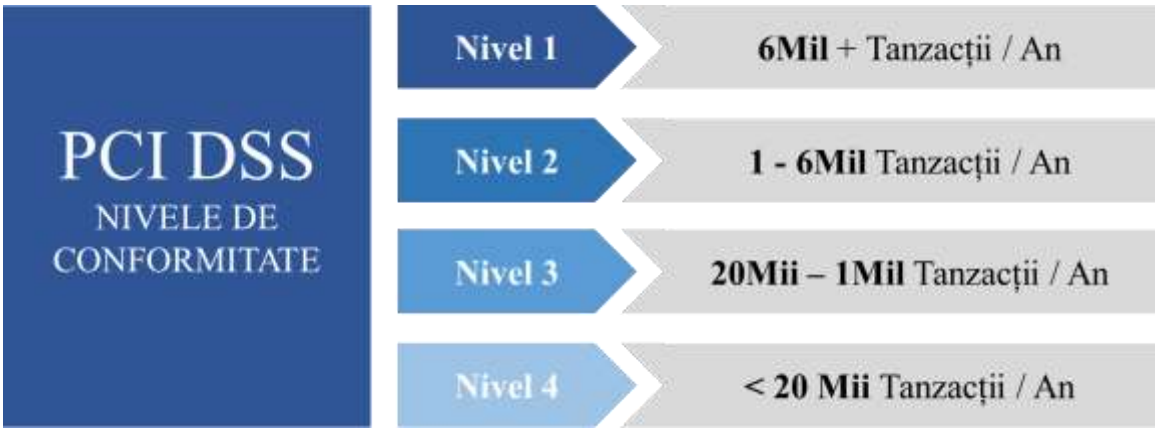


Figura 1.11. Clasificarea BC pe niveluri de conformitate cu PCI DS

(Adaptată de autor în baza [78])

Tabelul 1.1 elucidează explicit ce trebuie să facă o întreprindere (e.g. BC, comerciant) pentru a rămâne conformă cu PCI DSS în funcție de nivel/numărul anual de tranzacții.

Tabelul 1.1. Clasa entității în funcție de tranzacții cu carduri de plată pe an

Nr. nivel	Controale aferente și căror entități se aplică
1	Entități ce procesează anual **peste șase milioane de tranzacții** reale cu carduri de credit sau de debit. Control în cadrul unui audit intern de către un auditor autorizat o dată pe an + o dată pe trimestru trebuie să se supună scanării de către un furnizor aprobat.
2	**Între unu și șase milioane de tranzacții** reale cu carduri de credit sau de debit. O evaluare o dată pe an folosind un chestionar de autoevaluare (SAQ) + poate fi necesară o scanare PCI trimestrială.
3	**Între 20.000 și un milion de tranzacții** de comerț electronic anual. O evaluare anuală folosind un SAQ relevant + poate fi necesară o scanare PCI trimestrială.
4	**Mai puțin de 20.000 de tranzacții** de comerț electronic anual sau celor care procesează până la un milion de tranzacții în lumea reală. O evaluare anuală folosind un SAQ relevant și poate fi necesară o scanare PCI trimestrială.

Noua versiune PCI DSS 4.x reprezintă o schimbare semnificativă în modul în care companiile mențin conformitatea, dar are la bază același 12 cerințe *(Fig. 1.10)*, operează cu aceleași patru niveluri de conformitate PCI DSS *(Fig. 1.11)* în funcție de numărul anual de tranzacții cu cardurile de credit sau de debit procesate de o afacere.

1.2.3. Cerințe privind protecția datelor cu caracter personal

Odată cu migrarea masivă a diverselor afaceri în spațiul cibernetic virtual global (*e-educație, e-guvernare, e-distracții, jocuri electronice, e-comerț etc.)* și creșterea simțitoare a numărului de calculatoare, laptopuri, telefoane mobile și alte gadgeturi conectate la Internet și a accesibilității și folosirii lor ușoare în completarea/procesarea numeroaselor formulare și documente electronice a **crescut esențial și volumul informațiilor sensibile** care circulă pe Internet. Această afirmație se referă în special la **creșterea volumului plăților online** prin diferite aplicații de electronic banking, mobile banking, carduri bancare, monedă electronică, bani virtuali etc. și **creșterea simultană a riscurilor aferente de SecInf** prin folosirea informațiilor cu rea-intenție, furturi de identitate, fraudă, extorcare/stoarcere ilicită de bani etc.

Ca urmare, a apărut necesitatea clasificării tipurilor de informații sensibile care circulă pe Internet, care pot fi stocate și prelucrate on-line și a stabilirii unui cadru legal de reglementare. Asemenea cadre legale și reglementări există, atât pe plan național, cât și la nivel internațional, global. De exemplu, în Republica Moldova, există un șir de **strategii, legi, reglementări privind documentul electronic, semnătura electronică, securitatea cibernetică, autorități de supraveghere și control** etc.

Conform Legii cu privire la protecția datelor cu caracter personal nr. 133 din 08.07.2011 [14] „*date cu caracter personal înseamnă orice informații referitoare la o persoană fizică, identificată sau identificabilă, care poate fi identificată direct sau indirect prin referire la un număr de identificare, la unul ori mai multe elemente specifice identității sale fizice, fiziologice, psihice, economice, culturale, sociale și altele, precum nume, prenume, cod numeric personal, adresa, telefon, imaginea"* etc. Datele cu caracter personal *(de identificare, speciale etc., Fig. 1.12)* sunt considerate sensibile conform legislației RM și UE privind protecția datelor cu caracter personal și beneficiază de protecție specială.

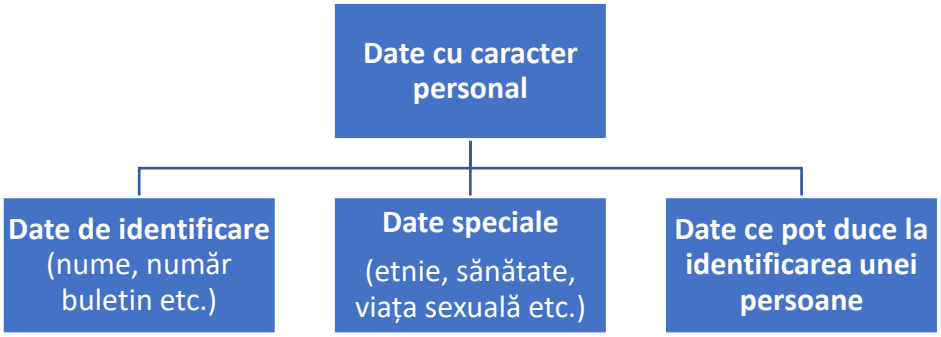


Figura 1.12. Conținutul datelor cu caracter personal

Asemenea date sunt protejate conform legilor RM și UE și pot fi stocate, procesate, prelucrate, dezvăluite de către diferite organizații și entități doar în anumite condiții legale și doar dacă există garanții speciale prescrise [14], [15].

În afară de cele prezentate în *(Fig. 1.12)* există și alte categorii speciale de date cu caracter personal, ce dezvăluie originea rasială sau etnică a persoanei, convingerile politice, religioase sau filozofice, apartenența socială, starea de sănătate, condamnările penale, sancțiunile contravenționale ș.a. Pe de altă parte, este de menționat că **nu există o listă completă de date personale care trebuie protejate**, pentru că orice informații care pot duce la identificarea unei persoane pot fi considerate date personale. De exemplu, pe lângă nume, adresă, cont bancar, amprentă, fotografie etc. **adresele IP deja pot fi considerate date cu caracter personal.** Mai mut chiar, simple cuvinte introduse într-un motor de căutare *(cum ar fi Yahoo, Bing, Google)* pot duce la identificarea unei persoane. Așa că protejarea datelor cu caracter personal ține nu doar de cadrul legal, ci și de profilul activității, de industria din cate face parte entitatea etc.

Procesarea datelor cu caracter personal semnifică orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea,

adaptarea ori modificarea, extragerea, consultarea, utilizarea, blocarea, ștergerea sau distrugerea, dezvăluirea prin transmitere, diseminare sau în orice alt mod.

Regulamentul GDPR al UE [15], aprobat de către Parlamentul European și Consiliul UE la 27 aprilie 2016 se referă la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date. GDPR a devenit aplicabil din 25 mai 2018 și oferă un cadru legal modernizat de conformitate bazat de responsabilitate pentru protecția datelor în Europa. Regulamentul prevede:

- Reguli noi pentru operatorii de date;
- O mai mare responsabilizare a acestora;
- Obligativitatea numirii unui responsabil sau a persoanei împuternicite pentru protecția datelor la nivelul fiecărui operator sau procesator de date personale;
- Rolul autorităților naționale de supraveghere;
- Măsuri corective;
- Sancțiuni pentru nerespectarea dispozițiilor regulamentului.

Conform GDPR, articolul 4, alineatele (13-15), articolul 9, art. 51-56, următoarele date cu caracter personal sunt considerate „sensibile” și fac obiectul unor condiții speciale de procesare:

- Date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice;
- Apartenența la sindicate;
- Date genetice, datele biometrice prelucrate doar pentru identificarea unei ființe umane;
- Date privind sănătatea;
- Date privind viața sexuală sau orientarea sexuală a unei persoane.

1.3. Importanța, provocări și probleme majore de securitate a informației în activitatea bancară

Prezintă elucidarea unor probleme de SecInf/SC pentru entitățile bancare și provocările majore în domeniul securității informației, care urmează să fie abordate în cadrul SMSI, demonstrează elocvent importanța securității informației.

1.3.1. Creșterea importanței informației și securității informației în societatea modernă

În prezent informația este omniprezentă, a crescut simțitor rolul ei, evaluat de către Emilia Curras *(chimistă, documentaristă și informaticiană, filozof și istoric al științei, pionier în studiul bazelor filosofice-științifice ale informației și documentării)* la nivelul celui de **al patrulea**

element vital după apă, aer și foc [22]. Conform NIST, ISO, IEC, ITU și altor organisme internaționale preocupate de domeniul TIC și aprobarea bunelor practici, **informația a devenit un bun fundamental al organizației, statului, societății, care trebuie protejat corespunzător**. Iar TIC a devenit elementul esențial în crearea, procesarea, stocarea, transmiterea, protecția și distrugerea informației. Pe măsură ce societatea se dezvoltă, crește consumul de informații și semnificația securității informației. Iar prezența masivă a oamenilor în spațiul virtual, utilizarea masivă a TIC și SI în toate domeniile activității umane au transformat informațiile în **resurse critice pentru persoane, organizații, țări** și **societate.**

Într-adevăr, astăzi informația a devenit **forța motrice a noii economii** *(digitale, electronice).* Simultan **au crescut și continuă să crească amenințările** la adresa securității informației. Astfel, organizațiile au nevoie de o mai bună protecție a informației, deoarece majoritatea afacerilor, devenite afaceri electronice, sunt desfășurate în spațiul cibernetic informațional global.

Actualmente, societatea modernă, numită Societate (Informațională) Bazată pe Cunoaștere/KBS, se află într-o evoluție vertiginoasă; este preocupată de transformarea informației digitale în valori economice și sociale și are la bază TIC moderne, Internet și Web [23]. Această mișcare de edificare a societății informaționale a fost lansată oficial de S.U.A. la 22 februarie 1993, când a fost făcut public memorandumul inaugural Clinton-Gor *„Tehnologiile pentru dezvoltarea economică a Americii”.* Ulterior, mișcarea sprijinită de UE și de țările G8 *(Canada, Franța, Germania, Italia, Japonia, Marea Britanie, S.U.A., Rusia)* a rezultat în *„Carta pentru Societatea Informațională Globală de la Okinawa*”, adoptată la 22 iulie 2000 [24].

Treptat, conceptul de KBS a câștigat tot mai mult teren, devenind o tendință și o realitate globală. Astfel, din momentul exploziei Internetului în ultimul deceniu al secolului XX, majoritatea statelor lumii au adoptat **strategii de edificare a KBS** la nivel național. În anul 2005 a fost adoptată prima Strategie Națională de edificare a Societății informaționale *„Moldova electronică”* și respectivul plan de acțiuni pentru realizarea acesteia, iar în 2013 – a II-a strategie, *„e-Moldova/Moldova digitală 2020”*, aprobată prin Hotărârea Guvernului nr. 857 din 31 octombrie 2013, odată cu care KBS a devenit o realitate și pe plan național în RM. În 2022, Guvernul RM prin Hotărârea sa nr. 653 din 22.09.2022 a aprobat *Strategia națională de dezvoltare „Moldova Europeană 2030”,* în care adaptează prioritățile, obiectivele, indicatorii și țintele angajamentelor internaționale asumate de către Republica Moldova la contextul național.

În KBS noua economie se constituie din economia digitală, economia Internet, noi produse și servicii digitale, noi genuri de e-afaceri, noi moduri de a învăța, de a se distra, de a lucra etc. Pe de altă parte, evoluția rapidă a TIC, a e-afacerilor, e-educației, e-guvernării, e-distracțiilor, Smart

home, IoT, IoB etc. duce la **creșterea concomitentă a riscurilor informaționale și a modului în care instituțiile statului, organizațiile private, persoanele individuale și societatea în întregime ar trebui să răspundă provocărilor și oportunităților create de revoluția tehnologică**. Or, în KBS, dependența de TIC este în creștere continuă, iar informațiile distribuite pe Internet și Web sunt din ce în ce mai frecvent supuse riscurilor.

Câteva cifre convingătoare privind atacurile cibernetice Conform Cybercrime Magazine:

- În fiecare zi au loc peste 4.000 de atacuri de tip ransomware. Se estimează că un atac ransomware va lovi o întreprindere sau un consumator la fiecare 2 secunde până în 2031 [25];
- Costul pagubelor provocate de ransomware se așteaptă să crească de cca 13 ori, de la 20 miliarde USD în 2021 la 265 miliarde USD până în 2031;
- 91% dintre atacurile cibernetice încep cu un e-mail de spear-phishing, utilizat în mod obișnuit pentru a infecta organizațiile cu ransomware [25].

Valoarea pierderilor din atacurile cibernetice din ultimii 13 ani în S.U.A. a crescut de la 32 mii USD în 2010 la 6,9 milioane USD în 2022, de cca 215 ori mai mari în 2022 decât în 2010 *(Fig. 1.13, [26]).*

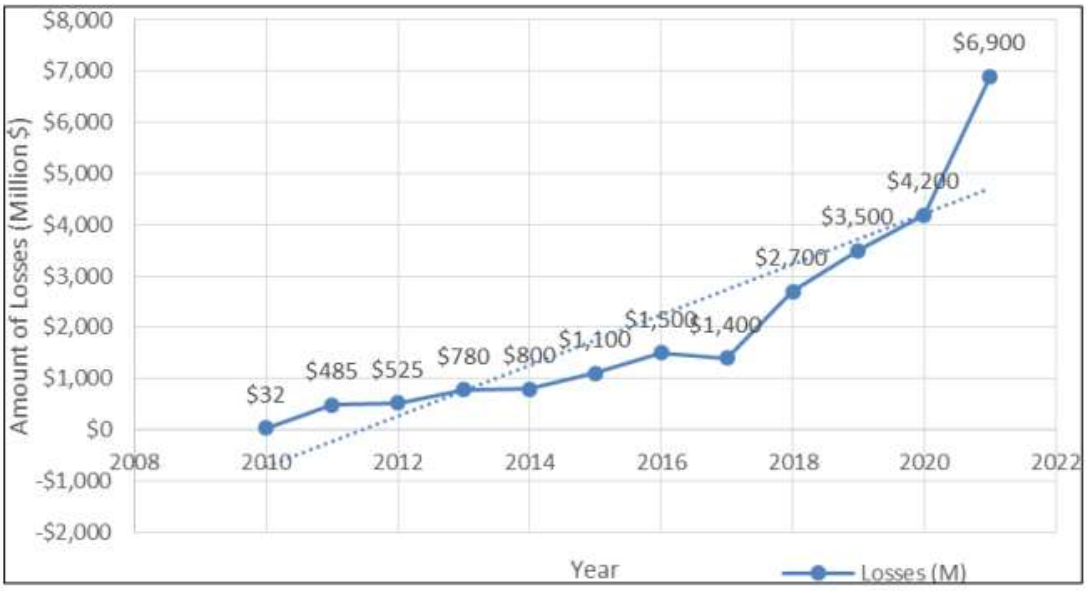


Figura 1.13. Valoarea pierderilor din atacurile cibernetice în anii 2010-2021, S.U.A.

Cea mai bruscă creștere se observă în perioada pandemiei COVID 19.

Conform altor statistici și estimări, realizate de *Statista Technology Market Outlook*, costurile crimelor cibernetice în perioada de cinci ani de la 2018 pană la 2022 au crescut de peste 13 ori, de la 0,86 la 8, 44 trilioane USD. Iar estimarea creșterii pentru următorii 5 ani, din 2022

până în 2027 este de peste trei ori, de la 8,44 la 23,82 trilioane USD *(Fig. 1.14, adaptată de autor în baza [1]).*

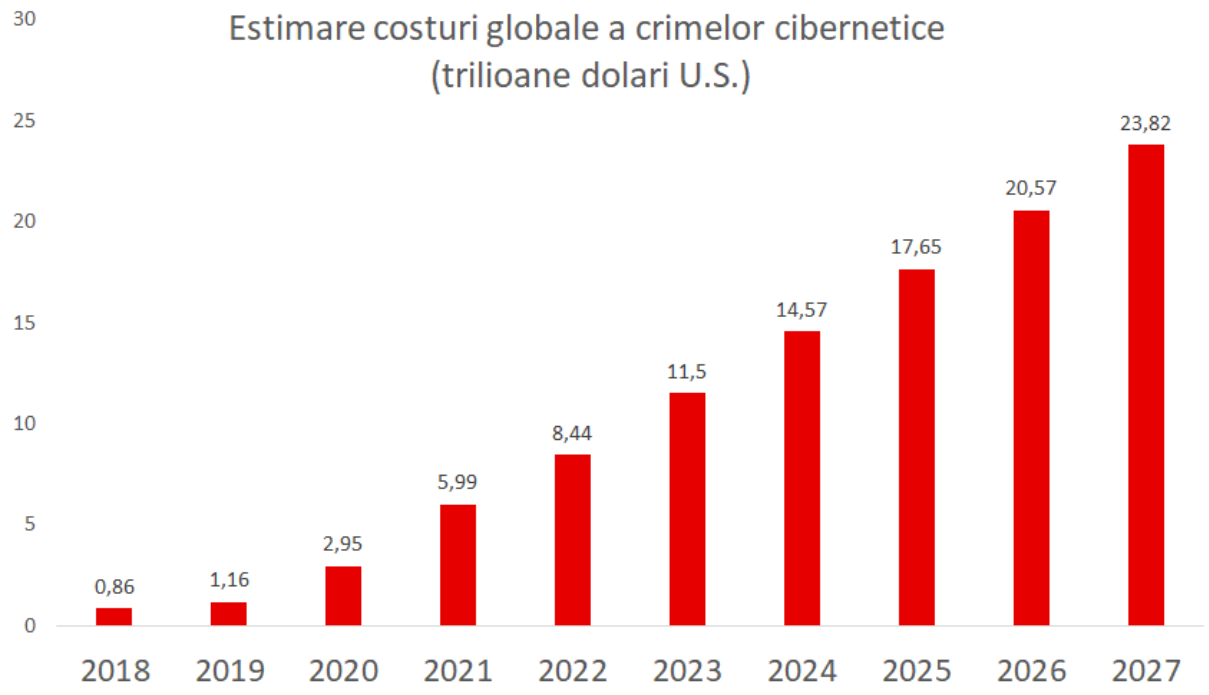


Figura 1.14. Creșterea costurilor crimelor cibernetice

Alte câteva constatări notabile:

- Unul din 50 de site-uri este rău intenționat;
- Aproximativ 25% dintre acestea sunt găzduite pe domenii de încredere și utilizează protocolul securizat HTTPS;
- Peste 90% din programe malware sunt livrate prin e-mail;
- 74% din toate încălcările includ factorul uman, fie prin eroare, utilizare greșită a privilegiilor, utilizarea credențialelor furate sau inginerie socială;
- 83% dintre încălcări au implicat factori interni;
- 19% dintre încălcări au implicat factori externi:
- Cele mai atacate active sunt serverele, peste 80%;
- 95% de încălcări au fost motivate financiar;
- 24% din încălcări constituie Ransomware etc. Pentru alte detalii a se vedea [27].

Astfel, gestionarea adecvată a securității informației și a siguranței tranzacțiilor electronice are o importanță crucială și devine un element esențial al bunelor practici informaționale în contextul KBS. În Republica Moldova importanța securității informației este subliniată inclusiv în *„Strategia securității informației a RM 2019-2024”* și în *Planul de acțiuni pentru implementarea*

Strategiei, adoptate prin Hotărârea Parlamentului nr.257 din 22.11.2018 (https://www.legis.md/cautare/ getResults?doc_id=111979&lang=rol).

Amenințările și riscurile, atacurile și incidentele de SecInf se materializează prin exploatarea vulnerabilităților care pot proveni în cea mai mare parte din trei surse principale:

- **Omul**, prin acțiuni sale voite sau nu, e.g. pierderea sau furtul sau distrugerea unui laptop cu informații sensibile, atacuri efectuate de hackeri asupra unui site, sistem etc.
- **Infrastructura critică**, tehnologiile și sistemele de suport ale afacerilor (*rețele informatice și comunicaționale, mașinăria, serverele, dispozitivele, inclusiv periferice, IoT, IoB, inclusiv software-ul incorporat în toate acestea)* incapabile de a menține respectivele funcții din cauza penelor, exploatării vulnerabilităților etc.
- **Natura**, e.g. calamități naturale, incendii, inundații etc.

Securitatea informației a devenit un **subiect fierbinte**, care persistă pe agenda tuturor forurilor de specialitate, constituie obiectul mai multor programe de studiu, proiecte de cercetare și strategii de dezvoltare. Aceasta deoarece, pe de o parte, ***informația este estimată la nivelul celui de-al patrulea element vital, după aer, apă și foc*** iar, pe de altă parte, era informațională a adus *schimbări profunde în evoluția riscurilor informaționale* și a modului în care instituțiile statului, organizațiile private, persoanele individuale și societatea în întregime ar trebui să răspundă provocărilor și oportunităților create de revoluția tehnologică.

Simultan cu creșterea informatizării și disponibilității dispozitivelor electronice, **cresc și amenințările la adresa securității informației**, crește dependența de infrastructura TIC. Riscurile au crescut simțitor odată cu apariția dispozitivelor portabile/mobile, a accesului fără fir la Internet, a dezvoltării TIC, a extinderii ariei afacerilor electronice operaționale, a hiper-conectivității globale, a serviciilor de Cloud computing *(SaaS – Software as service, IaaS – Infrastructure as service, PaaS – Platform as service),* a numărului de IoT, IoB, case inteligente – toate conectate la Internet. Ușurința în utilizarea TIC, a dispozitivelor mobile, Internet și Web, costul lor scăzut, rapiditatea și anonimitatea fac din acestea un mediu favorit pentru diverse infracțiuni, care ar trebui tratate în mod eficace și în timp util.

Conform statisticilor, criminalitatea informatică rămâne a fi o amenințare perpetuă pentru interesele naționale și economice ale țărilor și corporațiilor. Iar securitatea informației a devenit esențială, atât pentru persoane fizice și juridice, cât și pentru societate și stat în întregime, ca componentă semnificativă a securității naționale și regionale.

1.3.2. Amenințării specifice pentru securitatea cibernetică a unei bănci

După cum a fost deja menționat, în spațiul cibernetic în continuă evoluție, când majoritatea entităților sunt prezente pe Internet, SecInf/SC a devenit o preocupare majoră pentru a proteja datele, informațiile, resursele informaționale, infrastructura SI/TI. Conform raportului Verizon din 2023 [27], cele **trei moduri principale prin care atacatorii accesează o organizație** sunt **credențialele furate, phishing-ul** și **exploatarea vulnerabilităților**. O listă a amenințărilor și vectorilor de amenințări tipice oricărei afaceri, organizații, exemple de vulnerabilități și amenințări asupra SecInf a se vedea *Anexa D.1 a standardului ISO/IEC 27005:2022* [28]. Câteva dintre diversele probleme privind organizarea și gestionarea eficientă a securității informației la nivelul entităților bancare a se vedea *(Tab. 1.2)*.

Tabelul 1.2. O listă incompletă de cine/de ce ar trebui să protejăm informația

Tip de amenințare	Exemplu
Erori umane involuntare	Adresa greșită de e-mail, pierdere laptop, telefon cu informații importante, cultură informațională scăzută.
Acțiuni umane voite, premeditate	Acces neautorizat, furt de date, extorcare, șantaj, sabotaj, vandalism și alte activități criminale sau teroriste.
Frauda	Furtul de identitate, fraudarea cheltuielilor.
Atac asupra SO/ rețelei/Aplicației	Viruși, viermi, troieni, hackeri, DoS *(Denial of Service)*, DDoS *(Distributed DoS)*, MiTM *(Man in the Middle*), phishng etc.
Dezastre naturale	Incendii, inundații, cutremure, fulgere, erupție vulcanică.
Defecțiuni hard	Erori de alimentare cu energie electrică, erori de funcționare.
Probleme software	Bug-uri sau defecte (imprevizibile) de proiectare, coruperea datelor.
Rootkits	Programe concepute să controleze un calculator fără a fi vizibile.
Atacuri de tip phishing	Tentative de obținere a unor date despre conturi bancare sau alte date cu caracter personal prin intermediul e-mail, pagini web false.
Ransomware	Viruși care criptează fișiere ce conțin date importante, pentru a căror decriptare se pretind apoi diverse sume de bani.

Ransomware este una dintre cele mai mari amenințări cibernetice de azi, deja menționat anterior, de exemplu a se vedea [25]. Atacatorii criptează datele victimelor și estorchează bani pentru a le debloca prin livrarea cheii de decriptare. Cele mai frecvente pricini ale acestui tip de amenințare este păstrarea datelor importante necriptate și/sau accesul nesancționat la cheile de criptare inclusiv în rezultatul phishing-ului.

Atacurile de blocare a serviciilor DoS/DDoS nu afectează informația, dar supraîncarcă serverul prin generarea unui mare exces de solicitări false, blocând accesul utilizatorilor reali la servicii mediate de servere și/sau site-uri web.

Programele malware. Dispozitivele finale ale utilizatorilor, precum computerele și telefoanele mobile, care au fost compromise de malware, de fiecare dată când se vor conecta la rețeaua BC reprezintă un risc major pentru SecInf a băncii. Datele sensibile trec prin această conexiune și dacă dispozitivul final are instalat malware pe el, fără o securitate adecvată acest malware ar putea ataca rețelele băncii prin intermediul dispozitivelor compromise.

O altă pricină a compromiterii SecInf sunt **serviciile terțiare slab securizate.** Multe bănci angajează servicii de la terțe persoane fizice sau juridice în efortul său de a-și servi mai bine clienții. De exemplu, provideri de Internet, centre de procesare etc. Dacă acești furnizori terți nu au măsuri bune de securitate cibernetică în vigoare, banca ar putea suferi pierderi. BC ar trebuie să analizeze cum se vor putea proteja de amenințările de securitate induse de terți înainte de a implementa soluțiile lor.

Printre alte probleme ale SecInf unei entități sunt de menționat [2]:

- Vehicularea mai multor termeni apropiați, atât la nivel internațional cât și la nivel național cum ar fi: securitatea informațională, securitatea informației, securitatea cibernetică, securitatea informatică, securitatea TI, SI etc.;
- Se atestă o multitudine de standarde/cadre diferite de abordare și reglementare a protecției datelor cu caracter personal, securității informației, securității cibernetice, tehnologiei informației și sistemelor informaționale în spațiul cibernetic, virtual, peste *„300 de standarde cu o multitudine de măsuri, proceduri, bune practici (în total peste 3500!) care sunt astăzi în vigoare, sunt sistematic revizuite, îmbunătățite și reeditate”*
- Marea diversitate a termenilor apropiați, a cadrelor de reglementare și a controalelor de SecInf, aplicate la diferite niveluri, pentru diferite industrii etc. complică și îngreunează selectarea celor potrivite cazului, impun cerințe înalte de calificare și duc la un consum mare de timp și de resurse necesare pentru asigurarea SecInf. Totodată, majoritatea controalelor sunt prea abstracte pentru utilizarea lor directă în cadrul unor entități concrete, cu cerințe specifice de SecInf, e.g. medicină, industria bancară, servicii guvernamentale etc., se repetă în diferite cadre în diferite arii, sub diferite nume etc.;
- Adesea SecInf nu este prea bine înțeleasă de industrie, de furnizori, de top-management, de utilizatori – ceea ce impune cercetarea, conștientizarea, promovarea culturii securității informației la toate nivelurile;

- Adesea SecInf nu este aliniată la ultimele versiuni ale standardelor de bune practici, necesare pentru asigurarea conformității activităților bancare cu cadrul de reglementare global, național și local, ceea ce impune actualizarea-transformarea continuă a SMSI;
- SecInf nu răspunde prea bine amenințărilor perpetue și în creștere permanentă *(numărul celor necunoscute este de cca 2 ori mai mare decât a celor cunoscute)*, nu se potrivește prea bine cu creșterea continuă a complexității mediilor TIC și de e-afaceri – trebuie revigorată și orientată spre soluții simple, transparente, inteligente și eficiente;
- Doar certificarea periodică a conformității SMSI cu standardele de securitate nu mai este suficientă pentru medii cu amenințări perpetue și în continuă creștere. Pentru a face față apariției noilor riscuri și a ajuta organizația să-și gestioneze riscurile la niveluri acceptabile SecInf ar trebui să evolueze continuu.

Un set minim de resurse informaționale ce trebuie protejate pentru a diminua nivelul de fraudă se referă în special la mediile TI, SI, Internet și web;

- **Personal** (angajați, clienți, furnizori);
- **Active tangibile** (documente, date, cunoștințe, expertize, BD, înregistrări);
- **Active fizice** TI, SI (echipamente, computere, routere, discuri etc.);
- **Software** (de sistem, aplicativ, web, personal, comercial, SGBD etc.);
- **Servicii** TI, SI (interne, externe, ISP etc.);
- **Locații/sedii fizice și virtuale**, platforme, site-uri web etc.

Statisticile consultate indică creșterea continuă a crimelor cibernetice, care constituie principala problemă a securității informației.

Conform statisticilor din luna mai anul 2020, *Figura 1.15,* primele cinci cele mai răspândite tehnici de atac acoperă 88% din toate atacurile:

- Programe malware 34,8%,
- Vulnerabilități necunoscute 20,1%,
- Spargerea contului 16,3%,
- Atacuri vizate 10,9%,
- DDoS 5,4%.

Iar primele cinci ținte preferate ale atacurilor acumulează cca 61% din toate fraudele:

- Industrii multiple 22,3%,
- Activități tehnice științifice profesionale 10,9%,
- Financiar și asigurări 10,9%,
- Informații și comunicare 10,3%,

- Vânzări, inclusiv cu amănuntul 6,5%.

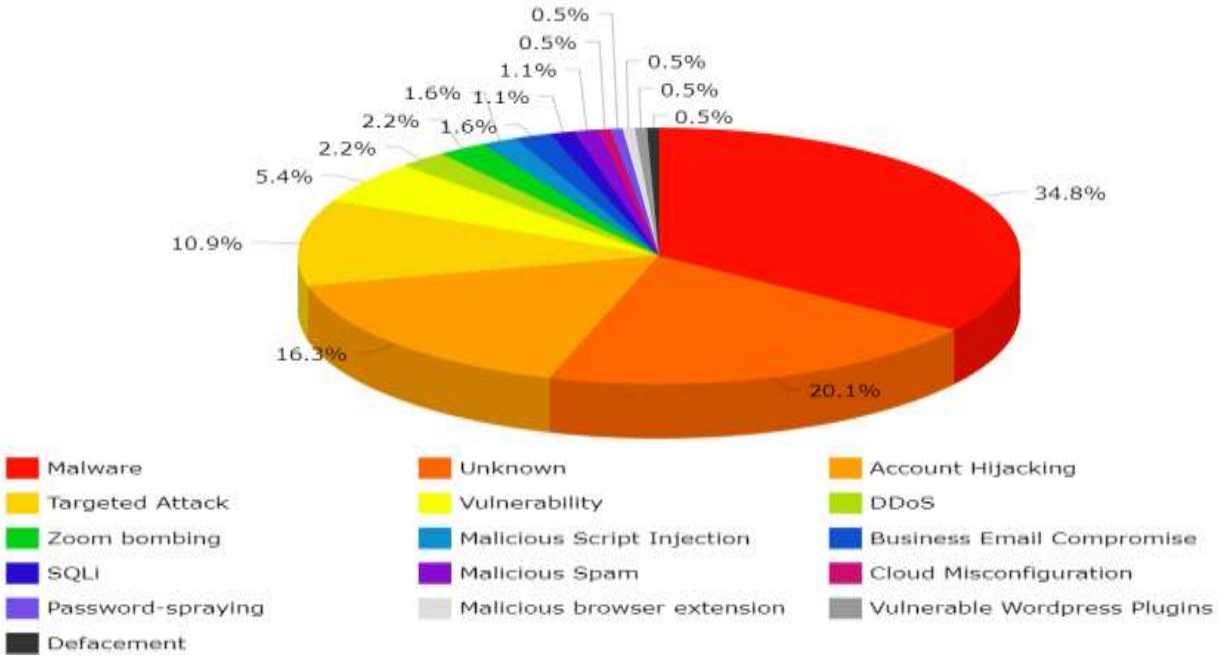


Figura 1.15. Tehnici de atac a securității informației [79]

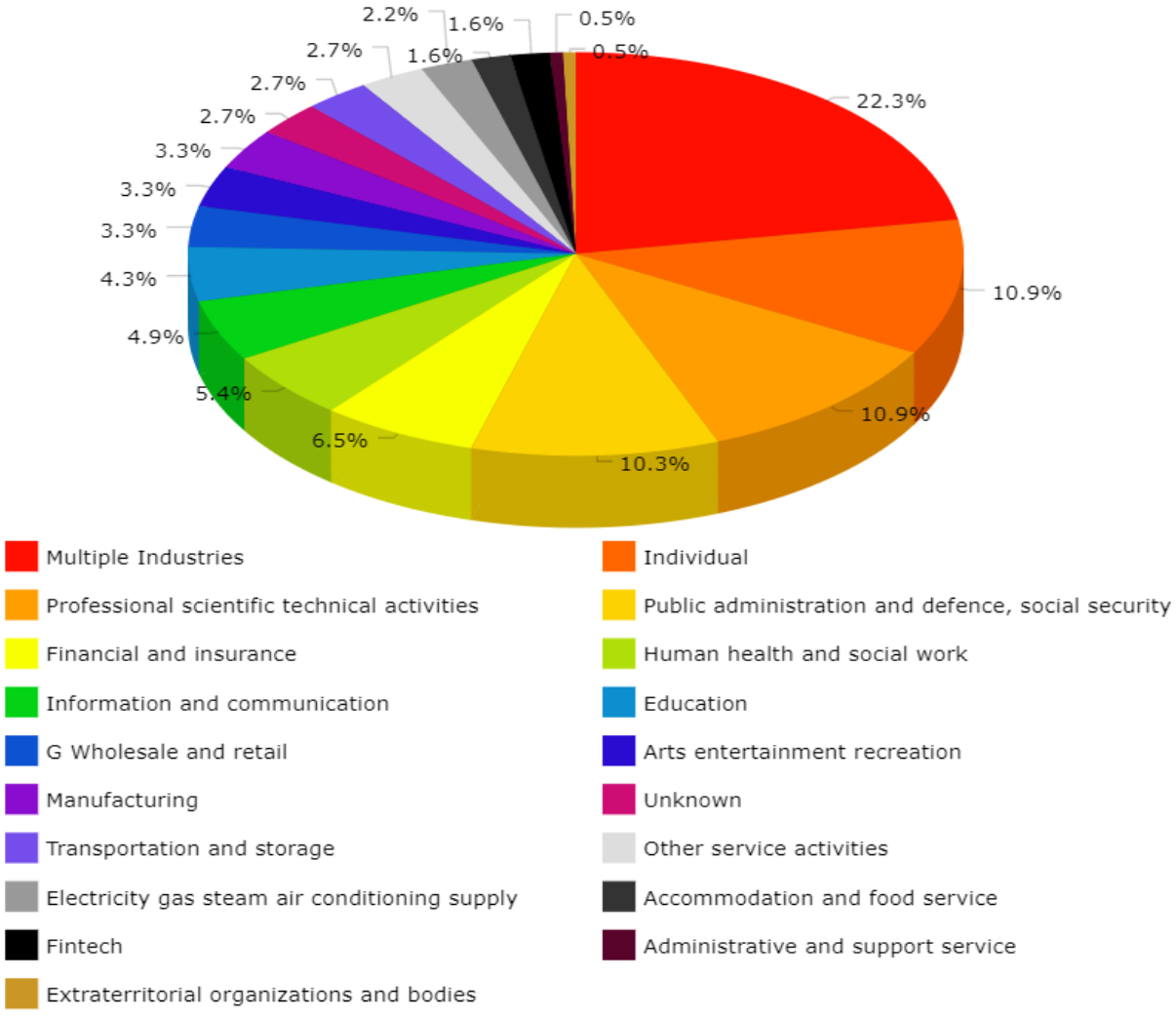


Figura 1.16. Țintele de atac [79]

1.4. Metode, instrumente și tehnici asistate de calculator pentru asigurarea SecInf

Lupta cu complexitatea SecInf în entități este susținută de sisteme și instrumente software profesionale destinate, care cu timpul au devenit mult mai numeroase și mai accesibile din punct de vedere financiar. În continuare, și doar ca exemplificare, sunt enumerate și/sau succint prezentate câteva dintre asemenea instrumente.

1.4.1. Programe instrumentale de securitate a informațiilor

Există versiuni gratuite a instrumentelor de SecInf, pornind de la aplicații antivirus *(e.g. Top 10 cele mai bune teste antivirus gratuite [80]) și terminând cu instrumente de pre-audit a SecInf (e.g. Top CIS/SANS controls [30], CSAT [31], CMMC [32], Evaluare gratuită a securității cibernetice [83], Cadrul de securitate cibernetică NIST [84]).* Utilizarea acestor instrumente profesionale specializate ajută entitățile la eliminarea scurgerilor de informații, realizarea de pre-audit al SecInf *(depistarea punctelor vulnerabile, planificarea și realizarea îmbunătățirilor continue etc.)* și permit a face față sarcinii din ce în ce mai complexe de asigurare a securității informațiilor. Asemenea programe instrumentale încep să fie implementate și în companiile cu un număr relativ mic de angajați.

Programele instrumentale de securitate a informațiilor prezintă soluții moderne și cuprinzătoare, cu diverse funcții, precum detectarea amenințărilor și a atacurilor de viruși, identificarea incidentelor și reacția la accesul neautorizat etc. Aceste instrumente permit obținerea informațiilor necesare despre funcționarea sistemului din diverse jurnale în care sunt înregistrate informații importante; colectează date despre utilizatori, rețeaua locală, dispozitivele conectate și alte obiecte; monitorizează potențialele amenințări și previn răspândirea acestora; oferă diagnosticare cuprinzătoare prin diverse analize avansate. Clienții pot folosi aceste instrumente fie ca software, fie ca dispozitive virtuale într-un mediu local sau în Cloud Computing.

Ca exemple pot servi **IBM QRadar SIEM, SolarWinds, Sumo Logic, ManageEngine, AlienVault, LogRhythm, Rapid7 InsightlDR, Splunk** și altele.

Certificarea modelului de maturitate a securității cibernetice/**CMMC** este un standard unitar pentru a îmbunătăți lanțul de aprovizionare pentru departamentul de apărare (DoD) al S:U.A. Toți contractorii DoD ar trebui să dețină un certificat CMMC de nivelul 1 – *cu 17 practici de SC* sau 2 – c*u 100 practici de SC (ambele niveluri 1-2 conform NIST SP 800-171)* sau 3 cu *un subset de controale suplimentare NIST SP 800-172*. CMMC [32, 37, 42] este conceput să ofere o asigurare sporită că o companie poate proteja în mod adecvat informațiile sensibile neclasificate, luând în considerare fluxul de informații către subcontractanții dintr-un lanț de aprovizionare.

Un instrument util în alegerea produselor software poate **fi Pătratul magic interactiv de la Gartner** [85]. Acest instrument poziționează jucătorii pe piața instrumentelor pe Magic Quadrant Gartner, oferă o vedere de ansamblu pe piața. Instrumentul diferențiază furnizorii în cele patru cadrane în funcție de segmentul de piață ocupat, maturitatea produsului etc. Caracteristicile interactive ale Magic Quadrant Gartner permit generarea unor **vederi personalizate** prin ajustarea ponderilor aplicate fiecărui criteriu de evaluare specifice utilizatorului, salvarea și partajarea acestei vederi pentru analize interne și luarea deciziilor.

Pătratul magic interactiv de la Gartner reunește, de asemenea, opinia experților și recenziile P2P într-o singură experiență; ajută utilizatori în orientarea rapidă asupra furnizorilor de soluții, reflectarea propriilor obiective, nevoi și priorități de afaceri, justificarea alegerii potrivite etc. Un exemplu de pătrat magic privind instrumentele/sistemele de Securitate a Informației și Management al Evenimentelor/SIEM a se vedea în *Figura 1.17.*

Figura 1.17. Pătratul Magic Gartner cu Top 6 platforme SIEM [82]

Un sistem de management al informațiilor și evenimentelor de securitate reprezintă o bază, o platformă a Centrului corporativ modern de operațiuni de SecInf. SIEM colectează jurnalele și evenimentele din instrumentele de securitate și sistemele TI, SI din întreaga întreprindere, analizează datele și utilizează informații despre amenințări, reguli și analize pentru

a identifica incidentele de securitate. Iar **Splunk** este un instrument eficient de tip SIEM, destinat pentru protejarea entității de accesul neautorizat, detectarea rapidă a amenințărilor, evaluarea riscurilor reale, colectarea de informații etc.

1.4.2. Metode, instrumente și tehnici de audit asistat de computer

Auditul ca parte indispensabilă a SMSI, este responsabil de reacția inversă a controalelor și masurilor de SecInf. Ghiduri și instrumente de audit al SMSI, cum se efectuează un audit de securitate cibernetică a se vedea [83], [84], [86], [87].

Generic esența auditului poate fi exprimată prin citatul „*In God we trust. Everyone else we audit!",* B. Baczko, 2007. Crede, dar verifică, aceasta este esența. Ca și oricare alt domeniu al unui SM, auditul recurge la metode computerizate pentru a reduce din complexitatea și rutina mare. Se referă la tehnici de audit asistat de computer, software specializat de analiză a riscurilor de SecInf, Instrumente de interogare a BD, Statistici și analize de date etc.

Anume pentru a reduce din complexitate auditul SecInf trebuie să utilizeze diverse **metode, instrumente și tehnici de audit automatizate**, asistate de calculator, bazate pe tehnologii informaționale, numite tehnici de audit asistate de calculator CAAT sau CAATs, de la *Computer-Assisted Audit Techniques*. Standardele actuale de audit încurajează auditorii să adopte CAATs pentru a îmbunătăți eficiența și eficacitatea auditului.

CAATs sunt aplicate în procesul exercitării diverselor proceduri de audit prin identificarea domeniilor prioritare pentru efectuarea testării substanțiale/detaliate a controalelor TI, SI și utilizarea diferitelor CAATs în scop de **anchetare, extragere și analize de date** necesare pentru justificarea concluziilor de audit. CAATs pot fi utilizate și pentru **analiza jurnalelor utilizatorului, raportarea excepțiilor, filtrarea de date, compararea fișierelor, prelevarea de probe, analiza decalajului datelor, „îmbătrânirea" datelor, calcule virtuale** etc.

Principalele avantaje ale utilizării CAATs includ analiza volumelor mari de date, repetabilitatea testelor pe diferite seturi de date și criterii diferite cu documentarea automată a testelor de audit și a rezultatelor cu marcajele de timp. Auditorii se pot asigura că dovezile electronice colectate și documentate sunt suficiente, fiabile și precise pentru a susține observațiile de audit. Astfel de dovezi electronice pot consta din fișiere de date, jurnalele utilizatorilor, modele analitice, rapoartele TI, SI colectate și stocate corespunzător.

Printre avantajele și funcțiile acoperite de CAATs sunt de menționat:

- Înlocuiesc multe din procedurile manuale, prin care se atinge economisirea de timp și costuri de audit fără a pierde calitatea sau precizia;
- Simplifică analiza datelor și generarea rapoartelor specifice, cu efort minim de ajustare;

- Contribuie la reducerea numărului de teste de audit;
- Permit interogări complexe ale bazelor de date, totalizări, stratificări, extrageri, eșantionări pentru audit;
- Mențin integritatea probelor de audit, permit verificarea integrității fișierelor;
- Oferă posibilitatea verificării integrității sistemului.

Pentru scopul tezei este important **software-ul specializat de audit**, care reprezintă programe utilizate de auditor ca parte a proceselor și/sau a procedurilor de audit și testare a controalelor de securitate a informației la nivel tehnic și/sau de operare TI, SI precum:

- Teste de penetrare;
- Securitatea web aplicațiilor (OWASP);
- Securitatea sistemelor de operare, sistemelor de gestiune a bazelor de date;
- Evaluarea vulnerabilităților, e.g. conform CVE *(Common Vulnerabilities and Exposures, https://cve.mitre.org/).*

Exemple de asemenea utilități și instrumente specifice de audit pentru analiza și monitorizarea securității TI, SI sunt:

- Instrumente de scanare/scanere de securitate pentru rețea: *Nessus, Netcat, OpenVAS, XSpider, Lumension Security Vulnerability Scanner, Retina Network Security Scanner, metasploit, nexpose, backtrack, MBSA, Kali-Linux, Burp Suite, OWASP dirbuster, ProxyStrike;*
- Spărgătoare de parole de rețea: *Brutus, Hydra, LC5;*
- Utilități standard de rețea: *host, showmount, traceout, finger, ping;*
- Instrumente de inventariere și scanare a resurselor de rețea: *LanScope, nmap;*
- Sniffere de rețea și analizoare de protocol: *tcpdump, wireshark;*
- Sisteme de prevenire a intruziunilor IPS sau de detectare a intruziunilor IDS, care pot genera alarme dacă sunt detectate acțiuni neautorizate. De exemplu, Snort (jargon, engl.), un sistem open source pentru detectarea și/sau prevenirea intruziunilor, care poate efectua înregistrarea de pachete și analiza traficul în rețelele IP în timp real pentru a găsi semne ale unor tipuri cunoscute de atacuri de rețea;
- Data Loss/Leak Prevention (DLP), prevenirea pierderilor/scurgerii de date, tehnologie software și/sau hardware, de prevenire a scurgerii informațiilor confidențiale dintr-un sistem informatic spre exterior. DLP se bazează pe analiza fluxurilor de date care traversează perimetrul sistemului protejat;

- SIEM ca sistem/proces ce colectează log-urile, analizează și prezintă informații de la dispozitivele de rețea și dispozitivele de securitate. Include și aplicații de gestionare a identității, accesului, instrumente de gestionare a vulnerabilităților și baze de date și aplicații;
- Instrumente/metode computerizate de analiză și evaluare a riscurilor: CRAMM (CCTA Risk Analysis and Management Method, o metodologie destinată utilizării în gestionarea riscurilor *în Anglia, United Kingdom, Insight Consulting, http://www.cramm.com, unde CCTA = Central Computer and Telecommunications Agency)*, RiskWatch *(S.U.A., RiskWatch);* Risicare/Mehari *(France, BUC S.A./Clusif);* Digital Security, MSAT *(Microsoft Security Assessment Tool)*, Condor, OCTAVE *(Operationally Critical Threat, Asset, and Vulnerability Evaluation, o metodologie pentru comportamentul de evaluare a riscurilor într-o organizație, dezvoltată de Institutul de Inginerie Software (SEI) de la Universitatea Carnegie Mellon, http://www.cert.org/octave);*
- Colectarea de informații/dovezi: *Maltego, Ncat, Nmap/Zenmap*. De exemplu, Maltego este utilizat în investigații online pentru automatizarea procesului de căutare a conexiunilor între informațiile care sunt postate pe diverse surse de pe Internet;
- Utilități de căutare și analiză a vulnerabilităților: *OpenVAS, Nessus, MSBA.* De exemplu, scannerul de vulnerabilități în rețea Nessus conține o bază de date actualizată cu vulnerabilități cunoscute;
- Exploatarea/verificarea vulnerabilităților: *Metasploit/Armitage, SET, Hydra, Johnny;*
- Auditul aplicațiilor WEB: *w3af, OWASP ZAP*. De exemplu, OWASP ZAP este un instrument ușor de utilizat pentru găsirea vulnerabilităților în aplicațiile web și testarea penetrării web aplicațiilor;
- Investigarea incidentelor*: NetworkMiner, Wireshark, Splunk;*
- Raportare: *CaseFile, Dradis.*

Chiar dacă multe dintre metodele enumerate *(e.g. CRAMM, RsikWatch, OCTAVE)* au la bază ISO 17799, astăzi scos din uz, unele dintre ele sunt încă destul de utilizate. Multe din softurile CAATs, îndeosebi comenzi de sistem și/sau utilități de diagnosticare în rețele TCP/IP *(e.g. Arp, Hostname, Ipconfig, Netstat, Netsh, Ping, Route, Tracert),* analizoare de protocol etc. sunt publice, deschise. Altele sunt produse de proprietar, includ costuri de procurare, licențe și drepturi speciale de utilizare.

De exemplu, testul de penetrare PENTEST permite verificarea cât de mult este protejată compania împotriva atacurilor hackerilor. În fapt simulează acțiunile hackerilor reali, identifică vulnerabilități pe site-ul web, pe infrastructura corporativă, „atacă" codul sursă, aplicațiile mobile și orice alte sisteme informatice. În rezultatul analizei pot fi elaborate planuri specifice și recomandări detaliate pentru reducerea riscurilor și remedierea vulnerabilităților.

Pentest-ul poate avea diferite obiective, principalele fiind:

- **Analiza securității:** încercarea de a identifica cât mai multe vulnerabilități, cu oprirea testului atunci când este detectată o vulnerabilitate critică și/sau a expirat perioada.
- **Test de penetrare:** o încercare de a „intra în interior" și de a obține informații confidențiale, de a extrage fonduri sau de a atinge un alt obiectiv stabilit.
- **Încercări îndelungate de a intra ascuns în sistem**, cu minimum de restricții. Aceasta poate include phishing, încercări de infiltrare fizică la birou și, de asemenea, include monitorizarea și rezistența angajaților clientului.

Scanarea rețelei este implementată în două etape de bază:

- Colectarea de informații inițiale despre *gazdă/gazde, porturi deschise, utilizatori înregistrați pe gazdă, tipul de servicii de rețea care rulează pe gazdă* etc.
- Căutarea de vulnerabilități în acele servicii de rețea și informații care au fost colectate în prima etapă.

Exemple de **scanere de rețea:** *Advanced IP Scanner, SoftPerfect Network Scanner Portable, Acunetix, METASCAN*. Exemple de **instrumente de analiză a setărilor de securitate a gazdelor**: *Security Benchmarks, CIS Scoring Tools, CIS Router Audit Toolkit, Windows Security Templates, Security Analysis Tool.* Îndrumări detaliate privind utilizarea CAATs concrete și detalii pot fi obținute în manualele de utilizare ale instrumentelor/versiunilor respective.

1.4.2.1. Instrumentul de autoevaluare a riscurilor de securitate MSAT

MSAT *(Microsoft Security Assessment Tool)*, versiunea din 2009, este o aplicație desktop pentru **identificarea și abordarea riscurilor de securitate a informației** în mediul TI, SI în baza profilurilor de risc prin răspunsul la circa 200 de întrebări. Întrebările și recomandările instrumentului se bazează pe standardele existente la acel moment *(e.g. ISO 17799 și NIST-800.x, recomandări și îndrumări de la Microsoft Trustworthy Computing Group).* Instrumentul adoptă o abordare holistică pentru evaluarea securității prin analiza impactului factorului uman, al proceselor și al tehnologiei. Din 15 iunie 2022 MSAT nu mai este întreținut de Microsoft. Dar rapoartele explicite ale MSAT rămân a fi încă utile pentru cei care au instrumentul.

După ce răspunde la întrebări, utilizatorul poate vizualiza un raport detaliat generat din rezultatele sondajului și poate compara rezultatele cu alte sondaje efectuate, inclusiv media pe industrie. Raportul furnizat utilizatorului conține recomandări de reducere a amenințărilor și îndrumări detaliate privind îmbunătățirea SecInf a entității evaluate. MSAT *(de altfel ca și oricare alt instrument)* nu poate înlocui un auditor/un consultant profesionist de securitate. Acest raport are doar scop informativ în cadrul unui pre-audit. Un fragment de raport de evaluare realizat cu MSAT a se vedea *Figurile 1.18, 1.19*

Figura 1.18. Fragment al raportului de evaluare

Legendă:

- *Culoarea verde - Îndeplinește cele mai bune practici*
- *Culoarea orange - Are nevoie de îmbunătățire*
- *Culoarea roșie - Discrepanțe grave*

Cel mai bine este ca rating-ul DiDi să fie aproape egal cu rating-ul BRP *(Fig. 1.19)*, unde:

- **BRP** este o măsură a riscului legat de industria și modelul de afaceri al companiei;
- **DiDi** este o măsură a controalelor de securitate cu referire la personal, procese și tehnologie pentru a ajuta la atenuarea riscurilor identificate pentru afacere.

Orice dezechilibru, fie în cadrul unei categorii, fie între categorii, în oricare direcție, poate indica necesitatea realinierii investițiilor în SecInf.

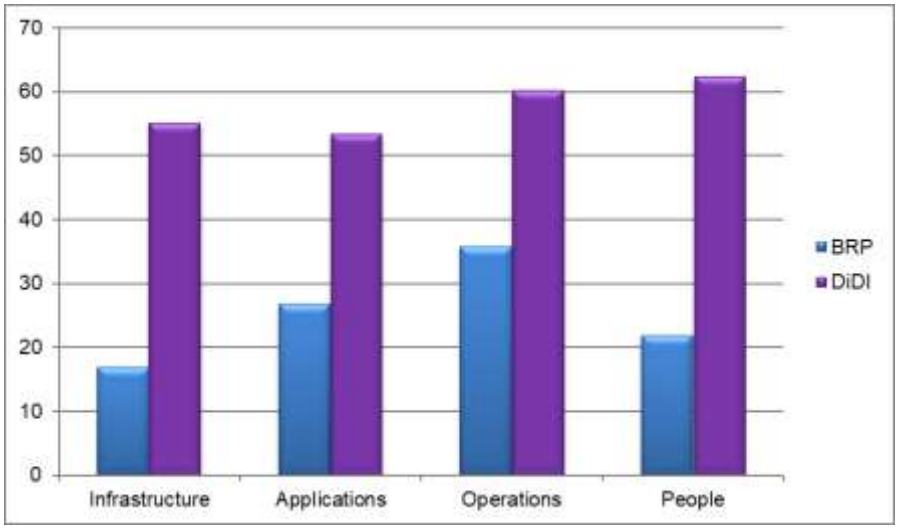


Figura 1.19. Scorul sumar al evaluării realizat cu MSAT

1.4.2.2. Controalele CIS/SANS și Instrumentul de autoevaluare CIS CSAT

Controalele CIS de versiunea 8 [30], dezvoltate de mii de experți în securitatea cibernetică din întreaga lume și mapate la alte multe cadre de securitate, reprezintă un set prescriptiv simplificat de bune practici de securitate cibernetică, care clasifică entitățile utilizatoare în **3 tipuri de implementare a controalelor CIS: *IG1, IG2, IG3***. Fiecare dintre IG1- IG3 conține un subset al controalelor CIS pe care comunitatea le-a determinat ca prioritare și entitatea ar trebuie să le implementeze. CIS definește IG1 ca *„igienă cibernetică de bază*" cu un set de controale recomandat pentru orice entitate, care dorește realizarea protecției împotriva celor mai frecvente atacuri de SC. Controalele IG2 le includ pe cele din IG1, iar cele din IG3 – pe toate din IG1 și IG2.

Instrumentul de autoevaluare a controalelor CIS (CIS CSAT [31]) ajută organizațiile în adoptarea controalelor CIS. Acesta este un instrument puternic, care facilitează implementarea, urmărirea și documentarea progresului de către echipe și gestionarea controalelor de securitate CIS/SANS.

CIS CSAT permite:

- Colaborarea între echipe și atribuirea rolurilor de utilizator;
- Alegerea sub-controalelor specifice;

- Încărcarea documentației ca dovezi justificative;
- Urmărirea evaluărilor în timp;
- Monitorizarea alinierii la alte cadre de securitate;
- Compararea în mod anonim a rezultatelor cu o medie a industriei sau cu alte grupuri de colegi/entități similare.

Există **două versiuni de CIS CSAT**: o versiune gratuită găzduită de CIS și o versiune locală pentru membrii CIS Secure Suite numită **CIS CSAT Pro**. Versiunea **CIS CSAT gratuită** poate fi utilizată în mod necomercial pentru a efectua evaluări ale controalelor CIS pentru orice entitate. Versiunea locală a CIS CSAT Pro este disponibilă exclusiv pentru membrii CIS SecureSuite®. Această versiune oferă caracteristici și beneficii suplimentare:

- Permite economisirea de timp în baza unei metode simplificate de punctare cu un număr redus de întrebări;
- Rezultatele pot fi partajate (la decizia utilizatorului) pentru analize comparative cu scorurile medii ale industriei;
- Are o flexibilitate mai mare pentru urmărirea organizațiilor, filialelor și evaluărilor;
- Permite atribuirea diferitelor roluri utilizatorilor din diferite organizații, filiale, precum și o mai mare separare a rolurilor administrative și non-administrative;
- Permite urmărirea mai multor evaluări simultane în aceeași entitate.

1.5. Concluzii

Dominanta dezvoltării lumii moderne în cadrul KBS este caracterizat de:

- **E-transformarea, schimbarea continuă** a valorilor, structurilor, fenomenelor, proceselor, modului de a lucra, de a învăța, a se distra etc. prin **utilizarea masivă TIC, Internet și Web** în toate domeniile activității umane, dezvoltarea economiei digitale și competitivitatea sporită a e-afacerilor;
- **Creșterea semnificației informației**, estimată la nivelul celui de-al patrulea element vital după apă, aer și foc, informația devenind unul dintre cei mai importanți factori ai progresului social și **Creșterea simultană a amenințărilor în adresa SecInf**;
- **Hiper-conectivitatea** rețelelor corporative, IoT, IoB, și rețelelor Wi-Fi la Internetul global, digitizarea în masă, care duce la sporirea suplimentară a atacurilor informatice.

Toate acestea denotă o dată în plus că SecInf/SC a devenit o problemă critică pentru succesul afacerii. Valoarea informației este, de obicei, legată de consecințele asupra organizației dacă informația este compromisă într-o oarecare formă. Compromiterea informației se referă la **dezvăluirea** sau **utilizarea necorespunzătoare** a ei, **modificarea accidentală** sau **deliberată** a

informației, **indisponibilitatea** informației atunci când este necesar accesul la aceasta. Consecințele unor astfel de compromiteri pot duce la pierderi financiare, daune de renume și de marcă, încălcări ale obligațiilor legale, de reglementare sau contractuale, incapacitatea organizației de a furniza produsele/serviciile preconizate de afacere etc.

BNM supraveghează activitatea băncilor comerciale, inclusiv exercitarea atribuțiilor stabilite de cadrul legal național și internațional privind protecția datelor sensibile în sistemele informaționale, web aplicațiile bancare și SADD, bazate pe TIC moderne. Conform Articolului 139 al Legii cu privire la BNM [16], printre alte măsuri de supraveghere, BNM poate să dispună băncii, dar fără a se limita la acestea, **reducerea riscurilor aferente SecInf/SC.**

Sunt de menționat **probleme, dificultăți majore** în abordarea SecInf, precum:

- *Domeniul SecInf este în continuă schimbare; amenințările cibernetice sunt în permanentă evoluție;*
- *Angajații reprezentă o vulnerabilitate majoră, fiind impusă educația și conștientizarea continuă a personalului;*
- *Entitățile utilizează o varietate de sisteme, rețele și aplicații, gestionarea, actualizarea constantă și securizarea cărora este relativ dificilă;*
- *Lucrul de la distanță, utilizarea dispozitivelor mobile BYOD în cadrul organizației crește riscul de pierdere sau furt de date;*
- *Entitățile trebuie să se asigure că sunt în concordanță cu reglementările privind SecInf, dar demonstrarea conformității este dificilă și costisitoare;*
- *Ca urmare a subaprecierii semnificației SecInf și celor menționate mai sus, adesea bugetele unor entități pentru SecInf sunt restrânse și SecInf este încălcată, compromisă.*

Toate acestea justifică **necesitatea unui cadru adecvat** pentru gestionarea securității informațiilor la nivelul unui model de referință pentru măsurarea proceselor SMSI și SecInf, adaptarea/îmbunătățirea lor continuă la mediul schimbător și alinierea la cerințele legale. În acest scop entitățile pot utiliza modele de maturitate pentru a evalua nivelul de performanță al proceselor și pentru a dezvolta planuri de acțiune pentru asigurarea SecInf/SC în conformitate cu cadrul legal și cu cerințele de bune practici, elucidate în numeroase standarde și cadre de abordare discrete, separate.

Dați-mi un punct de sprijin și
voi muta Pământul din loc
(Arhimede)

2. ASPECTE TEORETICE, METODOLOGICE ȘI PRACTICI DE ABORDARE A SECURITĂȚII INFORMAȚIEI PRIN PRISMA SMSI

În capitolul curent se face o trecere în revistă, o expres analiza a paradigmelor și principiilor de bază, a cadrului normativ și de reglementare privind abordarea SecInf prin prisma unor standarde de bune practici global recunoscute, elucidarea noii paradigme de abordare a SecInf prin prisma SMSI cu scopul de a justifica modul de abordare a SecInf prin prisma modelelor multiprofil de maturitate. Sunt discutate abordarea bazată pe risc, pe standarde și pe modele de maturitate.

2.1. Paradigme, principii și cadre de abordare a SecInf

Principalele paradigme privind realizarea SecInf se referă la *Apărarea în adâncime; Prevenire, detectare și răspuns; Securitatea incorporată prin design; Ciclul Shewhart sau roata (calității) lui Deming (PDCA); Păstrarea unui SMSI simplu; Paradoxul lui Mayfield; Privilegii minime; Obiectiv-valoare-activitate; Oameni, procese și tehnologie* etc., unele mai importante pentru scopul tezei fiind succint examinate în continuare.

2.1.1. Paradigma abordării moderne a SecInf bazată pe SMSI

Abordarea SecInf prin prisma SMSI se înscrie perfect în asigurarea securității informației în adâncime, unde SMSI poate fi considerat acel sistem multistrat, acea cetate cu multiple linii eșalonate de apărare, în centrul căreia sunt plasate cele mai importante valori și cele mai valoroase informații care trebuie apărate. Realizarea SecInf în cadrul unui SMSI permite folosirea diferitelor cadre și metode independente, introducerea mai multor bariere, controale de securitate și bune practici pentru a face față diferitelor tipuri de amenințări, pentru a detecta și intercepta atacurile, a descoperi vulnerabilitățile, amenințările și a preveni exploatarea acestora, a evalua riscurile, urmările și impacturile posibile pentru tratarea prioritizată a riscurilor.

Actualmente SecInf este în proces **de trecere de la paradigma/modelul concentrat pe probleme tehnice-tehnologice**, gestionate la nivel de TI și centrate pe sisteme discrete, **spre un model mai structurat, mai flexibil**, care să ia în considerare obiectivele controalelor de SecInf și riscurile gestionate în acord cu obiectivele afacerii [7]. Numeroasele cadre/standarde de

securitate examinate servesc pentru crearea bazei de date a aplicației M^{3}SI și identificarea domeniilor de interes comun pentru profilurile tipice unor industrii precum și a domeniilor de interes individual, particularizat conform politicilor unei entități concrete.

O primă decizie privind asigurarea SecInf este necesitatea imperativă de regândire a abordării sale conform tendințelor moderne *(Tabelul 2.1).*

Tabelul 2.1. Abordarea modernă a SecInf vis-á-vis de abordarea tradițională [7]

Nr d/o	Abordarea tradițională	Noua abordare impusă în prezent
1.	Problemă tehnică	Problemă organizațională
2.	Gestionată de TI	Gestionată de organizație
3.	Bazată pe cheltuieli	Bazată pe investiții
4.	Realizată ad-hoc și tactic	Realizată managerial și strategic
5.	Centrată pe sisteme	Centrată pe procese (PDCA)
6.	Cu valoare adăugată	Cu valoare incorporată

Schimbarea accentului de pe decizii tehnice-tehnologice *(cca 20%, configurări hardware – software)* **pe decizii organizaționale** *(cca 80%, politici, proceduri, conștientizare, legalitate, evaluare riscuri, Fig. 2.1, sus)* impune nu doar prezența rolurilor respective în cadrul organizației, ci și subordonarea și interacționarea lor corectă *(Fig. 2.1, din partea dreapta de jos).*

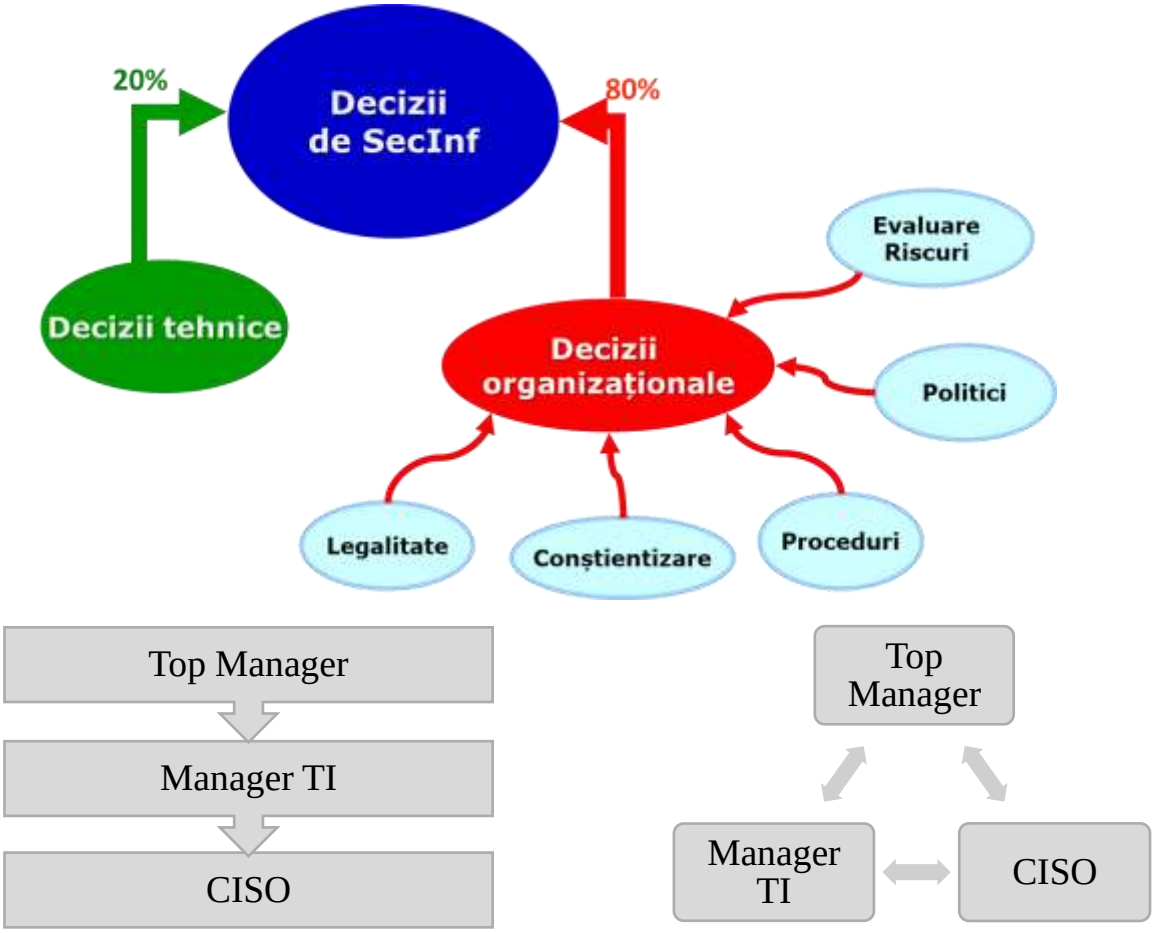


Figura 2.1. De ce trebuie regândită abordarea securității informației (adaptată în baza [7])

Și subordonarea veche este depășită *(Fig. 2.1, din partea stânga, jos).* Dacă înainte SecInf era atribuită departamentului TI, în prezent aceasta se cere a fi **gestionată aparte la nivel de organizație** și **acordată cu obiectivele afacerii**. Vechea structură face vulnerabilă organizația din punct de vedere a SecInf, deoarece comunicarea cu top managerul nu este directă, iar înțelegerea cheltuielilor financiare nu doar că este dificilă, uneori aceasta greșit este considerată ca și inutilă. Prin noua abordare organizațională și prin Declarația politicii de SecInf, SM actuale nu doar că **legiferează includerea top managementului în asigurarea SecInf**, ci și stabilește angajamentele, responsabilitățile financiare și relațiile dintre persoanele interne și externe interesate în SecInf.

O altă problemă a SecInf este marea diversitate a cadrelor, standardelor, cerințelor de reglementare (circa 500!), printre care: 136 de standarde și reglementări tehnice a comitetului ISO/IEC JTC 1/SC 27 privind securitatea informațiilor, securitatea cibernetică și protecția vieții private [33]; circa 80 de standarde operaționale din familia ISO27k privind sistemul de management și audit al securității informației [34], 64 de standarde privind managementul serviciilor TI din seria ISO/IEC 20000, guvernarea TI și a tehnologiilor conexe *(COBIT, ISACA [35])*, seria de circa 200 de publicații speciale NIST SP 800 (S.U.A., [36]), Integrarea modelului de maturitate a capabilității *(CMMI®02, [37], Fig. 2.2)* în sistemele moderne de management etc.

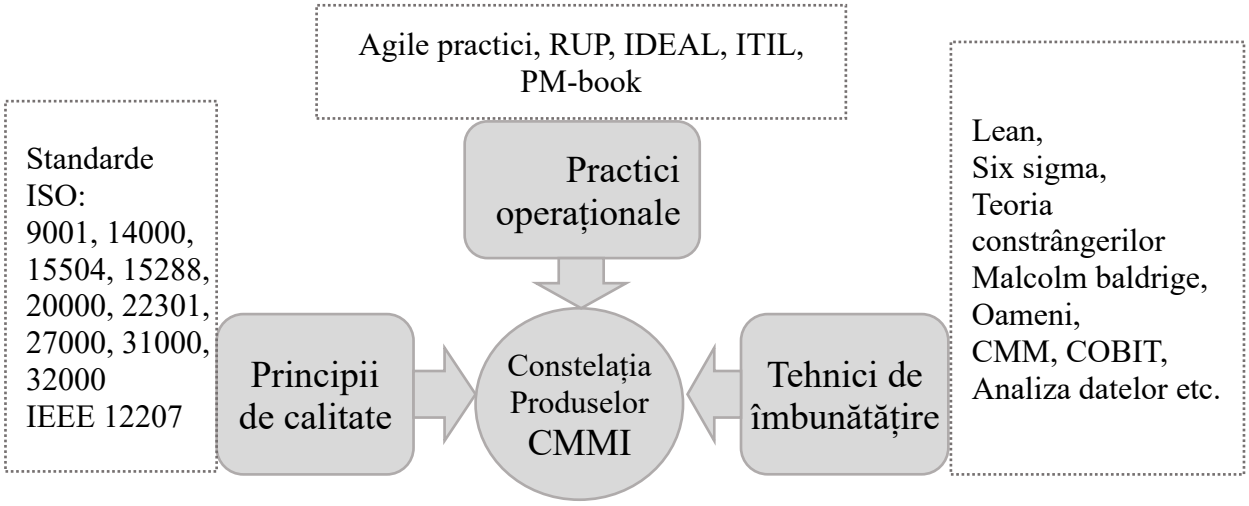


Figura 2.2. CMMI ca set de cele mai bune practici de management [7]

CMMI®02, lansat în 2018, înlocuiește vechiul model CMM, dezvoltat din 1987 până în 1997. Însă doar în **ultimele două decenii,** simultan cu dezvoltarea familiei ISO27k se observă utilizarea **în masă a abordărilor PDCA** și **CMMI**. CMMI®02 reprezintă o colecție de cele mai bune practici, care sunt utilizate de către organizații pentru a crește calitatea, a îmbunătățiți satisfacția clienților și rentabilitatea angajaților în dezvoltarea și menținerea **capacității organizației de a urma procese repetabile**.

Idea, sarcina de bază este acordarea cerințelor ISO, NIST, ISACA, CMMI etc. cu cerințele, necesitățile organizației și contextele concrete ale sistemelor de management al calității, SecInf, continuității activității, incidentelor (evenimentelor) de securitate *(SIEM, Securitate a Informației și Management al Evenimentelor)* și altor SM. Dezavantajul major al integrării SM este creșterea complexității și duratei implementării. Un MM are la baza abordarea procesuală-ciclică PDCA, acceptată de toate SM, inclusiv și CMMI v. 02 [37], care permite creșterea capacității de perturbare, transformare, inovare și îmbunătățire continuă a SecInf, ajută organizațiile să devină mai rezistente și agile, să depășească concurența, să asigure conformitatea diverselor cerințe de calitate, securitate etc.

Abordarea PDCA se înscrie perfect și în standardul ISO/IEC 27001 *(Fig. 2.3).*

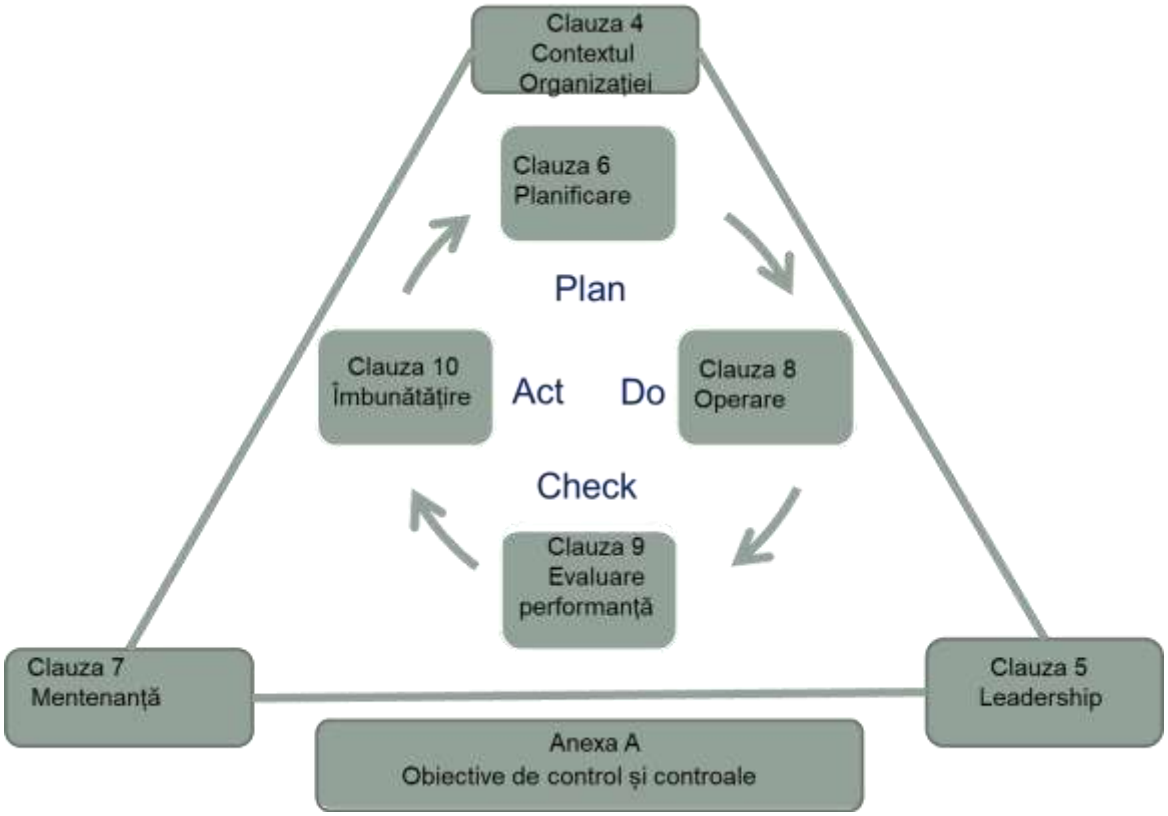


Figura 2.3. Corespunderea fazelor PDCA cu clauzele ISO/IEC 27001

Această sarcină este confirmată de noua ediție a standardelor-pereche ISO/IEC 27001:2022 [11] și ISO/IEC 27002:2022 [19], care și-au extins cel mai de sus titlu de la *„Securitatea informațiilor”* la „*Securitatea informațiilor****, securitatea cibernetică și protecția vieții private”.*** Evident, extinderea titlului a condus la extinderea respectivă a sferei de aplicare a familiei de standarde ISO27k [34] și „comasarea” tratării diferitelor tipuri de securitate în cadrul unui model unic și integrat.

2.1.2. Principii generale de abordare a SecInf și SMSI

Oricare ar fi paradigma și cadrul de abordare, **conceptul modern al securității informației unei organizații are la bază domeniile, obiectivele și controalele unuia dintre standardele formatoare** precum ISO/IEC 27001:2022 [11] sau seria NIST SP 800-53 rev.5 [44] sau COBIT 2019 [35] sau O-ISM3 [8, 39, 42] etc. În toate cazurile enumerate este aplicată abordarea procesuală PDCA și îmbunătățirea continuă ca cerințe-cheie. Alte cadre standard, e.g. PCI DSS [20], ISO/IEC 27032 [4], ISO/IEC 27003:2017 [46], ISO/IEC 27004:2016 [47], ISO/IEC 27005:2022 [28], ISO/IEC 27007:2020 [48] etc. au rolul preponderent de *suport tehnic specific domeniului, contextului, controlului* etc., ținând cont de misiunile și țintele urmărite de organizație. Inclusiv standardele comitetului *ISO/IEC JTC 1/SC 27 Securitatea informațiilor, securitatea cibernetică și protecția vieții private,* seria ISO28K *(sisteme de management a securității pentru lanțul de furnizare/aprovizionare),* seriei ISO29K [49] *(standarde/cerințe tehnice – TS/TR)* etc.

Totodată, în realizarea SMSI și gestionarea SecInf sunt utilizate o serie de alte principii și paradigme. De exemplu, principiile general acceptate pentru orice sistem de management, inclusiv SMSI, cel mai bine expuse în standardul de management al calității ISO 9001:2015 [41] *(identic cu standardul european EN 29000)* și reproduse în ISO/IEC 27001:2022. În continuare foarte succint este expusă esența acestor principii în conformitate cu [41]/EN 29000.

1. **Orientarea spre client** – activitățile trebuie proiectate și realizate în așa fel, încât să determine satisfacția clientului. Satisfacția clientului este direct legată de cunoașterea necesităților și așteptărilor clientului. Iar domeniul serviciilor bancare, îndeosebi a plăților electronice, mediate de telefonia mobilă, carduri bancare, Internet și Web este unul foarte practicat de clienții băncilor.

2. **Leadership/**angajamentul și susținerea conducerii de vârf – liderii stabilesc unitatea scopurilor și direcțiilor de activitate ale organizației. Aceștia trebuie să creeze și să mențină o platformă de lucru în care echipa SMSI să fie total implicată în atingerea obiectivelor organizației în condiții de siguranță a informației, ca avere importantă a firmei.

3. **Angajamentul/implicarea personalului** – nu doar echipa SMSI este cheia succesului. Implicarea totală a personalului de la toate nivelurile constituie esența organizației și ar permite aplicarea capacităților și experienței acestora în beneficiul organizației, inclusiv în asigurarea SecInf.

4. **Abordarea ciclică bazată pe proces/PDCA** – rezultatele scontate/dorite sunt mai eficient atinse/realizate când activitățile sunt gestionate ca procese, ca ansamblu de activități, pași care prin realizarea lor transformă elementele de intrare în elemente de ieșire conform unor reguli prestabilite și documentate.

5. **Îmbunătățire continuă** – ca obiectiv stabil și dezirabil al organizației. Fiecare subdiviziune poate și trebuie, întru asigurarea SecInf, să își îmbunătățească permanent propria activitate prin procesele de formare și perfecționare continuă, buna colaborare cu celelalte subdiviziuni, clienți și parteneri de afaceri.

6. **Luarea deciziilor bazată de dovezi** – toate rezultatele proceselor desfășurate de SecInf trebuie documentate și păstrate pentru asigurarea trasabilității lor, pentru auditul intern sistematic al SMSI/SecInf (1-2 ori pe an) și trasarea măsurilor de înlăturare a neconformităților majore, importante pentru SecInf și succesul afacerii.

7. Abordarea sistemică (și integrată) – cuvântul cheie este **„sistem”**, ca set de elemente corelate, în interacțiune, formând un tot organizat și unitar de componente cu noi proprietăți, ce lipsesc componentelor. Sistemul are calități sinergice, mai multe decât simpla sumare a caracteristicelor componentelor sale și este în legătură cu alte SM.

8. **Managementul relațiilor cu părțile interesate** – organizația și clienții săi sunt interdependenți, iar o relație mutual benefică crește abilitatea de succes a ambelor părți și de conservare a proprietăților fundamentale primare și secundare ale SecInf.

De exemplu, conform [41] în cadrul abordării ciclice PDCA, un **proces** este definit ca una sau mai multe tipuri de activități gestionate care utilizează resurse și care vizează transformarea cerințelor inițiale în ieșiri/îndeplinirea cerințelor *(Fig. 2.4)*.

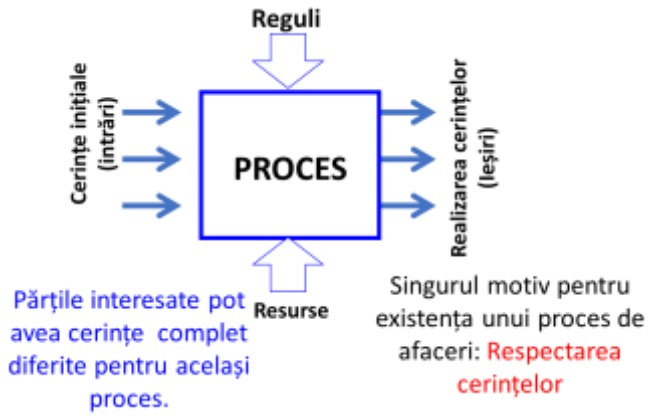


Figura 2.4. Definirea procesului în SM

O dilemă a abordării sistemice este nivelul de integrare a SMSI cu alte SM care duce spre o complexitate sporită, creșterea duratei implementării *(Fig. 2.5)*.

Figura 2.5. Integrarea SMSI cu alte în SM

Integrarea masivă a SMSI vine în contradicție cu principiul simplității și decizia trebuie adoptată cu mare acuratețe, ținând cont de scop, circumstanțe, nivel de maturitate etc.

Alte zece principii sunt examinate în O-ISM3, 2017 [8], [42] printre care sunt de menționat: *Abordarea bazată pe risc, Arhitectura zero trust (ZTA) [45], Privilegii minimale, Securitate incorporată prin design, Apărarea în profunzime, Paradoxul lui Mayfield [43]* și altele, unele dintre ele fiind expuse succint în continuare.

Abordarea bazată pe risc. Crearea unui profil particular al controalelor de securitate pentru o organizație presupune o analiză a riscurilor de securitate [5, 8, 28] pentru a stabili **apetitul și pragul de risc**. În mod ideal, este necesară o analiză cantitativă a riscului prin inventarierea, analiza, evaluarea, aprecierea și prioritizarea riscurilor în funcție de valoarea lor, calculată ca produs dintre probabilitate și impact . Dar, în realitate **determinarea probabilității și impactului se realizează prin analiza calitativă**, cu calificative de genul *foarte mic – mic – mediu – mare – foarte mare*, care ulterior se transformă prin coeficienți în valori cantitative.

Arhitectura zero trust sau zero încredere *(NIST SP 800-207:2020, [45])* este termenul pentru un set de paradigme de securitate a informației, care permit organizațiilor să securizeze aplicații, API- uri *(interfețe de programare a aplicației)* și orice integrări de date/informații, în orice rețele interne/corporative și rețele publice/Internet, pe orice dispozitive, inclusiv în Cloud sau în rețele nesigure (zero trust) oriunde acestea s-ar afla, fără să le forțeze să fie pe o rețea „sigură”. **Încrederea zero** presupune că **nu există încredere implicită** acordată activelor sau conturilor de utilizator bazate exclusiv pe locația lor fizică sau de rețea sau pe

baza proprietății activelor și dispozitivelor *(corporative sau deținute personal)*. Autentificarea și autorizarea utilizatorilor și dispozitivelor sunt funcții discrete efectuate înainte de stabilirea unei sesiuni către o resursă de întreprindere. Arhitectura ZTA este un răspuns foarte potrivit cu tendințele telelucrului la distanță și a politicilor moderne ale majorității companiilor de a permite angajaților utilizarea propriilor dispozitive mobile la locul de muncă, generic numite BYOD *(Bring Your Own Device)* și utilizarea activelor bazate pe Cloud, care nu se află în zona demilitarizată a organizației. Pentru detalii a se vedea *Principiile de bază zero trust [45], [50].*

Paradoxul lui Mayfield [43], un principiu fundamental al securității informației, reprezentat grafic prin două curbe asimptotice în spațiul bidimensional, **curba riscurilor** și **curba investițiilor** cu costul sistemului pe axa verticală și cota persoanelor ce poate accesa sistemul pe axa orizontală, cu un optim în punctul de întretăiere a curbelor *(Fig. 2.6)*. Paradoxul lui Mayfield subliniază că **acces perfect** *(fără restricții de securitate)* și **securitate perfectă** *(fără restricții de acces)* **sunt cazuri extreme** cu costuri ce tind la infinit, **între care trebuie găsit un optim**. Or, la un moment dat, securitatea suplimentară devine nerealist de costisitoare, la fel cum și adăugarea de utilizatori suplimentari devine nerealist de scumpă, iar diferența dintre aceste două costuri este relativ mică. Deoarece **este nevoie de o sumă infinită de bani, atât pentru a ține pe toți în afara unui sistem informațional, cât și pentru a asigura accesul tuturor la acest sistem**, a cheltui bani suplimentari pentru îmbunătățirea securității dincolo de un anumit punct produce randamente diminuate, iar creșterea accesului duce la o gestionare deficitară. Semnificația acestui paradox pentru SecInf constă în soluționarea dilemei tipice de management de **corelare a riscurilor cu bugetul de securitate** în mod realist, ceea ce confirmă principiul **SMSI privind tratarea doar a informațiilor valoroase** pentru o persoană/organizație în atingerea obiectivelor urmărite și doar în măsura în care trebuie. În aplicarea practică Paradoxul Mayfield poate fi ilustrat prin regula/ principiul Pareto pentru echilibrarea **cost - securitate** a măsurilor de SecInf *(Fig. 2.6)*.

Curbele sunt variabile în timp în funcție de condițiile de mediu și au valoare pentru o analiză calitativă. Curba riscurilor are relevanță cantitativă doar pentru un anumit tip de risc. Iar investițiile în securitate cuprind:

- Achizițiile de echipamente și software;
- Consultanță și mentenanță;
- Cheltuieli de întreținere (licențe, actualizări, garanții etc.);
- Costuri cu personalul de deservire;
- Costuri prin restricții în activitățile care penalizează profitul.

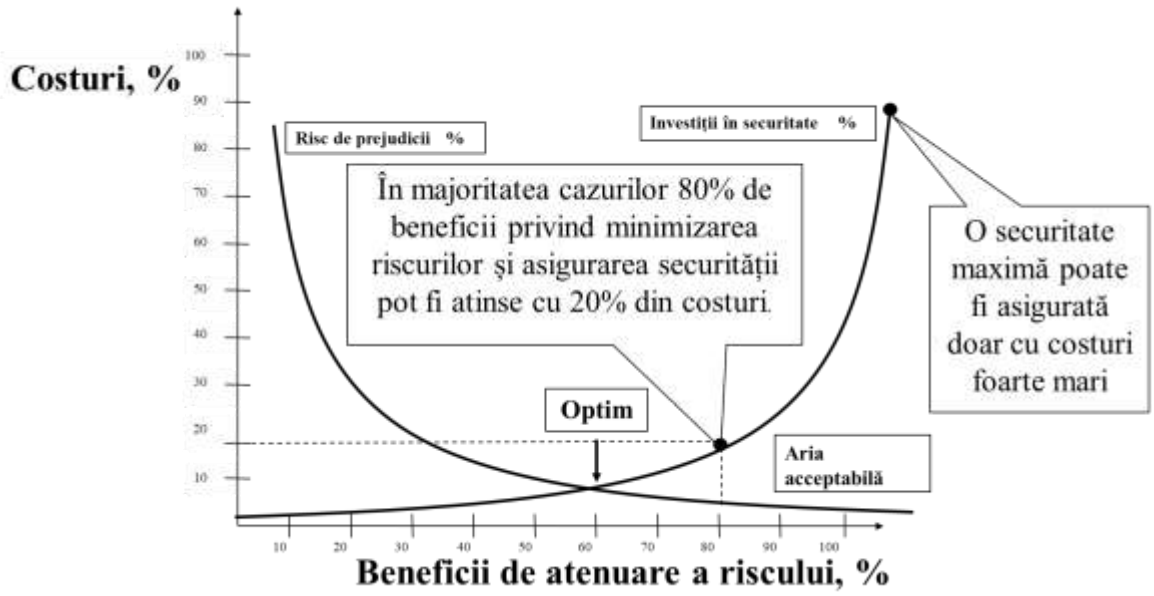


Figura 2.6. O ilustrare a paradoxului Mayfield pe diagrama de echilibrare

În realitate nu există și nici nu este rațională o securitate ideală, absolută; fiecare organizație își are propriile sale necesități, limite, care trebuie corelare cu bugetul de securitate în mod realist. Iar pentru a sublinia necesitatea prioritizării riscurilor de SecInf este binevenită regula Pareto. Cel mai des această regulă este ilustrată în cifre, e.g.: *20% din cumpărători aduc 80% din veniturile unui magazin; sunt necesare cca 20% de efort pentru a atinge 80% din rezultatul preconizat* etc. Însă trebuie menționat că regula Pareto nu este despre cifrele 80/20, care pot fi și 70/30 sau 60/40. **Regula Pareto este despre ordonarea, prioritizarea sarcinilor**, acțiunilor, valorilor etc. Acest lucru este confirmat de **abordarea SecInf bazată pe riscuri,** cu prioritizarea celor mai valorase active și resurse informaționale, ce au impact semnificativ asupra afacerii, cu identificarea, analiza, evaluarea și tratarea riscurilor majore ce amenință SecInf de la cele mai mari spre cele mai mici, **cât permite timpul și resursele alocate.** Paradoxul lui Mayfield și Diagrama de echilibrul cost – securitate oferă vizualizarea ariei de decizii acceptabile, care depinde de necesitățile și de resursele disponibile pentru securitate:

- Deplasarea spre dreapta față de optim semnifică o investiție în viitor;
- Deplasarea spre stânga față de optim semnifică o rămânere în urmă.

Evident, în realitate totul este ceva mai complicat decât în aparență *(„Viața e mai complicată decât pare”, un citat din operele lui A. Cehov*): uneori sunt cheltuiți bani suplimentari pentru pseudo-îmbunătățirea securității dar, cel mai des, SecInf este slab conștientizată și investițiile, bugetele pentru SecInf sunt diminuate. Creșterea culturii SecInf fiind un vector constant de-a lungul timpului.

2.1.3. Cele mai răspândite cadre și surse de bune practici de abordare a SecInf

Astăzi trăim într-o societate informațională globală în care organizațiile de la mici și mari, publice și private au sarcina de a respecta multiplele politici, cadre legale de reglementare în domeniul securității cibernetice la nivel global, național și local, o parte a acestora fiind afișată în *Figura 2.7*

Figura 2.7. O parte din sursele celor mai bune practici

La nivel global, cel mai universal și recunoscut cadru de abordare al SecInf este *ISO/IEC 27001* de la ISO. Standardele Comisiei *ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection* [33] abordează cele mai comune provocări de securitate a informației, indiferent de tipul organizației, industrie, mărime, dislocare, specificând cerințe flexibile pentru crearea, implementarea, operarea, revizuirea, menținerea și îmbunătățirea continuă a SMSI. Familia ISO27k [34] este o normă internațională formatoare cu circa 80 de standarde operaționale dintre cele 100 planificate, care definesc cerințele pentru conceperea și administrarea unui SMSI, aspectele de securitate logică, fizică și organizațională, precum și recomandările de bune practici. De exemplu, cerințele față de: SMSI *(ISO/IEC 27001:22, 4 domenii, 93 de controale [11])*, securitatea în Cloud (ISO/IEC 27017:2015 [51]), securitatea cibernetică (ISO/IEC 27032:2023 [4]), continuitatea funcționării/activității TIC ISO/IEC 27031:2011 [52], securitatea în rețea (ISO/IEC 27033, 7 părți [53]) etc.

Conform ISO/IEC 27001:2022, SMSI realizează gestionarea SecInf la trei niveluri:

- **Strategic,** se ocupă de obiective pe termen lung și furnizarea de resurse;
- **Tactic,** se ocupă de obiective specifice pe termen scurt și gestionarea resurselor;
- **Operațional,** se ocupă de atingerea obiectivelor definite la primele două niveluri.

Într-o organizație de dimensiuni mici și mijlocii este posibil ca cele trei niveluri să fie comprimate în două, conducerea de vârf asumându-și atât responsabilități strategice, cât și responsabilități tactice. Iar managementul junior ar putea deține atât roluri tactice, cât și roluri operaționale de aplicare a SMSI.

Un alt cadru global general, amplu și cuprinzător este COBIT 2019 *(Control OBjectiv for TI, [35])* de la ISACA (*Information Systems Audit and Control Association),* o evoluție a versiunii anterioare COBIT 5. În versiunea COBIT 2019 pentru evaluarea procesului, structurii organizaționale, informațiilor și altor tipuri de componente de management din nou sunt utilizate nivelurile de maturitate între 0 *(lipsa oricăror capacități de bază)* și 5 *(conformitate deplină).* Inițial lansat în 1996 ca instrument de audit și control, ulterior COBIT a devenit un **model de proces universal** care ajută nu doar în evaluarea TI, SI, ci și în construirea unui sistem eficient de management al informației și tehnologiei informației, adecvat obiectivelor stabilite de conducerea organizației. COBIT 2019 include 5 domenii de management *(Evaluare, direcționare și monitorizare (EDM); Aliniere, planificare și organizare (APO); Construire, achiziționare și implementare (BAI); Livrare, servicii și asistență (DSS); Monitorizare, evaluare și apreciere (MEA))* cu sumarul de patruzeci de procese. Pentru detalii a se vedea *(COBIT® [35]).*

Un alt cadru elaborat de *National Institute of Standards and Technology (NIST S.U.A.)* [36] și utilizat pe larg în toată lumea pentru gestionarea securității cibernetice este seria de **publicații speciale NIST SP 800.x.** De exemplu, NIST SP 800-39 se referă la gestionarea riscului de securitate a informațiilor; NIST SP 800-61 Rev. 2 se referă la gestionarea incidentelor de securitate; NIST SP 800-66, Rev. 1 este un ghid introductiv de resurse pentru implementarea HIPAA. Însă cea mai importantă este seria NIST SP 800-53 rev. 5 din 2020. Toate publicațiile NIST pot fi găsite la adresa *http://csrc.nist.gov/publications/.* Implementarea cadrului NIST SP se bazează pe obținerea rezultatelor descrise în profiluri-țintă cu patru niveluri: *nivelul 1 – parțial, nivelul 2 – informat despre risc, nivelul 3 – repetabil, nivelul 4 – adaptiv.* Un profil permite organizației să stabilească o foaie de parcurs pentru reducerea riscului de securitate cibernetică, aliniată la obiectivele organizaționale și industriale, ia în considerare cerințele legale de reglementare și cele mai bune practici și reflectă prioritățile de gestionare a riscurilor. Organizațiile pot alege să aibă profiluri multiple conform nevoilor individuale, aliniate la anumite componente și/sau misiuni.

Modelul **Open Information Security Management Maturity Model** *(O-ISM3, 2017, [8], [39], [42])* este dezvoltat de către consorțiul independent The Open Group, este compatibil cu/și ține cont de cerințele ISO27k, COBIT, ITIL. La fel ca și acestea, **modelul O-ISM3 cere ca**

procesele ISMS să fie documentate, măsurate și controlate. De asemenea, O-ISM3 se bazează pe o abordare completă a procesului de management al SecInf și pe maturitate, în baza cărora **fiecare control are nevoie de un proces pentru gestionarea sa**. Nivelurile de maturitate în O-ISM3 sunt aceleași ca și în COBIT 2019. Modelul O-ISM3 a fost dezvoltat ca o metodologie de suport a managerilor de SecInf în evaluarea propriilor medii de lucru și în planificarea proceselor de gestionare a securității. Ca și ISO27k, O-ISM3 este aplicabil oricărui tip de organizații *(firme comerciale, organizații neguvernamentale, întreprinderi industriale)*, indiferent de dimensiune, context și resurse și, de asemenea, cere ca procesele de SecInf să fie „*documentate, măsurate și controlate"*.

General Data Protection Regulation *(GDPR, 2016, [15])* este un cadru legal de conformitate bazat pe responsabilitatea pentru protecția datelor cu caracter personal în Europa, lansat în 2016 cu aplicare din 25 mai 2018 pentru toate statele membre ale UE. GDPR impune reguli noi pentru operatorii de date, o mai mare responsabilitate a acestora prin numirea administratorilor cu protecția datelor (DPO), sancțiuni pentru nerespectarea dispozițiilor regulamentului și altele în vederea controlului și supravegherii prelucrării datelor cu caracter personal.

2.1.4. Abordarea SecInf bazată pe modele de maturitate

Un model multiprofil de maturitate a securității informației este o metodologie/un cadru structurat care ajută organizațiile să măsoare, să evalueze și să îmbunătățească capacitatea lor de a proteja **informațiile sensibile** de-a lungul timpului. Permite determinarea nivelului actual de securitate a informației în cadrul unei organizații și identificarea domeniilor care necesită îmbunătățiri. Este structurat pe mai multe niveluri sau etape de maturitate, de la cele mai primitive practici de securitate, până la cele mai avansate și integrate procese de management al securității.

Cu toate că M^3SI se concentrează pe aceleași domenii, politici, proceduri, tehnologii, comportamente și măsuri/controale de securitate a informației ca și standardele globale de bune practici, diferă de acestea prin abordarea holistică, integrală etc. Principala diferență este că M^3SI propune și mecanismul de îmbunătățire continuă prin înseși etapizarea bazată pe cele cinci niveluri de maturitate, ce permite o continuitate a proiectelor de îmbunătățire continuă. Implementarea unui model multiprofil de maturitate a securității informației poate ajuta organizațiile să își îmbunătățească în mod sistematic și eficient securitatea informației, reducând astfel riscurile de securitate și protejând mai bine datele și resursele informaționale.

Principalele caracteristici ale unui model multiprofil de maturitate a SecInf se referă la:

- Evaluarea holistică;

- Niveluri de maturitate;
- Personalizabil și adaptabil;
- Focusare pe îmbunătățirea continuă;
- Managementul riscurilor.

2.1.4.1. Evaluarea holistică

Evaluarea holistică în contextul unui model multiprofil de maturitate a securității informației se referă la o abordare completă și integrată de examinare a tuturor aspectelor securității informației într-o organizație. Include evaluarea și gestionarea riscurilor asociate cu SecInf, asigurând că măsurile de protecție sunt proporționale cu nivelul identificat de risc. Aceasta nu se limitează doar la tehnologiile de securitate implementate, ci include o gamă largă de elemente, cum ar fi **politici, proceduri, comportamente** umane și **aspecte organizatorice**. Evaluarea holistică este fundamentală pentru a asigura o protecție eficace și cuprinzătoare a informațiilor. Printre componentele-cheie ale evaluării holistice sunt de menționat:

1. Politici și Proceduri: Evaluarea include revizuirea politicilor de securitate a informației ale organizației, pentru a verifica dacă sunt actualizate, relevante și în conformitate cu standardele și reglementările în vigoare ale industriei. De asemenea, analizează modul în care aceste politici sunt implementate și respectate în practică.

2. Managementul Riscurilor: Un aspect crucial al evaluării holistice este identificarea, evaluarea și gestionarea riscurilor de securitate a informației. Aceasta implică o înțelegere a amenințărilor potențiale, a vulnerabilităților sistemelor și a impactului potențial al incidentelor de securitate, pentru a putea prioritiza și implementa măsuri adecvate de atenuare.

3. Tehnologie: Se examinează tehnologiile de securitate utilizate de organizație, cum ar fi firewall-uri, sisteme de prevenire a intruziunilor, software antivirus și criptare. Evaluarea include, de asemenea, configurarea și managementul acestor tehnologii, pentru a se asigura că sunt eficiente în protejarea împotriva amenințărilor cunoscute și emergente.

4. Conștientizarea și formarea: Este esențial să se evalueze nivelul de conștientizare a securității informației în rândul angajaților și eficacitatea programelor de formare. Angajații bine informați constituie o linie importantă de apărare împotriva incidentelor de securitate.

5. Gestionarea incidentelor și planurile de continuitate a afacerii: Se analizează procedurile organizației pentru răspunsul la incidente de securitate și planurile de continuitate a afacerii. Este crucial să existe planuri bine definite și testate pentru a răspunde rapid și eficient la incidente și pentru a asigura continuitatea operațiunilor în caz de întreruperi cauzate de forța majoră.

6. Cultură organizațională: Se examinează cultura de securitate a organizației, care include angajamentul conducerii, comunicarea deschisă despre securitatea informației și promovarea unui mediu în care securitatea este o responsabilitate partajată.

Evaluarea holistică permite organizațiilor să obțină o imagine completă a stării SecInf și să identifice punctele forte, precum și domeniile care necesită îmbunătățiri. Prin abordarea securității informației într-un mod integrat și cuprinzător, organizațiile pot implementa strategii eficace de securitate, îmbunătățind astfel protecția datelor și a sistemelor lor de informații.

2.1.4.2. Niveluri de maturitate

Nivelurile de maturitate *(Fig. 2.8)* în cadrul unui model multiprofil de maturitate a securității informației reprezintă **diferite etape prin care o organizație trece în procesul de îmbunătățire a gestionării și protecției informațiilor**, permițând organizațiilor să identifice unde se află la un moment dat în domeniu securității informației și ce pași trebuie să urmeze pentru a avansa.

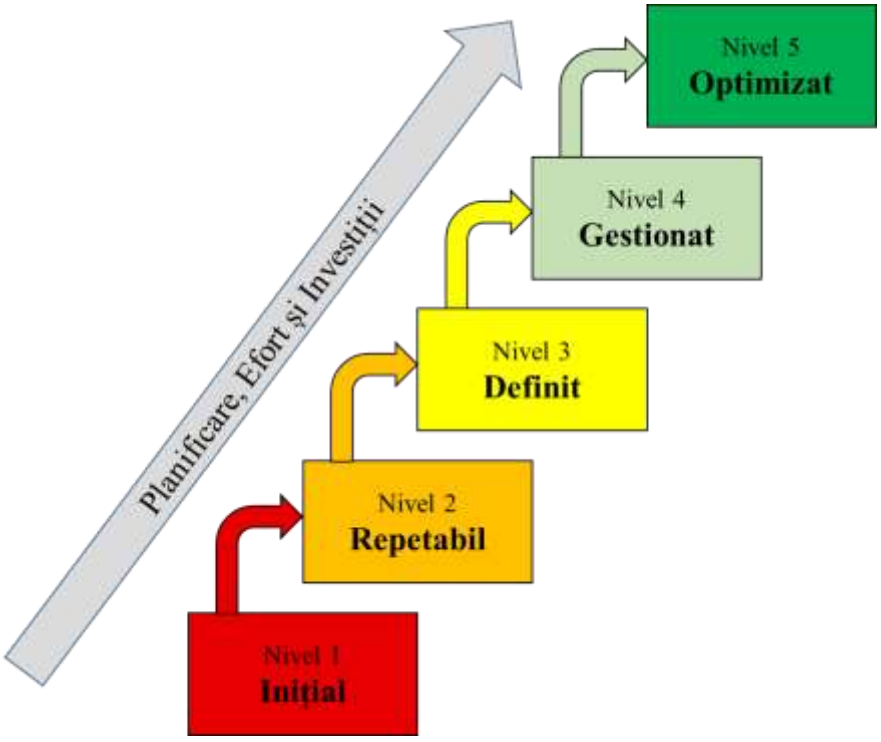


Figura 2.8. Scările modelului de maturitate (Adaptată de autor în baza [69])

Aceste niveluri ajută la **evaluarea capacității curente** a unei organizații de a proteja informațiile și la **gestionarea mai eficientă** a securității informației. În mod tipic, modelele de maturitate includ între trei și cinci niveluri, fiecare descriind un grad de complexitate și integrare a proceselor de securitate a informației.

Nivelul 1: Inițial (Ad-hoc)/nonconformitate. Nevoia de control intern nu este recunoscută. Controlul intern nu este parte din cultura organizațională sau din misiune. Există un risc ridicat de incidente și deficiențe ale controlului.

Caracteristicile nivelului: La acest nivel, practicile de securitate a informației sunt nestructurate și realizate ad-hoc. Măsurile de securitate pot fi implementate, dar fără o planificare sau o coordonare consistentă. **Identificare:** Există o lipsă de procese formalizate și reacțiile la incidente de securitate sunt mai degrabă reactive decât proactive.

Nivelul 2: Repetabil (Definit), Conformitate inițială. Nevoia de control intern este oarecum recunoscută. Abordarea riscurilor și cerințele necesare controlului sunt ad-hoc și dezorganizate, fără comunicare sau monitorizare. Deficiențele nu sunt identificate. Este posibil ca angajații să nu fie conștienți de responsabilitățile lor.

Caracteristici: Organizația începe să dezvolte și să implementeze politici și proceduri standardizate pentru securitatea informației. Practicile de securitate sunt încă dependente de persoane individuale și nu sunt complet integrate în operațiunile de zi cu zi. **Identificare:** Se recunoaște necesitatea unui cadru de securitate și se fac eforturi pentru a stabili reguli și proceduri.

Nivelul 3: Definit (Standardizat), Conformitate de bază. Controalele se desfășoară și sunt documentate adecvat. Eficacitatea operațională este evaluată în mod periodic și există un număr mediu de probleme. Cu toate acestea, procesul de evaluare nu este documentat. Deși conducerea este capabilă să rezolve în mod previzibil majoritatea problemelor de control, unele puncte slabe ale controlului persistă și impactul poate fi încă dur. Angajații sunt conștienți de responsabilitățile lor în ceea ce privește controlul.

Caracteristici: La acest nivel, practicile de securitate sunt formalizate și documentate. Politicile și procedurile de securitate sunt integrate în procesele de afaceri zilnice. **Identificare:** Organizația are un cadru de gestionare a securității informației care este urmat consecvent în toate departamentele.

Nivelul 4: Gestionat, Conformitate acceptabilă. Există un control intern eficient și un mediu de management al riscului. Evaluarea controalelor, formală și documentată, are loc frecvent. Multe controale sunt automatizate și revizuite în mod regulat. Conducerea poate detecta majoritatea problemelor de control, dar nu toate controalele sunt definite în mod regulat. Există o etapă următoare în care se abordează punctele slabe ale controlului, care au fost identificate. O folosire tactică, dar limitată a tehnologiei este aplicată pentru controale automate.

Caracteristici: Practicile de securitate sunt acum gestionate și revizuite periodic pentru eficacitate. Organizația utilizează metrici pentru a măsura performanța securității informației și se

angajează într-un proces continuu de îmbunătățire. **Identificare:** Exista un angajament clar față de îmbunătățirea continuă, bazată pe evaluarea performanței și pe feedback.

Nivelul 5: Optimizat, Conformitate deplină. Un program pentru control și riscuri, extins în toată compania, asigură controlul eficient și continuu și rezolvarea problematicii riscurilor. Controlul intern și managementul riscului sunt incluse în practicile întreprinderii, sprijinite de monitorizarea automatizată în timp real, ce presupune luarea întregii răspunderi pentru monitorizarea controlului, managementul riscului și impunerea respectării sarcinilor. Evaluarea controlului este un proces continuu, bazat pe autoevaluare și analiza breșelor și a cauzelor primare. Angajații sunt implicați proactiv în îmbunătățirea controlului.

Caracteristici: La cel mai înalt nivel, procesele de securitate a informației sunt complet integrate în toate aspectele operațiunilor organizației. Organizația inovează și se adaptează continuu la noi amenințări și tehnologii, îmbunătățind constant securitatea informației. **Identificare:** Existența unei culturi organizatorice care promovează securitatea informației ca parte integrantă a tuturor activităților

Importanța nivelurilor de maturitate constă în faptul că acestea oferă un cadru pentru organizații de a evalua eficacitatea gestionării securității informației și de a identifica domeniile de îmbunătățire. Progresul de la un nivel la altul necesită investiții în tehnologie, formare, procese de măsurare și evaluare și, cel mai important, o schimbare culturală în organizație, astfel încât SecInf să devină o prioritate constantă și integrată în toate activitățile organizației. Prin urmare, nivelurile de maturitate nu doar că măsoară progresul, dar și ghidează organizația în planificarea și implementarea măsurilor necesare pentru a avansa către o securitate a informației mai robustă și mai integrată.

Focusare pe aspectele critice. Avansarea prin nivelurile de maturitate ajută organizațiile să se concentreze asupra aspectelor critice ale securității informației, inclusiv pe gestionarea riscurilor, conformitatea cu reglementările, protecția datelor personale și prevenirea breșelor de securitate. Acest lucru asigură că eforturile de securitate sunt aliniate cu obiectivele generale de afaceri și cu cerințele legislative și normative.

Măsurare și evaluare. Implementarea în entitate a unui model de maturitate oferă mijloacele necesare pentru a măsura și evalua eficacitatea practicilor de securitate a informației. Organizațiile pot folosi indicatori cheie de performanță (KPI) și alte metrici pentru a monitoriza progresul și pentru a face ajustări acolo unde este necesar.

Cultura de Securitate. Progresul către niveluri superioare de maturitate reflectă și o schimbare culturală în organizație, unde securitatea informației devine o responsabilitate comună,

împărtășită de toți membrii organizației. Acest lucru crește conștientizarea și responsabilitatea individuală, contribuind la o protecție mai eficace a informațiilor.

În concluzie, nivelurile de maturitate în cadrul unui model de securitate a informației sunt esențiale pentru a ghida organizațiile în procesul de consolidare a securității informației. Ele oferă un cadru pentru evaluarea situației curente, pentru stabilirea obiectivelor de îmbunătățire și pentru măsurarea progresului. În timp, acest proces continuu de evaluare și îmbunătățire ajută la crearea unei fundații solide pentru protecția eficientă a datelor și a sistemelor informaționale în fața amenințărilor în evoluție.

2.1.4.3. Personalizabil și adaptabil

Caracteristica „Personalizabil și adaptabil" a unui model multiprofil de maturitate a securității informației subliniază flexibilitatea acestui tip de cadru în a se adapta la diversele nevoi, contexte și obiective specifice ale diferitelor organizații. Această caracteristică este crucială, deoarece fiecare organizație se confruntă cu un set propriu de riscuri de securitate a informației, are o cultură organizațională distinctă și operează într-un mediu de reglementare specific industriei sale. Prin urmare, un model rigid, cu o abordare unică pentru toți, adesea este ineficient.

Posibilitatea de personalizare și adaptare a modelului permite particularizarea sa adecvată în funcție de specificul industriei/sectorului de activitate, de dimensiunea organizației, de nevoile organizației și de riscurile specifice de securitate cu care aceasta se confruntă. Personalizarea și adaptarea modelului înseamnă că, deși nivelurile de maturitate sunt predefinite, modul în care o organizație progresează prin aceste niveluri poate varia, reflectând prioritățile și obiectivele specifice ale organizației. Detaliile acestei caracteristici pune în evidența mai multe aspecte, expuse în continuare.

Adaptabilitate la dimensiunea și complexitatea organizației. Modelul se poate ajusta pentru a se potrivi cu dimensiunea organizației, fie că este vorba de o întreprindere mică, o organizație de dimensiuni medii sau un conglomerat internațional. În funcție de resursele disponibile, un model personalizabil permite ajustarea complexității și profunzimii evaluărilor și inițiativelor de securitate.

Personalizare în funcție de sectorul de activitate. Diferitele industrii se confruntă cu diferite tipuri de riscuri de securitate și au reglementări specifice de conformitate. Un model personalizabil permite organizațiilor să se concentreze pe amenințările cele mai relevante pentru sectorul lor și să respecte cerințele legislative și normative specifice, cum ar fi GDPR pentru protecția datelor în Europa, HIPAA pentru confidențialitatea informațiilor medicale în S.U.A., sau PCI DSS la nivel global pentru securitatea datelor cardurilor de plată.

Flexibilitate în alocarea resurselor. Organizațiile pot aloca resurse în mod eficient, concentrându-se pe domeniile cu cel mai mare risc sau pe cele care necesită îmbunătățiri urgente. Un model personalizabil permite prioritizarea inițiativelor de securitate bazate pe evaluarea riscurilor specifice organizației, asigurându-se că bugetul și eforturile sunt direcționate acolo unde pot avea cel mai mare impact.

Integrare cu cultura organizațională. Adaptabilitatea la cultura organizațională este esențială. Securitatea informației nu se limitează doar la tehnologie și procese, ci include și comportamentele și atitudinile angajaților. Un model personalizabil poate încorpora abordări de formare și conștientizare care rezonează cu valorile și stilul de lucru specific organizației, promovând o cultură de securitate pozitivă.

Evoluție și scalabilitate. Pe măsură ce organizațiile cresc și se dezvoltă, și riscurile de securitate evoluează. Un model multiprofil de maturitate personalizabil poate scala și evolua împreună cu organizația, asigurându-se că practicile de securitate rămân relevante și eficiente în fața noilor provocări și oportunități de afaceri.

Reactivitate la schimbările tehnologice. Adaptabilitatea la inovațiile tehnologice permite organizațiilor să integreze noi soluții de securitate și să răspundă eficient la amenințările emergente. Un model flexibil permite actualizarea rapidă a practicilor de securitate pentru a include tehnologii emergente, cum ar fi inteligența artificială, blockchain sau Cloud Computing.

Adaptare la schimbările din mediul de afaceri. Un model de maturitate a securității informației care este personalizabil și adaptabil permite organizațiilor să răspundă rapid la schimbările din mediul de afaceri. Aceste schimbări pot include expansiunea pe noi piețe, adoptarea unor noi modele de afaceri, fuziuni și achiziții sau schimbări în lanțul de aprovizionare. Prin adaptabilitate, organizațiile pot asigura că măsurile de securitate a informației rămân aliniate cu obiectivele strategice și cu dinamica pieței.

Aliniere cu tehnologiile emergente și modelele de lucru. Organizațiile adoptă în mod constant noi tehnologii și modele de lucru, cum ar fi munca de la distanță, BYOD, cloud computing și internetul lucrurilor/IoT. Un model personalizabil de maturitate a securității informației permite integrarea acestor evoluții în cadrul de securitate, abordând riscurile specifice asociate cu ele și asigurând protecția datelor într-un mediu din ce în ce mai digitalizat și interconectat.

Încurajarea inovației. Prin permiterea personalizării, organizațiile nu sunt constrânse de un set rigid de practici și pot experimenta cu soluții inovatoare de securitate. Acest lucru stimulează inovația, permițând organizațiilor să exploreze noi tehnologii și metodologii pentru a îmbunătăți securitatea informației. Adaptabilitatea modelului de maturitate încurajează gândirea creativă și soluțiile personalizate, care pot oferi un avantaj competitiv.

Facilitarea conformității. Reglementările privind securitatea și protecția datelor sunt în constantă evoluție, iar organizațiile trebuie să se conformeze unui peisaj legislativ divers și dinamic. Un model de maturitate a securității informației care este personalizabil și adaptabil facilitează conformitatea prin ajustarea la cerințele specifice de reglementare și prin integrarea acestor cerințe în practicile de securitate ale organizației.

Susținerea dezvoltării durabile. Adaptabilitatea și personalizarea permit organizațiilor să abordeze securitatea informației într-un mod care susține dezvoltarea durabilă. Prin optimizarea resurselor și concentrarea pe măsuri de securitate eficiente și adaptate la nevoile specifice, organizațiile pot reduce risipa și pot contribui la un mediu de afaceri mai sustenabil.

În concluzie, caracteristica de a fi „Personalizabil și adaptabil" este esențială pentru un model de maturitate a securității informației, deoarece asigură relevanța și eficacitatea acestuia într-un peisaj tehnologic și de afaceri în continuă schimbare. Prin personalizarea și adaptarea modelului la nevoile specifice ale fiecărei organizații se pot dezvolta strategii de securitate robuste, care nu doar protejează informațiile, dar și sprijină inovația și creșterea organizației.

2.1.4.4. Focusare pe îmbunătățirea continuă

Această caracteristica încurajează organizațiile să urmărească constant îmbunătățirea practicilor și proceselor de securitate a informației, promovând un ciclu de îmbunătățire continuă. Progresul prin nivelurile de maturitate subliniază angajamentul unei organizații față de îmbunătățirea continuă. Fiecare nivel atins reprezintă o etapă în consolidarea securității informației, de la stabilirea unor baze inițiale la baze solide spre optimizarea și inovarea continuă a practicilor de securitate.

Asemenea abordare recunoaște că securitatea informației **nu este un obiectiv static**, ci **un proces dinamic** care necesită adaptare continuă la noile amenințări, tehnologii și schimbări ale mediului de afaceri. Implementarea unui ciclu de îmbunătățire continuă ajută organizațiile să rămână reziliente în fața riscurilor și să asigure protecția eficientă a datelor. În continuare sunt examinate câteva aspecte esențiale ale acestei caracteristici.

Focusarea pe îmbunătățirea continuă corespunde principiului de bază al SM, prevăzut de ISO 9001 și ISO/IEC 27001 și cunoscut ca **Ciclul PDCA,** ciclul lui **Shewhart** sau **roata calității lui Deming** *(Plan-Do-Check-Act, Planifică-Execută-Verifică-Acționează) [8, 23, 41])***.** Implementarea ciclului PDCA oferă cadrul structural pentru îmbunătățirea continuă. Organizațiile planifică inițiative de securitate (Plan), le implementează (Do), evaluează eficacitatea acestora prin monitorizare și audituri (Check) și apoi iau măsuri pentru a rectifica orice deficiențe sau pentru a

face îmbunătățiri (Act). Acest ciclu se repetă sistematic permițând organizațiilor să se adapteze și să se îmbunătățească constant.

Evaluarea periodică a riscurilor de SecInf este esențială pentru identificarea și prioritizarea amenințărilor la adresa securității informației. Prin reevaluarea regulată a peisajului de risc organizațiile pot ajusta strategiile de securitate pentru a aborda noile vulnerabilități și amenințări, asigurându-se că măsurile de protecție sunt întotdeauna relevante și eficace.

Monitorizarea și revizuirea performanței securității informației prin indicatori cheie de performanță și alte metrici permite organizațiilor să evalueze eficacitatea măsurilor de securitate implementate. Revizuirea periodică a acestor indicatori ajută la identificarea domeniilor care necesită îmbunătățiri și la prioritizarea acțiunilor corective.

Formare continuă și conștientizare. Mai multe cercetări din domeniul SC pun accent pe „factorul uman", în contextul în care oamenii sunt considerați ca cea mai slabă verigă *(asociată cu de la 70% la 95% de incidente de SC)*. Cheia în diminuarea pierderilor din cauza factorului uman constă în **formarea continuă adecvată a utilizatorilor de orice nivel**. De regulă, formarea și conștientizarea este diferită pentru diferite categorii de personal, fiecare conform rolului său, necesităților sale și formei potrivite *(Fig. 2.9)*.

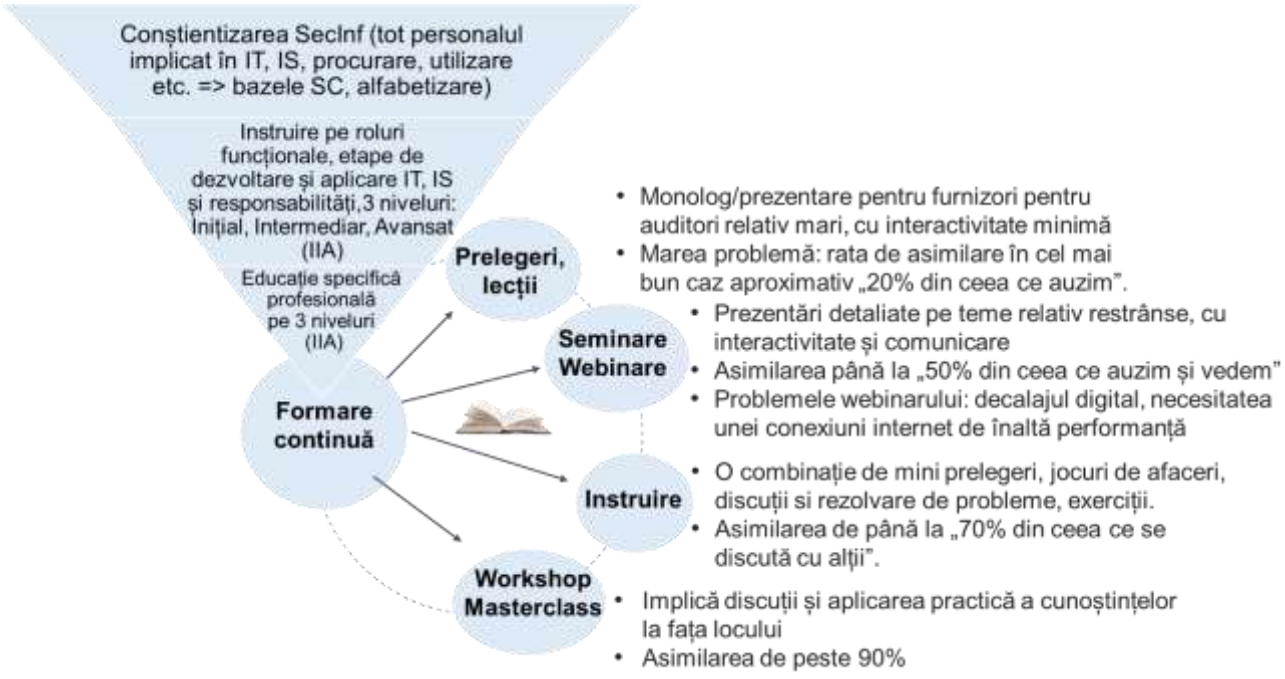


Figura 2.9. Formare continuă în domeniul securității informației

Programul de formare și conștientizare pentru angajați trebuie revizuit și actualizat periodic pentru a reflecta noile amenințări și cele mai bune practici. Educația continuă a personalului este vitală pentru a asigura că toți membrii organizației de la simpli operatori la top management înțeleg riscurile de securitate și contribuie la protecția informațiilor *[55, 56, 57]*.

Cunoștințele, abilitățile, competențele pot fi obținute prin diferite forme de instruire, precum lecții, seminare/webinare, ateliere de lucru și antrenament, discuții etc. Există un șir de întrebări și reguli principale privind formarea continuă corporativă a personalului: *cum să se formeze grupurile de cursanți; care ar trebui să fie forma și stilul de învățare potrivite; cum să traduci teoria dobândită de angajați în abilități practice reale; cum să crești motivația cursanților* etc. pentru a face pregătirea personalului cât mai eficientă.

Adaptarea la schimbări. Capacitatea de a se adapta rapid la schimbări în tehnologie, în reglementările industriei și în mediul de afaceri este crucială. Îmbunătățirea continuă asigură că practicile de securitate a informației rămân aliniate cu aceste schimbări, protejând organizația împotriva vulnerabilităților emergente și asigurând conformitatea cu legile și reglementările în evoluție.

Cultura îmbunătățirii continue. Promovarea unei culturi organizaționale care valorizează îmbunătățirea continuă contribuie la succesul inițiativelor de securitate a informației. Aceasta implică angajamentul conducerii și implicarea angajaților la toate nivelurile, recunoscând că securitatea informației este o responsabilitate comună.

Astfel, focusarea pe îmbunătățirea continuă este esențială pentru menținerea eficacității securității informației într-un peisaj digital în continuă schimbare. Prin adoptarea acestui principiu, organizațiile pot asigura că sunt pregătite să răspundă la noi provocări, să protejeze datele sensibile și să își mențină reputația și conformitatea. Această abordare nu doar că sporește securitatea informației, dar contribuie și la succesul pe termen lung al organizației prin promovarea inovației și a adaptabilității.

2.1.4.5. Managementul riscurilor

Caracteristica „Managementul riscurilor” în cadrul M^3SI a securității informației reprezintă o abordare sistematică de **identificare, evaluare, gestionare și monitorizare a riscurilor** de securitate asociate cu informațiile și activele informaționale ale unei organizații, asigurând că măsurile de protecție sunt proporționale cu nivelul identificat de risc. Această caracteristică permite organizațiilor să prioritizeze resursele și eforturile de securitate către cele mai semnificative riscuri, asigurând astfel o protecție eficientă și eficace a informațiilor. În continuare sunt elucidate câteva dintre principalele detalii ale managementului riscurilor.

Procesul începe cu identificarea/inventarierea riscurilor, care implică recunoașterea amenințărilor potențiale *(de exemplu, atacuri cibernetice, erori umane, dezastre naturale)* și vulnerabilităților *(de exemplu, slăbiciuni în software, lipsa de formare a angajaților)* care pot

expune organizația la aceste amenințări. Identificarea comprehensivă a riscurilor necesită o înțelegere profundă a proceselor de afaceri, a tehnologiilor utilizate și a mediului operațional.

Evaluarea riscurilor implică determinarea probabilității de materializare a unei amenințări și a impactului potențial asupra organizației, permițând clasificarea riscurilor în funcție de severitatea lor. Aceasta ajută la prioritizarea riscurilor și la alocarea eficientă a resurselor pentru a le aborda. Tehnici precum analiza cost-beneficiu și modelarea riscurilor pot fi utilizate pentru a sprijini procesul de evaluare. Dar, de regulă, cele mai utilizate sunt tehnicile de analiză calitativă cu coeficienți de trecere spre valori cantitative.

Tratarea riscurilor se referă la selectarea și implementarea măsurilor adecvate de atenuare a riscurilor pentru a le aduce la un nivel acceptabil. Aceasta poate include aplicarea de controale tehnice (*de exemplu, criptarea datelor, autentificarea multifactor),* controale administrative *(de exemplu, politici și proceduri)* și controale fizice *(de exemplu, securitatea accesului la încăperi).* Decizia de a accepta, evita, transfera sau atenua un risc este luată pe baza evaluării riscului și a apetitului organizației pentru risc.

Monitorizarea și revizuirea continuă a riscurilor asigură că procesul de management al riscurilor rămâne relevant și actualizat în fața schimbărilor interne și externe. Aceasta include revizuirea periodică a peisajului de risc, a eficacității controalelor implementate și a incidentelor de securitate pentru a identifica orice nevoie de ajustare în abordarea riscurilor.

Comunicarea și consultarea cu părțile interesate relevante atât în interiorul, cât și în afara organizației sunt esențiale pentru a asigura o înțelegere comună a riscurilor de securitate și a măsurilor de gestionare a acestora. Aceasta include informarea conducerii executive, a angajaților, clienților și, dacă este cazul, a autorităților de reglementare.

Integrarea în procesele organizației. Managementul riscurilor trebuie să fie integrat în procesele de afaceri și decizionale ale organizației, asigurând că considerațiile de securitate și de risc sunt parte integrantă a planificării strategice și operaționale.

Caracteristica „Managementul riscurilor” subliniază importanța unei abordări proactive și bazate pe informații în protejarea activelor informaționale. Mai multe detalii privind managementul riscurilor a se vedea în compartimentul „*2.3. Abordarea securității informației bazată pe riscuri*”.

2.2. Abordarea securității informației în baza standardelor

Actual tot mai insistent se impune și devine general acceptată **abordarea securității informației în baza standardelor** de bune practici. Deoarece standardele internaționale din domeniul securității informației, TI, SI, Internet, Web etc., dezvoltate și îmbunătățite de-a lungul

anilor, au reușit să **absoarbă cele mai bune experiențe și practici** ale specialiștilor din toată lumea.

2.2.1. Beneficiile abordării securității informației în baza standardelor

Un prim avantaj al implementării SMSI în baza standardelor este **credibilitatea și imaginea organizației**: partenerii de afaceri și clienții actuali sau potențiali preferă să aibă relații cu firme, a căror activitate este bine controlată intern și certificată extern, de către organe specializate recunoscute. Acest lucru oferă încredere că organizația controlează în mod riguros toate procesele sale interne, asigurând îmbunătățirea lor continuă; controlează și gestionează eficient riscurile și oportunitățile, oferind produse cu costuri minime, de calitate garantată în condiții de siguranță.

O altă justificare ar fi **simplitatea și transparența** oferire de standarde**,** două cerințe imperative ale SecInf, ce corespund principiului universal ***KISS:*** *Keep Its Simple, Stupid.* Mai simplu – este mai bine. Ideea este să pornim de la o abordare „ușoară" și apoi să o facem mai complexă, dacă este nevoie. A complica e ușor, dar a simplifica lucrurile este destul de complicat. În acest sens, bunele practici și recomandări stabilite în standardele de bune practici permit combaterea complexității. Utilizarea lor sugerează că nu trebuie să „născocești" nimic. Trebuie doar să urmezi îndeaproape bunele practici. Totodată, dacă SMSI este sau pare a fi prea vast, prea complex – se poate urmări dezvoltarea sa eșalonată, în acord cu regula universală Pareto.

Mai concret, implementarea SMSI în baza standardelor de bune practici **oferă numeroase beneficii pentru organizațiile și persoanele interesate:**

- Ține organizația la curent cu toate informațiile actuale în domeniu;
- Introduce în organizație o metodă sistematică de control a confidențialității, integrității și accesibilități informației, un mediu unic ce conține toate mecanismele necesare pentru autocorectare și îmbunătățire continuă;
- Contribuie la păstrarea unui nivel bun de competitivitate pe piață, îmbunătățește credibilitatea și consolidează încrederea clienților;
- Contribuie la respectarea cerințelor legale privind securitatea informației;
- Oferă posibilitatea de îmbunătățire continuă prin audituri regulate;
- Asigură continuitatea afacerii, reduce costurile de asigurare și altele.

Actual la nivel global există cca 500 de standarde și reglementări în domeniul SecInf, cu mii de măsuri (controale) de securitate, inclusiv:

- Standarde și norme de management ale securității informației, e.g. familia ISO27k;

- Reglementări tehnice, e.g. securitatea echipamentelor/sistemelor TI, SI, Securitatea Web *(OWASP, [88]);*
- Reglementări administrative, e.g. ale serviciilor de telecomunicații, GDPR;
- Relații contractuale, e.g. cu clienți, furnizori și altele.

În asemenea condiții este necesar a stabili rolul și care dintre acestea sunt vitale, succint elucidat în continuare.

2.2.2. Ierarhia standardelor de management cu atribuție la SMSI

Setul de cerințe și standarde general acceptate pentru management în general și cel al domeniului SecInf sunt prezentate în (*Fig. 2.10).*

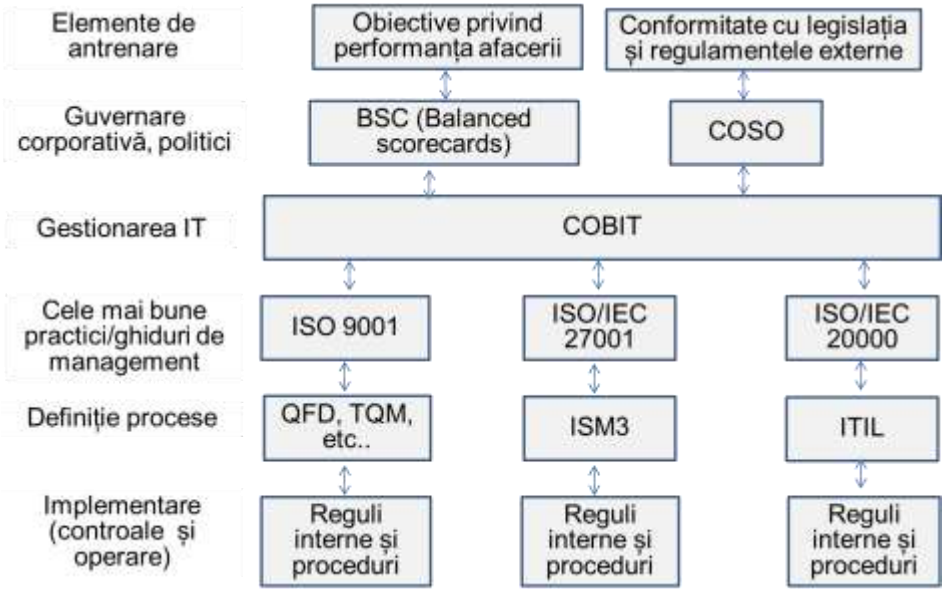


Figura 2.10. Standarde de management cu atribuție la SMSI

Aceste standarde incorporează o bogată experiența practică cu un grad mare de generalitate, reprezintă o bună structurare a informațiilor existente despre securitate și constituie ghiduri de bune practici privind construirea și utilizarea SMSI.

Conceptul **Balanced Scorecard/BSC** se referă la o metrică de performanță a managementului strategic, utilizată pentru a identifica și îmbunătăți diferitele funcții interne de afaceri și rezultatele acestora. BSC este calificat drept una dintre cele mai influente idei de afaceri din ultimii 75 de ani, este utilizat pe scară largă în afaceri și industrie, guvern și organizații nonprofit din întreaga lume. Mai mult de jumătate dintre companiile importante din lume folosesc BSC. BSC sugerează să examinăm o organizație din **patru perspective** diferite pentru a ajuta la dezvoltarea obiectivelor, factorilor critici de succes, țintelor și inițiativelor legate de acestea:

- Din perspectiva **financiară**, cu referire la performanța financiară a unei organizații și utilizarea resurselor financiare;

- Privind performanța organizațională din perspectiva **clienților** sau a **părților-cheie interesate**, pe care organizația este proiectată să-i deservească;
- Din perspectiva **proceselor interne**, prin viziunea calității, securității și eficienței unei organizații legate de produse, servicii sau alte procese-cheie de afaceri;
- Privind **capacitatea organizațională** *(învățare și creștere),* viziunea capitalului uman, a infrastructurii, tehnologiei, culturii corporative și altor capacități-cheie pentru creșterea performanței.

Toate acestea impun un sistem riguros de control intern, succint elucidat în continuare.

2.2.3. Modelul sistemului de control intern corporativ și standarde aferente

Sistemul de **control intern** în general constă din cinci componente-cheie, așa ca **mediul de control, evaluarea riscurilor, activitățile de control, informațiile, comunicarea** și **monitorizarea,** destinat pentru a asigura gestionarea riscului. Măsurile de control intern sunt menite să limiteze și să mențină riscurile asociate în limitele apetitului de risc acceptat de organizație. De regulă, *controalele interne constau din politici (uneori numite și reguli, norme, standarde interne), proceduri* și *practici* pentru a oferi o asigurare rezonabilă că obiectivele de afaceri ale organizației vor fi realizate în timp ce riscul va fi minimizat. Scopul principal al controlului intern este de a furniza o asigurare rezonabilă cu privire la atingerea obiectivelor generale ale entității. Obiectivele controalelor interne rezumă la două întrebări principale:

- Ce ar trebui să fie atins și
- Ce ar trebui să fie evitat?

Principalul model de control intern aplicat la nivel global este Modelul COSO *(Fig. 2.11).*

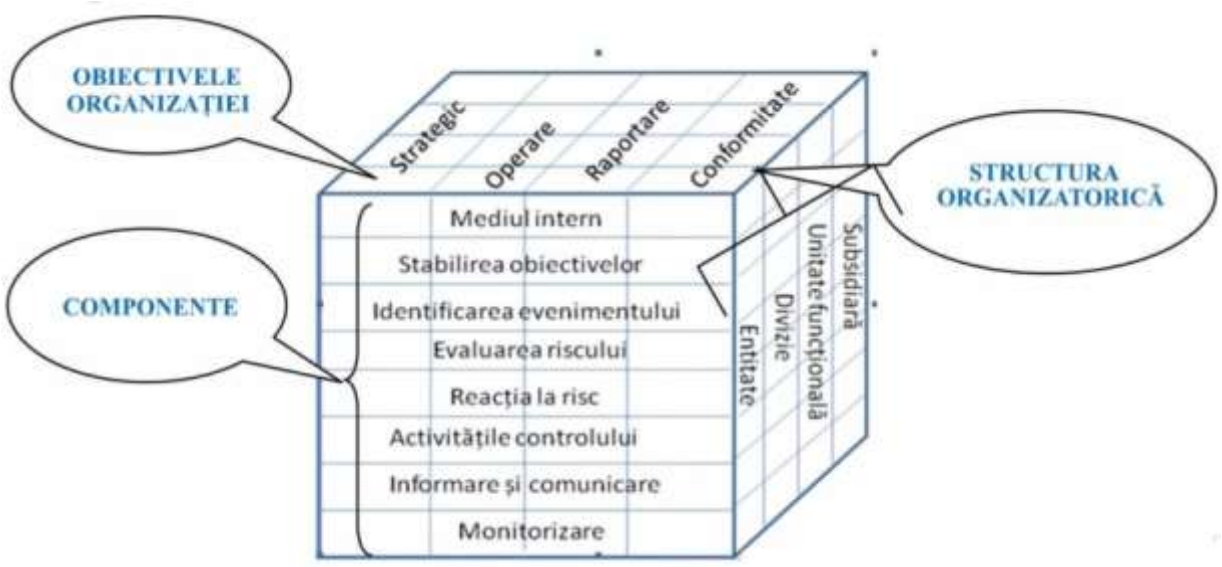


Figura 2.11. Modelul COSO al controlului intern [58]

Numele COSO provine de la *Comitetul de Sponsorizare al Organizațiilor* al Comisiei Treadway, instituită în 1985 de senatorul american Treadway, preocupată de controlul intern și a rolului sau în viața organizațiilor *și care a elaborat lucrarea intitulată „Cadrul controlului intern”*. Pentru detalii a se vedea [58]. La nivelul entităților bancare a se vedea Regulamentul [18].

Diferitele standarde oferă beneficiile unei „viziuni largi”, din diferite poziții, de exemplu:

- COBIT:2019 – un cadru organizațional TI;
- ISO/IEC 27001:2022 – abordarea sistemică și procesuală a SMSI;
- NIST SP 800-53 rev. 5 (2020) – abordarea problemelor tehnice ale securității informațiilor;
- ITIL v. 4:2019 [59] și ISO/IEC-20000 [60] – abordarea securității informației pentru furnizori de servicii, e.g. provideri de Internet etc.

Anterior deja a fost stabilit că pentru asigurarea securității informației **identificarea și gestionarea riscurilor informaționale este vitală.** Veriga principală care leagă între ele conceptele și standardele de SecInf examinate mai sus, precum și cu altele conexe, cum ar fi continuitatea afacerii, managementul incidentelor de securitate a informației etc. este managementul riscurilor *(Fig. 2.12)*.

Cu toate că unele standarde, e.g. **ISO 31000** și **ISO 22301, ISO 9001, ISO/IEC 20000-1** nu fac parte formal din familia ISO27k, NIST sau altor standarde special destinate pentru SecInf, majoritatea organizațiilor din lume au adoptate aceste standarde ca parte a cadrului lor de **gestionare a riscurilor** și de **continuitate a afacerii**.

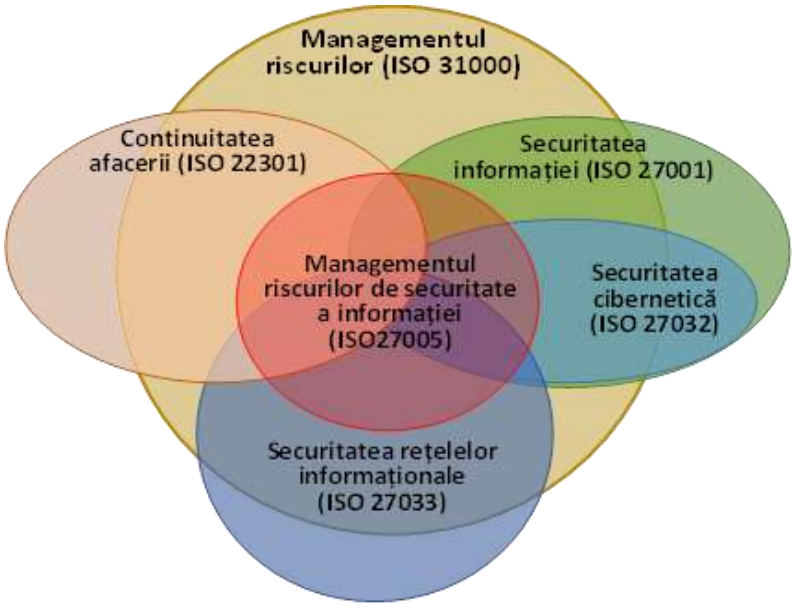


Figura 2.12. Relațiile dintre diferite concepte și standarde înrudite de SecInf: toate intră sub umbrela managementului riscului

Standardul **ISO 31000:2018** [61] se referă la toate riscurile în general, inclusiv la riscurile de SecInf. Iar asigurarea caracteristicilor fundamentale ale informației, care stă la baza conceptelor înrudite de securitate cibernetică, informatică etc. și abordarea procesuală comună bazată pe analiza riscurilor face posibilă integrarea conceptelor și sistemelor adiacente de management al calității, continuității afacerii, SecInf/SC, securității ecologice etc.

Standardul **ISO 22301:2019** [62] Security and resilience – Business continuity management systems – Requirements *(BCMS, https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en)* specifică structura și cerințele pentru implementarea și menținerea unui sistem de management al continuității activității adecvate cantității și tipului de impact pe care organizația îl poate accepta sau nu în urma unei întreruperi. Un BCMS include componente similare cu orice alt sistem de management, inclusiv SMSI. La fel ca și rezultatele întreținerii unui SMSI, rezultatele menținerii unui BCMS sunt modelate de cerințele legale, de reglementare, organizaționale și industriale ale organizației, produsele și serviciile furnizate, procesele utilizate, dimensiunea și structura organizației și cerințele părților interesate.

ISO/IEC 20000-1:2018 [60] specifică cerințele pentru o organizație privind stabilirea, implementarea, întreținerea și îmbunătățirea continuă a unui sistem de management al serviciilor. Cerințele specifică planificarea, proiectarea, tranziția, furnizarea și îmbunătățirea serviciilor pentru a îndeplini cerințele de servicii și a oferi valoare. Alte reglementări tehnice și industriale concrete a se vedea seriile de standarde ISO27k [33], ISO28k și ISO29k [49].

2.3. Analiza, evaluarea și gestionarea riscurilor securității informației

Pandemia COVID-19 a accelerat digitalizarea proceselor de afaceri, lucrul, accesul de la distanță la date sensibile și resurse informaționale corporative critice. Se observă extinderea rapidă a serviciilor de închiriere a componentelor TI *(cloud computing)*. Iar criminalitatea cibernetică urmează aceeași tendință: creșterea atacurilor globale de tip ransomware, furtul și divulgarea datelor cu caracter personal, atacurile pe site-urile de știri, atacurile de email de tip phishing etc. Creșterea criminalității cibernetice raportate de la începutul pandemiei este de cca 300%. Drept urmare, securitatea cibernetică a devenit foarte importantă pentru toate organizațiile, de toate tipurile și dimensiunile.

Tendințele moderne în analiza, evaluarea și tratarea riscurilor de securitate cibernetică ale unei entități vizează automatizarea proceselor de SecInf pentru eliminarea sarcinilor repetitive și reducerea influenței factorului uman. Deși aparent existența soluțiilor și tehnologiilor de securitate informațională și comunicațională ne face să ne simțim mai siguri, uneori acestea creează percepția

greșită a societății precum că securitatea cibernetică este o problemă pur tehnică-tehnologică, ceea ce duce la o abordare neproductivă a SecInf/SC cu urmări nedorite, precum:

- Lipsa de implicare și angajament a top-managementului în asigurarea SecInf/SC;
- Lipsa de conștientizare de către o mare parte din angajați, îndeosebi cei care și-au schimbat modul de lucru;
- Schimbări neproductive și așteptări nerealiste în domeniul SecInf/SC;
- Decizii și investiții slabe în SecInf/SC, cauzate de *informații publice exagerate, incomplete sau contradictorii, insuficienta atenție asupra eșecurilor reale* etc.

Ca urmare, se impun testări/investigații curente a SecInf și o abordare modernă, productivă a SecInf, cu implicarea managementului de toate nivelurile, conștientizarea pericolelor cibernetice de către toți angajații implicați, inclusiv antrenați în telelucru, dotați cu dispozitive mobile, cu acces la distanță. Top managementul și ofițerii de securitate informațională ar trebui să trateze securitatea cibernetică în contextul strategiei și misiunii afacerii și să o conecteze la rezultatele afaceri. Acest lucru ar însemna recunoașterea semnificației SecInf de către top management, angajarea în a schimba modul în care este tratată SecInf în organizație, a oferi resursele necesare pentru investigarea, analiza, evaluarea și tratarea riscurilor de SecInf, care au impact asupra rezultatelor afacerii precum și a resurselor necesare pentru conștientizarea SecInf de către toți utilizatorii TIC incluși în telelucru și accesarea la distanță a activelor și resurselor informaționale valoroase pentru afacere.

Chiar dacă existența tehnologiilor/soluțiilor de securitate TIC ne face să ne simțim mai siguri, oricum există factori de risc, atât externi cât și interni, care pun în pericol atingerea obiectivelor de afaceri. Acest efect de incertitudine cu privire la un eveniment care, în cazul producerii, ar avea impact și ar putea compromite realizarea obiectivelor strategice este frecvent cunoscut sub noțiunea de risc. Chiar dacă investițiile în SecInf sunt greu de justificat, chiar dacă testarea SecInf pare a fi costisitoare, aceasta este inevitabilă și esențială pentru asigurarea SecInf și a continuității afacerii, îndeosebi dacă afacerea este integral desfășurată în spațiul virtual. Iar **abilitatea de a înțelege riscurile** ne permite să acordăm prioritate resurselor și să întreprindem măsuri de protecție adecvate proporțional cu valoarea acestor resurse. Pentru a minimiza aceste riscuri, organizația trebuie, în primul rând, să conștientizeze SecInf, după care să-și gestioneze adecvat riscurile conform politicilor, criteriilor și procedurilor prestabilite.

Riscul de SecInf este probabilitatea că un anumit eveniment se va realiza și va avea **impact advers asupra confidențialității, integrității** sau **disponibilității** informației aferente proceselor de activitate și/sau a resurselor și/sau a activelor informaționale. Scenariul de bază în gestionarea riscurilor de SecInf este succint examinat în continuare.

2.3.1. Scenariul procesului de analiză, evaluare și gestionare a riscurilor

Activele informaționale din spațiul cibernetic pot aparține unuia dintre două domenii-cheie: personale și corporative. Câteva dintre cele mai răspândite tipuri de active informaționale care influențează SecInf/SC sunt:

- Date, informații;
- Software, cum ar fi programele de calculator, sistemele de operare etc.;
- Fizice, cum ar fi un computer, un dispozitiv mobil de transport de date etc.;
- Un serviciu, precum Internet, TV;
- Angajații, cunoștințele, calificările, abilitățile și experiența lor;
- Activele intangibile ale organizației, precum reputația și imaginea sa.

Un **agent de amenințare** este o persoană sau un grup de persoane, care au un rol în executarea sau susținerea unui atac. După cum a fost menționat mai sus, înțelegerea temeinică a motivelor *(politice, economice etc.)*, a capacităților *(cunoștințe, finanțare etc.)* și a intențiilor *(distracție, criminalitate etc.)* este esențială în evaluarea vulnerabilităților și riscurilor de securitate cibernetică precum și pentru dezvoltarea și implementarea măsurilor de tratament.

Gestiunea adecvată a riscurilor trebuie să fie *personalizată, structurată și cuprinzătoare, bazată pe cele mai bune informații disponibile, integrată, dinamică, îmbunătățită continuu ținând cont inclusiv de peisajul schimbător al riscului, de factorii interni și externi, de factorul uman.*

Gestiunea cu succes a riscurilor de SecInf este importantă pentru:

- Respectarea cerințelor legale și de reglementare aplicabile;
- Îmbunătățirea detectării amenințărilor;
- Creșterea probabilității de atingere a obiectivelor;
- Îmbunătățirea raportării obligatorii și voluntare;
- Minimizarea evenimentelor de daune și/sau pierderi;
- Construirea unei baze solide de încredere pentru luarea deciziilor și planificare;
- Îmbunătățirea prevenirii pierderilor și gestionare a incidentelor.

Pentru a gestiona riscurile cibernetice în cadrul organizației este necesar să înțelegem **contextul intern și extern al organizației**, să identificăm riscurile și amenințările la care organizația este expusă, să le evaluăm și să definim măsurile adecvate de tratament. Obiectivele gestionării cu succes a riscurilor de SecInf constau în **reducerea riscului inerent la un nivel acceptabil al riscului rezidual**, respectarea criteriilor de risc specificate și gestionarea continuă a acestora.

Scopul evaluării riscurilor privind SecInf este de a gestiona continuu riscurile, prin formularea criteriilor de decizie și prin identificarea:

- Activelor critice care pot afecta negativ realizarea obiectivelor organizației;
- Severității vulnerabilităților și amenințărilor externe și interne relevante pentru entitate;
- Controalelor pentru atenuarea riscurilor.

Procesul de gestiune a riscurilor este un proces ciclic, continuu și sistematic *(Fig. 2.13, realizată de autor în traducere din [28]),* cu responsabilități stabilite de identificare, evaluare/măsurare, monitorizare și adoptare de măsuri de control cu două puncte decizionale, fie prin **asumarea expunerii la risc** fie prin **tratamentul suplimentar** pentru a diminua valoarea riscului rezidual până la nivelul acceptabil.

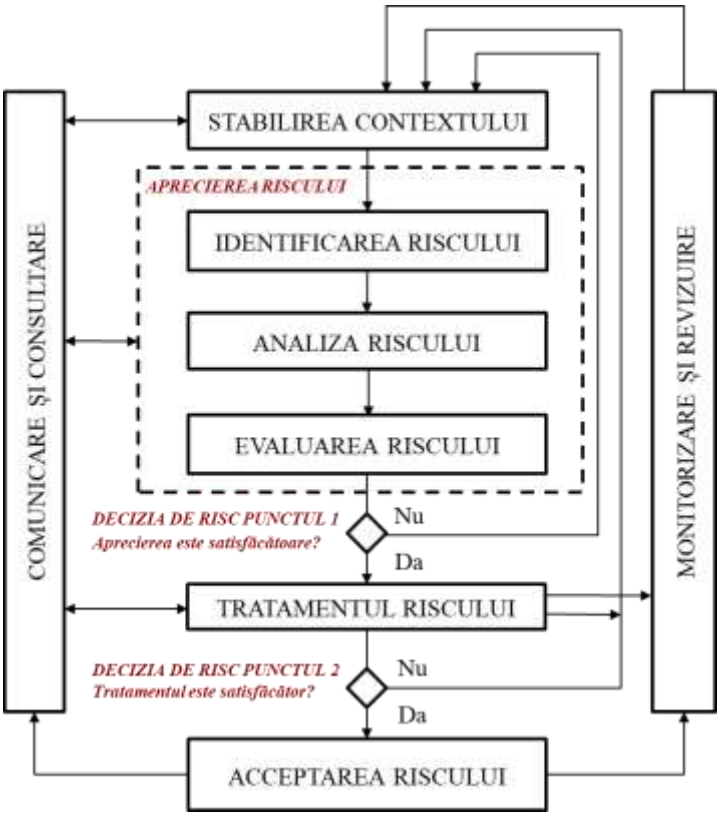


Figura 2.13. Procesul de gestiune a riscurilor

Evaluările riscurilor cibernetice ale unei companii sunt destinate pentru a identifica, estima și prioritiza riscurile operațiunilor organizaționale (de îndeplinire a misiunii, funcțiilor organizației în condiții de păstrare a imaginii și reputației sale) și activelor organizaționale (de exemplu date, informații, calculatoare, rețele și alte dispozitive ale infrastructurii critice), persoane fizice, alte organizații, rezultate din operarea și utilizarea sistemelor informaționale.

Pentru multe organizații evaluarea și gestionarea riscurilor informaționale/cibernetice este o parte crucială a strategiei de afaceri (de exemplu, pentru majoritatea e-afacerilor), pentru altele este o cerință obligatorie de conformitate unor cerințe/reglementări legale, atât de nivel local, cât

și la nivel de industrie și cel global. De exemplu, pentru bănci ce efectuează operațiuni cu carduri bancare sunt recomandate respectarea cerințelor PCI DSS [11]; pentru spitale și organizații medicale – respectarea dispozițiilor HIPAA întru protejarea și menținerea confidențialității informațiilor de sănătate etc.

După cum sugerează *Figura 2.13*, procesul de management al riscului SecInf poate fi repetat pentru activitățile de evaluare a riscului și/sau de tratament al riscului. O abordare repetitivă asigură un echilibru între minimizarea timpului și efortului necesar pentru identificarea controalelor, asigurând în același timp faptul că riscurile majore sunt evaluate în mod potrivit. Fluxul general de analiză și tratare conform ISO 27005:2022 [28] include stabilirea contextului *(Clauza 7*), aprecierea riscului *(Clauza 8),* tratarea riscului *(Clauza 9),* acceptarea riscului *(Clauza 10),* comunicarea riscului *(Clauza 11),* monitorizarea și revizuirea riscului *(Clauza 12).*

Activitățile necesare pentru analiza riscurilor cibernetice prezentate în *Figura 2.13* sunt descrise în detalii și în alte standarde, precum ISO 27001:2022 [11], ISO 31000:2018 [61], NIST SP-1800 [63] etc. și rezumă, în general, la:

1. Identificarea și documentarea vulnerabilităților și surselor de amenințare *(de exemplu, există două mari categorii de vulnerabilități tehnice: erori de configurare și/sau erori de programare; o a treia este factorul uman/slăbiciunea umană);*
2. Identificarea evenimentelor ipotetice ale amenințării *(de exemplu, acces neautorizat, utilizarea frauduloasă a informațiilor de către utilizatorii autorizați, scurgeri de date; expunere accidentală, pierderi de date, blocarea serviciilor etc.);*
3. Identificarea vulnerabilităților și condițiilor favorabile de exploatare *(de exemplu, amenințările împotriva activelor valoroase și/sau a infrastructurii critice digitale și/sau reale etc.)* și determinarea gravității acestora;
4. Determinarea probabilității că astfel de atacuri să aibă succes *(luând în considerare setul de vulnerabilități identificate și condițiile predispuse)*;
5. Identificarea impactului potențial;
6. Determinarea riscului inerent, a măsurilor de tratament și acceptarea riscului rezidual după tratare.

2.3.2. Practici de analiză, evaluare și tratare a riscurilor securității informației

De când a apărut COVID - 19 și majoritatea organizațiilor au trecut la activități online în spațiul cibernetic global, aproape fiecare companie este nevoită să evalueze și să gestioneze eficient riscurile cibernetice. Deoarece astăzi aproape fiecare organizație se bazează pe TIC, Internet, Web, sisteme informaționale și spațiul cibernetic virtual global pentru a-și desfășura

activitatea, există multe riscuri inerente în acest sens. Riscuri, cu care până în era digitală și a pandemiei COVID - 19 multe dintre companii nu s-au confruntat cu adevărat.

După migrarea majorității activităților în online, la distanță, de la domiciliu, când toată lumea este atât de interconectată, **aproape toate organizațiile au devenit o țintă foarte atractivă pentru atacanți**. De exemplu, dacă securitatea doar a unuia dintre conturile personale/de domiciliu ale unui telelucrător este încălcată, infractorii îl pot folosi pentru a încălca securitatea conturilor și datelor personale ale altor persoane, inclusiv a conturilor corporative, ceea ce poate afecta familia, prietenii, colegii și afacerea ca atare [5, 28].

Conform Hacking Statistics 2022 [65] și altor statistici alarmante privind securitatea cibernetică [66], [79] criminalitatea informatică constituie cea mai mare amenințare pentru fiecare companie din lume. Un raport din 2019 a constatat că încălcările de securitate au crescut cu 67% în ultimii cinci ani. La fiecare 39 de secunde are loc un atac cibernetic. Hackerii fură 75 de înregistrări în fiecare secundă. 73% dintre hackeri au declarat că securitatea tradițională firewall și antivirus sunt irelevante sau perimate. Hackerii creează zilnic 300.000 de noi programe malware. În medie, în fiecare zi, sunt piratate cca 30.000 de site-uri web noi. Circa 46% din web-aplicați au vulnerabilități critice. Fiecare două din trei întreprinderi mici și mijlocii sunt atacate sistematic.

Multe din întreprinderile mari își au subdiviziunile și personalul potrivit pentru desfășurarea acestor activități. Iar întreprinderile SMB (mici sau mijlocii), care nu dispun de specialiștii potriviți, adesea recurg la externalizarea evaluării.

Oricare ar fi organizația, aceasta trebuie și se poate călăuzi de ISO/IEC 27001 pentru analiza și evaluarea riscurilor, orientat spre a răspunde multor întrebări. Doar pentru exemplificare, în continuare sunt enumerate clauzele ISO/IEC 27001:2022, unde este abordat riscul:

- Generalități: 0.1, *SMSI asigură conservarea proprietăților fundamentale ale informațiilor/CIA prin aplicarea unui proces de risc management;*
- Clauza 4.1, *Organizația trebuie să determine problemele externe/interne relevante pentru scopul său;*
- Clauza 5, *Top managementul este obligat să promoveze gândirea pe baza de risc; să asigure disponibilitatea resurselor necesare pentru SMSI și că SMSI obține rezultatele prevăzute;*
- Clauza 6.1.1, *Organizația este obligată să determine riscurile și oportunitățile care trebuie abordate pentru a obține rezultatele prevăzute; a preveni sau a reduce efectele nedorite; a obține o îmbunătățire continu;*

- Clauza 6.1.3, *Organizația trebuie să definească și să aplice un proces de tratare a riscurilor de securitate a informației;*
- Clauzele 7 și 10, *riscul este implicit oriunde acolo, unde se menționează „adecvat" sau „potrivit";*
- Clauza 8, *Organizația trebuie să efectueze evaluarea riscurilor de SecInf* (Clauza 8.1); *Organizația trebuie să implementeze planul de tratare a riscurilor* (Clauza 8.2);
- Clauza 9, *Organizația este obligată să monitorizeze, să evalueze, să analizeze eficiența SMSI pentru a aborda riscurile și oportunitățile de îmbunătățire continuă;*
- Clauza 10, *Organizația trebuie să îmbunătățească în mod continuu potrivirea, adecvarea și eficacitatea SMSI, să corecteze, să prevină sau să reducă neconformitățile/efectele nedorite, să îmbunătățească SMSI și să actualizeze riscurile și oportunitățile.*

ISO/IEC 27001 cere să fie definit procesul de evaluare a riscurilor *(Clauza 6.1.2)*, dar nu impune metode concrete de *măsurare-evaluare-tratare* a riscurilor. Organizația ar trebui să selecteze metodele potrivite, aliniate cu metodologia generală de risc organizațional. Totodată, ISO/IEC 27001 face referire la ISO/IEC 27005:2022 ca standard de evaluare și tratare a riscurilor de SecInf, care, la rândul său, se aliniază principiilor și liniilor directoare generice furnizate de ISO 31000:2018 și cere să se țină cont de consecințele și probabilitatea riscului.

După cum deja a fost menționat, **un risc** este o funcție a impactului și a probabilității pentru un eveniment care poate împiedica realizarea obiectivelor și proceselor de afaceri și poate cauza pierderi. Este relativ ușor să evaluezi pierderile în urma unui incident de SecInf, dar este dificil să justifici investițiile în controale înainte de producerea incidentului [5, 28]. O soluție potrivită pentru încadrarea în aria de acceptabilitate a investițiilor de îmbunătățire a SI este analiza de riscuri.

Analiza de risc este un procedeu de identificare și evaluare a factorilor, care pot produce prejudicii activității cu scopul de identificare a controalelor potrivite de atenuare a acestor riscuri inerente pentru a menține impactul în limitele acceptabile (**risc rezidual**). Controalele și acțiunile de atenuare sunt concepute pentru a reduce probabilitatea de apariție a riscului sau a impactului riscului, care deja s-a produs. Cauzele riscurilor pot fi situațiile, condițiile sau evenimentele interne/externe specifice care provoacă apariția riscului. Cauzele sunt tipice, unice și foarte specifice procesului, produsului, serviciului sau activității organizației.

Cercetarea se concentrează pe metode de **analiză calitativ-cantitativă** a riscului securității informației în baza standardelor ISO/IEC 27005 [28] și ISO 31000 [61], având ca țintă lupta cu complexitatea și diminuarea influenței factorului uman prin automatizarea analizei riscurilor în

măsura posibilă. Web aplicația de suport a modelului M^3SI, realizată în cadrul tezei răspunde acestui deziderat.

Înainte de a începe evaluarea riscului, este necesară inventarierea datelor valoroase de care entitatea dispune, infrastructurii care trebuie protejată și altele. Eventual, procesul poate fi demarat cu un audit de date sau al securității informației. Un astfel de audit bine realizat identifică datele stocate de entitate și valoarea acestora.

Clauza 6.*1 ISO/IEC 27001* impune existența unui proces documentat:

a. De evaluare a riscului,
b. De identificare a criteriilor de evaluare a riscurilor,
c. De identificare a „proprietarului riscului” și
d. De documentare a criteriilor de acceptare a riscurilor.

Pentru realizarea acestui proces practicienii pornesc de la clasificarea factorilor de risc *(Fig. 2.14).*

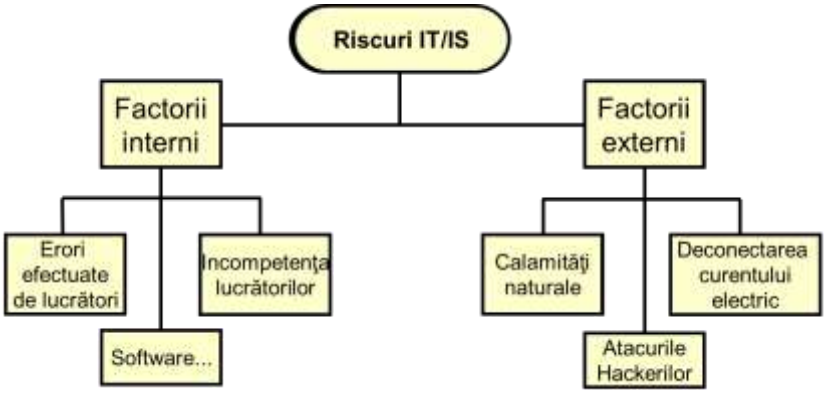


Figura 2.14. Factori de risc și cauzele apariției riscurilor în adresa SecInf [5]

Principalii factorii interni de risc în cadrul organizației includ, dar fă a se limita la:

1. Securitatea fizică și a mediului de lucru – se referă la securitatea fizică a infrastructurii și echipamentelor prin limitarea accesului fizic, inclusiv la servere, centre de date prin utilizarea perimetrelor de securitate, sistemelor de supraveghere, alarme, buna întreținere a dispozitivelor hardware, a suporturilor amovibile etc.

2. Securitatea logică a rețelelor, sistemelor și bazelor de date de accesul neautorizat la informații sensibile, de distrugeri voite sau accidentale prin segmentare, filtrare, sisteme puternice de autentificare, criptare, adoptarea de politici clare de autentificare și autorizare etc.

3. Securitatea personalului prin verificări, procese disciplinare, acorduri, instruiri tematice, inclusiv privind lucru la distanță, BYOD, limitarea cercului de persoane autorizate, revocarea accesului înainte, nu după plecarea unui angajat etc.

4. **Pregătirea/capacitatea TIC pentru continuitatea afacerii** prin elaborarea unor planuri de recuperare în caz de incidente, realizarea sistematică a copiilor de rezervă, păstrarea lor în diferite locuri distanțate etc.

Principalii factorii externi de risc privind SecInf includ, dar fă a se limita la:

1. Cadrul legal și reglementările normative, ce impun cerințe specifice de SecInf caracteristice pentru diferite industrii, e.g. Legea 133 a RM [14], GDPR [15], PCI DSS [20] etc.

2. Obligațiile contractuale cu parteneri de afaceri, furnizori, clienții, consumatori;

3. Prezența entităților în ciberspațiul global puternic interconectat, utilizarea de Cloud computing, servicii terțiare, e.g. Internet provideri, telefonie mobilă, rețele fără fir, conectarea unor dispozitive IoT slab protejate etc.

4. Riscuri și amenințări cibernetice în continuă schimbare etc.

Conform clauzei *6.1.2 ISO/IEC 27001 [11],* organizația ar trebui să stabilească și mențină:

- Criterii de evaluare a riscurilor (de valorificare);
- Criterii de impact (consecințe);
- Criterii de acceptare (tratament) a riscurilor.

Conform clauzei *6.1.2 (b) ISO/IEC 27001,* evaluările de risc trebuie să producă rezultate consistente, valide și comparabile la o evaluare repetată a riscului.

Criteriile de evaluare a riscului se pot baza pe valoarea strategică a proceselor și activelor informaționale ale afacerii; pe criticitatea bunurilor informaționale implicate *(de exemplu, importanța operațională și de afaceri pentru disponibilitate, confidențialitate și integritate);* pe așteptările și percepțiile părților interesate; pe consecințele negative asupra imaginii și reputației entității.

Criteriile de impact/consecință se referă la gradul de daune sau costuri pentru organizație cauzate de un eveniment de securitate a informațiilor, ținând cont de următoarele:

- Nivelul de clasificare a activului informațional afectat;
- Încălcările securității informației *(pierderea confidențialității, integrității, disponibilității);*
- Operațiunile afectate *(interne, externe, terțe),* planurile și/sau termenele afectate;
- Pierderea valorii de afaceri și/sau financiare și/sau daune ale imaginii/reputației.

Criteriile de acceptare a riscului depind de politicile, obiectivele, scopurile și interesele părților interesate ale organizației; de operațiuni, de TI, SI, de finanțe, de factorul uman și de factori sociali. **O entitate definește propriile scări ale nivelurilor de acceptare a riscurilor**, ținând cont de următoarele:

- Criteriile de acceptare a riscului sunt exprimate ca raportul dintre profitul și riscul estimat;
- Pentru diferite clase de riscuri sunt aplicate diferite criterii de acceptare, inclusiv praguri multiple în circumstanțe definite;
- Criteriile de acceptare pot include cerințe pentru tratarea suplimentară în viitor, de exemplu un risc poate fi acceptat dacă există aprobare și angajament pentru a lua măsuri de a-l reduce la un nivel acceptabil într-o perioadă determinată.

Evaluările riscurilor ar trebui să fie efectuate la intervale planificate *(Clauza 8.2 ISO/IEC 27001, [11]*) pentru a aborda modificările cerințelor de securitate **în situația de risc**, de exemplu când probabilitatea sau consecințele riscurilor au fost identificate anterior și, de asemenea, **atunci când apar** sau **sunt planificate modificări semnificative în TI, SI**.

2.3.3. Măsurarea probabilității, impactului și valorii riscului

Riscurile de securitate sunt analizate în funcție de probabilitatea (posibilitatea) apariției riscului și de gravitatea impactului asupra obiectivelor în cazul realizării riscului. Există diverse *metode calitative* și *metode cantitative* de analiză a riscurilor, inclusiv metode automatizate, care se bazează pe profiluri de risc.

Detalii și îndrumări privind selectarea și aplicarea metodelor de evaluare a riscurilor în diverse situații a se vedea *IEC 31010:2019 [64]*. Acest standard, ajuns la ediția a doua în 2019 (*prima ediția a apărut în 2009*), enumeră **41 tehnici de evaluare a riscurilor** *(31 în ediția anterioară).* Metodele utilizate ajută la luarea deciziilor în condiții de incertitudine. Standardul este complet aliniat cu *ISO 31000:2018 [61].*

Evaluarea probabilității producerii unui eveniment poate fi definită, determinată sau măsurată **în mod obiectiv** sau **subiectiv** și poate fi **exprimată calitativ** sau **cantitativ**. Pentru evaluarea riscurilor foarte utile sunt tabelele standardului *ISO/IEC 27005 [28*], precum *Tabelul A.1. Exemplu de scară a consecințelor și Tabelul A.2. Exemplu de scară de probabilitate.* Acestea exemplifică **calificativele impactului** de tipul 5 – Catastrofal, 4 – Critic, 3 – Serios, 2– Semnificativ, 1 – Minor și **calificativele probabilității** de genul: 5 – Aproape sigur; 4 – Foarte probabil; 3 – Probabil; 2–Puțin probabil; 1 – Improbabil. După care ușor se poate calcula valoarea riscului ca produs dintre probabilitate și impact, riscurile se pot aranja în ordinea descrescătoare și/sau pe matricea 5x5 pentru tratarea lor conform strategiilor adoptate.

Adesea, în cadrul modelelor de risc, pentru trecerea de la valori calitative la valori cantitative ale probabilității, impactului, valorii și nivelului de risc sunt utilizate valori semi-cantitative, descrise în *Tabelele 2.2-2.5*, elaborate de autor în baza recomandărilor [28, 61, 64] și

publicate în [5] și ținând cont că ciclul de viață al unor sisteme, dispozitive adesea este mai mic de 10 ani. Toate acestea împreună oferă o baza solidă pentru definirea nivelurilor de maturitate.

Tabelul 2.2. Probabilitatea riscurilor informaționale pentru planificarea strategică

Calificativ/ Valoarea calitativă	Valori semicantitative		Descriere
Improbabil, foarte rar	<1%	0	Mai puțin de o dată la 10 ani*
Puțin probabil, probabilitate scăzută	1-10%	2	La fiecare 5-10 ani
Posibil, Probabilitate medie	10 -50%	5	O dată la 3-5 ani
Probabil, probabilitate mare	50-84%	8	La fiecare 1-2 ani
Aproape sigur, cert	85 100%	10	Mai mult de o dată pe an

Tabelul 2.3. Probabilitatea riscurilor informaționale pentru planificarea anuală

Calificativ/ Valoarea calitativă	Valori semicantitative		Descriere
Improbabil, rar	0-4%	1	Poate apărea doar în cazuri excepționale în următoarele 12 luni
Puțin probabil	5-20%	2	Posibil, dar nu este de așteptat să apară în următoarele 12 luni
Posibil (mediu)	21-79%	3	Posibil ar putea apărea în următoarele 12 luni
Probabil	80-95%	4	Probabil va apărea în următoarele 12 luni
Aproape sigur	90-100%	5	Va apărea aproape inevitabil în următoarele 12 luni

Impactul este rezultatul negativ al unui eveniment, exprimat calitativ sau cantitativ, care afectează obiectivele trasate. Măsurarea consecințelor/impactului la fel este orientată spre forma tabelară *(Tab. 2.4)* de trecere de la valori calitative la valori cantitative, grupate în trei zone de securitate: **riscuri critice –** de nivelul I, **riscuri medii** – de nivelul II și **riscuri minore** – de nivelul III *(a se vedea și Tab. 2.5 și Fig. 2.16).*

Tabelul 2.4. Magnitudinea/valoarea impactului și a riscului pe 3 niveluri

Estimarea calitativă	Zona SecInf/ Valori semicantitative	Descrierea impactului și precizarea valorii
Mare	I, nivel critic /valori 6-8	Exploatarea vulnerabilității (6) poate rezulta în pierderi de mare valoare a bunurilor sau resurselor; (7) poate afecta în mod negativ misiunea, interesul sau reputație companiei; sau (8) poate rezulta în efecte fizice nedorite asupra angajaților (moarte, rănire, incapacitate fizică sau mentală).
Medie	II nivel mediu, /valori 3-5	Exploatarea vulnerabilității (3) poate rezulta în pierderi recuperabile a bunurilor sau resurselor; (4) poate afecta în mod negativ misiunea, interesul sau reputația companiei; sau (5) poate rezulta în efecte fizice nedorite asupra angajaților.
Mică	III, nivel scăzut /valori 1-2	Exploatarea vulnerabilității (1) poate rezulta în pierderi nesemnificative a bunurilor sau resurselor; (2) poate afecta în mică măsură negativ misiunea, interesul sau reputația companiei.

După evaluarea impactului și a probabilității, pentru fiecare activ/amenințare trebuie realizată **măsurarea/aprecierea riscului** prin determinarea unui scor/unei valori a riscului. Valoarea obținută în urma evaluării riscului va fi utilizată pentru a determina dacă este necesar un tratament suplimentar. De regulă, măsura riscului este determinată ca produs dintre probabilitate și impact:

Risc = Probabilitate x Impact

Un exemplu de trecere de la valorile probabilității și a impactului la aprecierea nivelului de risc a se vedea în *Tabelul 2.5*.

Tabelul 2.5 Exemplu de matrice/diagramă de analiză a riscurilor 5x5 („cinci pe cinci”)

Nivel de probabilitate	Nivel de impact/consecință				
	1	**2**	**3**	**4**	**5**
5 (Aproape sigur)	Mediu (2)	Înalt (3)	Foarte înalt (4)	Critic (5)	Critic (5)
4 (Probabil)	Mediu (2)	Înalt (3)	Foarte înalt (4)	Critic (5)	Critic (5)
3 (Posibil)	Scăzut (1)	Mediu (2)	Înalt (3)	Foarte înalt (4)	Foarte înalt (4)
2 (Improbabil)	Scăzut (1)	Scăzut (1)	Mediu (2)	Înalt(3)	Înalt (3)
1 (Rar)	Scăzut (1)	Scăzut (1)	Scăzut (1)	Mediu (2)	Mediu (2)
Nivel de risc	1 (Nesemnificativ)	2 (Minor)	3 (Moderat)	4 (Major)	5 (Catastrofal)

Adesea, un asemenea tabel unic este utilizat în întreaga organizație, ceea ce simplifică activitățile de evaluare a riscului. Pentru alte detalii a se vedea și ISO/IEC 27005:2022 [28]: *Tabelul A.3. Exemplu de abordare calitativă a criteriilor de risc, Tabelul A.4. Exemplu de scară logaritmică de probabilitate, Tabelul A.5. Exemplu de scară logaritmică a consecințelor, Tabelul A.6. Exemplu de scară de evaluare combinată cu matricea de risc tricoloră.*

Etapa finală în procesul de evaluare a riscurilor este **elaborarea unui raport de evaluare** a riscurilor, care să sprijine managementul în luarea deciziilor adecvate privind bugetul, politicile, procedurile de SecInf. Pentru fiecare amenințare, raportul ar trebui să descrie vulnerabilitățile corespunzătoare, activele supuse la risc, impactul, probabilitatea apariției și recomandările de control.

2.3.4. Tratarea riscurilor

După încheierea evaluării și aprecierii riscului, valoarea riscului este comparată cu criteriile convenite de acceptare a riscului și este realizată tratarea riscului. Dacă aprecierea riscului este mai mare decât nivelul acceptabil al opțiunilor de tratament, atunci riscul trebuie tratat, rezumând un risc rezidual *(Fig. 2.15, [5])*. Decizia de tratare se ia în conformitate cu matricea de analiză a riscului *(Fig. 2.16, [5])*. Proprietarul riscului trebuie să aprobe tratamentele de risc selectate și trebuie să accepte riscul rezidual conform criteriilor prestabilite. Acest lucru trebuie documentat.

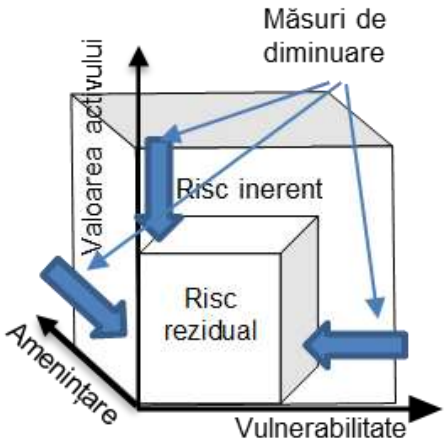


Figura 2.15. Risc rezidual vs risc inerent

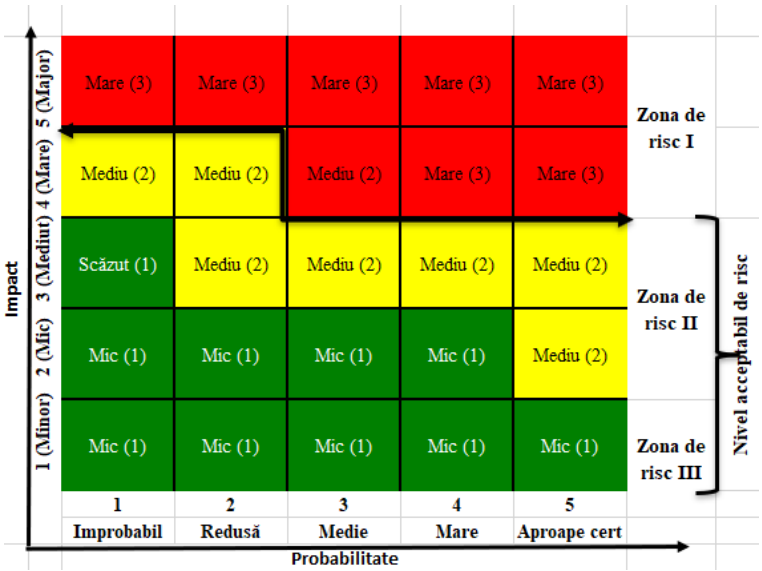


Figura 2.16. Matricea 5x5 de apreciere a riscurilor pe 3 niveluri

În digrama din *Figura 2.16* zona din partea de dreapta-sus (colorată cu roșu) sunt riscuri cu probabilitate mare și impact mare, pentru care trebuie aplicate controale de diminuare a valorii riscului, iar în stânga-jos (colorată cu verde) – cu probabilitate mică și impact mic, care pot fi

ignorate (nu afectează grav afacerea). Zona de mijloc (colorată cu galben) sunt riscuri cu probabilitate medie și impact mediu, care pot fi tratate conform criteriilor politicii de securitate.

Există patru strategii alternative pentru tratarea riscurilor, realizată în baza criteriilor ce determină când riscurile pot fi acceptate și când nu:

1. **Reducerea/atenuarea riscului** prin aplicarea unor controale suplimentare adecvate;
2. **Acceptarea riscului** în cunoștință de cauză și în mod obiectiv, cu condiția ca acesta satisface în mod clar politica organizației de gestionare a riscurilor privind nivelurile definite pentru a accepta riscuri (conform criteriilor de acceptare a riscurilor);
3. **Evitarea riscului** fie prin încetarea, fie prin evitarea activității care creează riscul;
4. **Transferul riscurilor** asociate de afaceri către alte părți, de exemplu, asigurătorii.

Opțiunile de tratament a riscurilor trebuie să fie selectate în baza rezultatului evaluării riscurilor, a costului preconizat pentru implementarea acestor opțiuni și a beneficiilor preconizate din aceste opțiuni. Ar trebui implementate opțiunile care pot obține reduceri mari de riscuri cu cheltuieli relativ mici. Alte opțiuni pentru îmbunătățiri pot fi neraționale și, în asemenea cazuri, trebuie efectuată o analiză de fezabilitate pentru a justifica cheltuielile.

Procesul de tratare a riscurilor rezumă în aplicarea măsurilor de control pentru riscurile care se află peste nivelul acceptat, aducându-le la nivelul acceptabil. Ca și tipuri de măsuri de control sunt măsurile *preventive, detective, corective* și *compensatorii*.

- Măsurile preventive au ca scop de a preveni materializarea riscurilor.
- Măsurile detective au ca scop identificarea evenimentului de securitate în timpul desfășurării sau după ce acesta a avut loc.
- Măsurile corective limitează impactul ca urmare a materializării riscului.
- Măsurile compensatorii sunt aplicate atunci când celelalte tipuri de măsuri nu sunt posibile de aplicat din diverse motive.

Dacă acțiunile corective permit ca vulnerabilitățile să fie descoperite și evaluate, măsurile preventive previzionează și anticipează exploatarea vulnerabilităților cu acțiuni prioritare, întreprinse pentru a schimba securitatea organizației și poziția de risc.

Controalele de remediere și cele compensatorii permit entității să reducă suprafața atacului vulnerabilității, determinând organizațiile să implementeze procese de excepție pentru a scuti anumite active sau aplicații de raportarea continuă a unei vulnerabilității care nu poate fi remediată. De regulă, excepțiile apar în rapoarte, iar utilizarea excepțiilor trebuie înregistrată și auditată.

Toate riscurile identificare sunt raportate către conducere, cu evidențierea celor care sunt peste nivelul acceptabil. Raportarea se poate face pe *domenii, procese, resurse* într-o *hartă generalizatoare a riscurilor (Figura 2.17).*

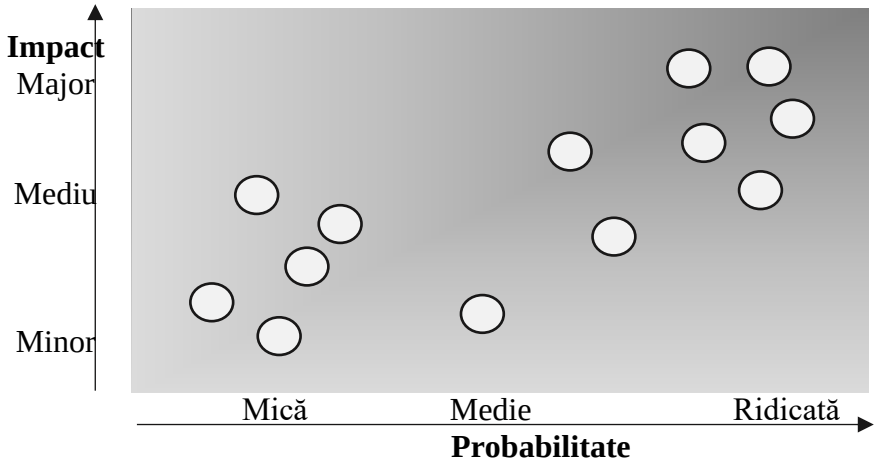


Figura 2.17. Exemplu de hartă generalizatoare a riscurilor

O vulnerabilitate este o slăbiciune a unui activ sau a unui control, care poate fi exploatată de o amenințare; un defect, o slăbiciune a proiectării sau a implementării unui sistem informațional sau a mediului său, care ar putea fi exploatate intenționat sau neintenționat și care ar putea afecta în mod negativ o organizație.

Problema cea mare e că numărul vulnerabilităților este în creștere continuă, și aproape că se dublează la fiecare doi ani. Ca urmare, **descoperirea manuală** a vulnerabilităților în funcție de serviciile oferite *(e.g. cercetarea acestora conform surselor http://www.kb.cert.org/vuls/, http://nvd.nist.gov/ etc.)* apare ca o sarcină destul de voluminoasă, deoarece necesită multă experiență și mult timp, adesea rezultatul fiind **fals negativ**. Iar **descoperirea automată** realizată prin scannere de vulnerabilități cunoscute *(e.g. Nessus, OpenVAS, QualisGuard, GFI LANGuard, Retina, Nikto, w3af, Paros, BurpSuite, WebScarab, DirBuster etc.)* adesea oferă un rezultat **fals pozitiv**.

Soluția potrivită ar fi prioritizarea tratării vulnerabilităților, dat fiind faptul că doar o mică parte din ele, de circa 2-3% sunt cel mai frecvent exploatate.

Ca urmare, o practică obișnuită a multor organizații este să se concentreze asupra evaluării vulnerabilităților și expunerilor comune *(CVE, de la the Common Vulnerability Enumeration),* care sunt *critice* și *ridicate*. Acest lucru are sens, deoarece există relativ puține vulnerabilități critice și ridicate, și anume acestea ar trebuie abordate mai întâi. Cu toate acestea, dacă organizațiile se concentrează doar asupra vulnerabilităților critice și ridicate, rămân deschise atacatorilor vulnerabilitățile medii și scăzute, care pot fi exploatate în mod repetat.

O altă problemă este că dacă o companie este vulnerabilă la atacuri și fiecare angajat este vulnerabil. Totodată, angajații nu totdeauna raportează incidentele de SecInf. Conform raportului Webroot Inc. [67]:

- 35% dintre lucrătorii atacați nu se grăbesc să-și schimbe parolele după incident;

- 49% de angajați recunosc că fac clic pe linkuri din mesajele de la expeditori necunoscuți în timpul muncii;
- 67% dintre lucrători au primit cel puțin un e-mail de phishing la locul de muncă;
- 40% dintre cei care au primit un e-mail de phishing nu l-au raportat.

Adesea evaluarea riscurilor [5, 28] și rezultatul gestiunii riscurilor de securitate sunt integrate în modele de maturitate a securității informației, SecInf, SMSI [6, 7].

După ce riscul a fost tratat, probabilitatea, consecința și valoarea riscului rezidual trebuie reevaluate/calculate din nou. La încheierea procesului de selectare a controlului, obiectivele și controalele selectate trebuie comparate cu obiectivele de control și controalele din *Anexa A [ISO 27001:2022]* pentru a se asigura că nu au fost omise controale necesare.

2.4. Concluzii

Gestiunea riscurilor de SecInf este un proces continuu, care ar trebui să permită organizației să-și atingă obiectivele de afaceri stabilite. Deși este un proces destul de complicat, reușita lui duce la creșterea nivelului de maturitate atât a SC/SecInf, cât și a organizației în întregime.

Securitatea informației implementată corect în condițiile migrării afacerilor în spațiul cibernetic, a telelucrului în masă și a accesului de la distanță a informațiilor sensibile presupune o noua abordare, orientată nu doar pe soluții tehnice-tehnologice, pe TIC și pe sisteme informaționale tradiționale, dar și pe securitatea dispozitivelor mobile, de domiciliu cât și pe securitatea IoT, IoB, cloud etc., inclusiv pe schimbarea paradigmei abordării SecInf, de la abordarea preponderent tehnică-tehnologică pe abordarea organizațională în cadrul sistemelor de management, care ar permite controlul și monitorizarea eficientă a riscurilor cibernetice.

Automatizarea operațiilor rutinare privind inventarierea activelor, amenințărilor și riscurilor cibernetice, evidenței dispozitivelor mobile și/sau de domiciliu, cu acces de la distanță, a resurselor informaționale critice, valoroase pentru afacere, măsurarea nivelului de maturitate a SecInf etc. pot spori esențial nivelul SecInf printr-o postură de securitate mai puternică și o productivitate operațională mai mare. Majoritatea informațiilor ar trebui extrase din soluțiile tehnice/tehnologice, jurnalele etc. Dar volumul, importanța acestora în/pentru adoptarea deciziilor de SecInf este de cca 20%, pe când problemele organizaționale, de personal, conștientizare etc. prevalează, ajungând până la 80%.

Multe dintre diversele cadre analizate de abordare a SecInf prin prisma unui SMSI pot fi recomandate ca bază pentru lansarea SMSI, e.g. NIST SP 800.x, COBIT, ISO/IEC 27001:2022. Dar cel mai recomandat rămâne a fi ISO/IEC 27001:2022. Printre argumentele forte de implementare a unui SMSI bazat pe ISO/IEC 27001 sunt de menționat:

- Adoptarea SMSI în cadrul organizației oferă un mediu unic în care sunt îndeplinite toate cerințele de securitate a informației. Totodată, SMSI conform ISO27k **conține toate mecanismele necesare** pentru autocorectare și îmbunătățire.
- Standardele pereche ISO/IEC 27001↔ISO/IEC 27002 **formează baza universală a controalelor necesare** pentru înțelegerea și gestionarea adecvată și eficientă a riscurilor, activelor, resurselor informaționale valoroase pentru entități, indiferent de apartenență la sectorul privat, public sau personal, indiferent de mărime, localizare etc.
- **Standardele ISO27k sunt de circulație internațională** și specifică cerințe flexibile pentru implementarea, operarea, revizuirea, menținerea și îmbunătățirea continuă a SMSI.
- Familia de standarde **ISO27k conține și multe alte standarde complementare** *(la moment cca 80 de standarde operaționale)*, **care acoperă tot spectrul de activități, ghiduri și linii directoare** privind implementarea, operarea, revizuirea, auditarea, menținerea și îmbunătățirea continuă a securității informației, inclusiv pentru domenii specifice, cum ar fi telecomunicații, sectorul bancar, sectorul energetic etc.

În funcție de țară, tradiții, preferințe, industrii, contexte specifice etc. sunt utilizate și alte cadre de reglementare, inclusiv naționale. De exemplu, seria de publicații speciale NIST SP 800 *(National Institute of Standards and Technology, http://nist.gov/, S.U.A.)* este pe larg utilizată în toată lumea. Toate publicațiile NIST pot fi găsite la adresa *http://csrc.nist.gov/publications/*. PCI DSS este utilizat în toată lumea pentru industria de plăți cu carduri, fiind adaptat contextului riscurilor comerciale, de mediu, tehnice și de reglementare specifice organizației, ramurii industriale și/sau specificului național. Totodată, aceste standarde nu contravin standardelor ISO27k sau altor bune practici internaționale privind organizarea și monitorizarea SMSI, dar le pot preciza pentru a spori nivelul de securitate a informației pentru anumite regiuni, industrii etc.

Produsele gen CIS Controls v.8, CIS Controls Self-Assessment Tool (CIS CSAT, 2022), Cybersecurity Maturity Model Certification v.1.02 (CMMC 1.2, 2020) și altele pot simplifica esențial abordarea inițială rapidă a securității cibernetice. Dar pentru certificarea SMSI oricum SecInf trebuie abordată conform ISO/IEC 27001:2022.

What gets measured, gets done.
What gets measured, gets improved.
What gets measured, gets managed.
(Peter Drucker)

3. MODEL MULTIPROFIL DE MATURITATE A SECURITĂȚII INFORMAȚIEI M³SI

Abordarea modernă a SecInf în baza modelelor de maturitate multinivel cu suport informatic privind generarea profilurilor tipice unor industrii PSITI și a profilurilor individuale PISI particularizate/concretizate, precum și evaluarea automatizară în acord cu politicile corporative concrete și valorile țintă ale criteriilor de evaluare a maturității SecInf constituie partea inovativă și originală a tezei. Domeniile de control și controalele sunt în baza standardelor deschise și standardelor directoare ale familiei ISO27k.

Parafrazându-l pe ilustrul P. Drucker [93] *ceea ce nu poți măsura, nu poți gestiona; ceea ce nu poți gestiona, nu poți îmbunătăți*. Abordarea SecInf bazată pe risc și evaluarea riscului de SecInf examinate mai sus constituie doar începutul. Pentru gestionarea eficientă a SecInf în cadrul SMSI este necesar a compara progresul în timp, a cuantifica, a comunica maturitatea pe baza standardelor acceptate la nivel global și național pentru a decide și a prioritiza investițiile și măsurile de SecInf.

Fiecare organizație are o limită superioară a vitezei cu care poate remedia vulnerabilitățile și aplana sau echilibra riscurile de SecInf în conformitate cu politicile stabilite. Acest lucru este în funcție de trei atribute cheie:

- Apetitul afacerii pentru riscul operațional;
- Capacitatea de a absorbi întreruperile legate de remediere;
- Eficiență în remedierea infrastructurii programo-tehnice-tehnologice vulnerabile.

De regulă, politicile corporative de SecInf specifică, în particular, regulile operaționale referitoare la intervalele de timp pentru remedierea vulnerabilităților și riscurilor în funcție de nivelul și/sau impactul lor și conform maturității proceselor. Entitățile ar trebui să aibă implementate numeroase procese de scanare, detectare și remediere a vulnerabilităților și riscurilor pentru multe și/sau toate sistemele operaționale corporative bazate pe TIC; de evidență a activelor informaționale și drepturilor de acces; de analiză și evaluare a riscurilor; de gestionare a riscurilor, incidentelor de SecInf; de asigurare a continuității afacerii; de măsurare a eficienței resurselor implicate, a performanței SMSI și îmbunătățirii sale continue etc. Toate acestea impun nu doar

măsurări, ci și comparări în timp ale stării SecInf, inclusiv cu alte entități din același domeniu de activitate și, în ultimă instanță au condus la abordarea SecInf prin modele de maturitate, având ca suport instrumente software, care să automatizeze operațiile rutinare și să permită urmărirea evoluției în timp.

3.1. Securitatea informației bazată pe modele de maturitate

ISO/IEC 27001:2022 [11], O-ISM3 [8, 39], Top 20 CIS Controls [31], CMMC [32], C2M2 [74] și altele pot fi privite sub unghiul de vedere a unor **modele de referință a proceselor de planificare, implementare, operaționalizare, monitorizare, măsurare, evaluare a performanței și îmbunătățirii** continue a SecInf**.** Înscrierea și adaptarea, integrarea acestora în M^3SI permite gestionarea securității informației în baza nivelurilor de maturitate, ținând cont de specificul entităților și de tendințele actuale și de bunele practici în domeniul sistemelor de management a securității informației.

3.1.1. Modele de maturitate existente și necesitatea unui model multiprofil

Maturitatea este o măsurare a capacității unei organizații de îmbunătățire continuă a unor domenii de management. Iar **modelele de maturitate** reprezintă colecții de bune practici pentru măsurarea progresării entității de la niveluri inferioare spre niveluri mai înalte de aptitudine sau de „maturitate”. **Nivelul de maturitate** reprezintă o etapă clar definită pe „scara” evoluției organizației spre maturizarea proceselor, evaluată pe bază unor seturi specifice de metrici. Modelele de maturitate sunt utilizate **pentru a îmbunătăți treptat** diferite procese ale entității *(pentru detalii a s vedea 2.1.4.2).*

De exemplu, Modelul de Maturitate a Capacității CMM [68] este orientat pe procese și abordarea procesuală PDCA (Plan-Do- Check-Act). La fel și modelul de maturitate al calității promovat de ISO 9000:2015 [41] și modelul de maturitate a securității informației promovat de ISO/IEC 27001 [11] și alte MM pentru SM se bazează pe abordarea procesuală și pe metrici specifice.

În esență, modelele de maturitate reprezintă **seturi de bune practici globale verificate**, care permit organizațiilor să construiască și să facă referință la capabilitățile-cheie, care abordează cele mai comune provocări ale afacerii lor. Deși marea majoritate a modelelor de maturitate existente, e.g. O-ISM3 [8, 39], COBIT [35], ITIL [59], ISO 9001:2015 etc. în general sunt compatibile cu cerințele ISO/IEC 27001, nu există o înțelegere clară a relaționării domeniilor și proceselor de bază folosite de către acestea. Spre deosebire de diferitele cadre de SecInf oferite de bunele practici/standarde internaționale și modelele de maturitate izolate, modelul multiprofil al

maturității securității informației M^3SI oferă **o imagine universală unică și integră asupra SecInf**, aplicabilă pentru orice entitate, la orice nivel, pornind de la cadrul global/național de reglementare și bune practici, continuând cu cerințele specifice pentru diverse industrii PSITI și terminând cu nivelul de aplicare local conform profilurilor individuale PISI, specifice cerințelor și contextelor particulare concrete al unei organizații și/sau a unei subdiviziuni a acesteia și/sau a unei misiuni.

Totodată, modelul de maturitate al unei entități concrete ar trebui să țină cont de un set foarte specific de metrici pentru a fi relevant necesităților organizației. Și mai mult chiar, maturitatea ar trebui măsurată și reflectată nu doar în cele 5 niveluri. Ar trebui luate în considerare, cel puțin, **trei dimensiuni ale modelului**:

- Cum modelul include cele mai bune practici și care este relația acestora cu cele patru etape de îmbunătățire a procesului: standardizare, îmbunătățire, control și desăvârșire;
- Cât de eficient sunt utilizate practicile în SecInf, SC, SMSI și îmbunătățirea lor continuă în cadrul entității;
- Care sunt capacitățile de măsurare-raportare-afișare a maturității conform primelor două dimensiuni.

În cadrul modelului multiprofil M^3SI a fost realizată și această idee **inovativă de multidimensionalitate**: modelul este adaptabil și extensibil, practicile pot fi continuu îmbunătățite și evaluarea realizată multiplu conform unor profiluri în acord cu nevoile individuale ale entității, orientate spre anumite componente, domenii ale SMSI și/sau misiuni de evaluare.

Iar **multinivel** se referă atât la ierarhia modelelor cât și a profilurilor, e.g. **model generic-model tipic industriei-model individual** și **profil generic-profil industrial-profil individual**. Profilul PISI este dezvoltat conform necesităților specifice ale entității, așa cum îl vede entitatea, cu indicatorii și metricile de care are nevoie, inclusiv modurile de afișare/comparare care să reflecte scopul urmărit. PISI sunt generate în baza profilurilor de securitate a informației tipice unor industrii/PSITI, care, la rândul lor sunt generate în baza modelului de maturitate generic, cu o bază generică comună de cunoștințe privind cele mi bune practici/controale de SecInf.

În linii mari, PISI ca model de maturitate al SecInf, SC, SMSI etc. este menit să simplifice complexitatea proceselor reale de creștere succesivă/îmbunătățire continuă a securității informației printr-un număr de faze/etape succesive, **fiecare marcată de caracteristici unice**, specifice nivelului de maturitate. Modelele și profilurile de maturitate au ca scop **stabilirea unei valori standardizate cu care să se poată determina starea SecInf și care să permită planificarea modului de atingere a țintelor de securitate dorite**. Tradițional, numărul nivelurilor de maturitate este de la 1/inițial (neconformitate) la nivelul superior 5/optimizat

(conformitate deplină) – o stare „ideală” în care procesele ar fi gestionate sistematic prin optimizarea și îmbunătățirea lor continuă.

Tocmai acesta și este soluția propusă de creștere a nivelului de maturitate prin aplicarea unui model multiprofil, multidimensional și multinivel de maturitate a securității informației M^3SI, ca sistem simplu și transparent, orientat spre generarea Profilurilor/Modelelor de Securitate a Informației subordonate la nivel de industrie PSITI și la nivel de entitate PISI. M^3SI are la bază cele mai bune practici de securitate a informației/cadre normative de reglementare cunoscute în acest moment, *e.g. O-ISM3:2017 [8], NIST SP 800-53 rev.5 (2020) [44], NIST 800-207 Zero Trust Architecture (2020) [45], standardele împerecheate ISO/IEC 27001:2022[11] și ISO/IEC 27002:2022 [19], PCI-DSS v4.x (2023) [20], COBIT:2019, ISO/IEC 20000-1:2018 [60], ITIL v4:2019 etc.*

Dacă implementarea unui nou SI în organizație poate fi relativ ușor justificată prin veniturile considerate, implementarea unui SIEM, care ar asigura SecInf/SC, adesea poate fi refuzat ca fiind greu de justificat. De aceea, **abordarea SecInf se impune la toate fazele de dezvoltare și implementare a proiectelor TI, SI**. Diverse standarde în domeniul SecInf propun diferite îmbunătățiri, care prescriu cum ar trebui implementată securitatea informației în organizație. Dar, alinierea la aceste standarde cu caracter general deseori este dificilă și greu de aplicat în practică. Dacă alinierea la cerințele legale privind operarea datelor cu caracter personal *(de exemplu Legea RM 133 sau GDPR la nivelul UE)* este aproape obligatorie pentru orice organizație, alte cerințe nu sunt evidente pentru creșterea nivelului de securitate al informației în organizație. Modelul propus de maturitate a securității informației este conceput ca **instrument de evaluare al capacității organizației de a îndeplini obiectivele securității** la un nivel optim în raport cu costurile aferente.

Esența modelului de maturitate este exprimată prin capacitatea organizației de a măsura îmbunătățirea continuă a unui proces, produs, serviciu. Or, MM, M^3SI sunt **modele de îmbunătățire organizațională**, care se bazează pe observația că **organizațiile implicate în eforturi complexe trec prin diferite niveluri de eficiență** la diferite **etape ale ciclului de viață**. Pe măsură ce organizațiile devin mai puternice în aceste eforturi și dezvoltă sisteme eficiente de susținere a activităților ele devin mai „mature” în demersul lor.

Obiectivul principal al M^3SI este de a facilita înțelegerea managementului privind nivelul SecInf în organizație. M^3SI elaborat include **corelarea cadrelor de abordare** deja menționate, precum suita **ISO27k,** seria **NIST SP 800-53 Rev.4, PCI DSS** pentru definirea domeniilor SecInf cu respectivele obiective și controale specifice, ajustate la piața Republicii Moldova și la specificul activității bancare.

Într-o oarecare măsură M^{3}SI a anticipat modificarea ISO/IEC 27001 și ISO/IEC 27002, ediția III din 2022, în care au fost schimbate numele standardelor. De exemplu, denumirea veche „*ISO/IEC 27001:2013 Tehnologia Informației – Tehnici de securitate – Sisteme de management a Securității Informației*." a devenit „*ISO/IEC 27001:2022 Securitatea informațiilor**, securitatea cibernetică și protecția vieții private** – Sisteme de management al Securității informațiilor*. Acest fapt subliniază abordarea unică a celor trei tipuri de securitate, menționate în titlul standardului și impune maparea diferitelor controale de securitate cu diferite cerințe și standarde, apropierea mai mare a celor trei concepte de securitate din titlul standardului.

Partea principală a ISO/IEC 27001:2022 *(clauzele de la 4 la 10)* au fost schimbate foarte puțin, doar la nivelul unor cuvinte izolate. Și modificările controalelor de securitate din *Anexa A* sunt relativ moderate față de versiunea din 2013. Astfel, numărul total de controale a scăzut de la 114 la 93, au apărut 11 controale noi, 35 au rămas aceleași, 23 au fost doar redenumite, 57 controale au fost comasate și un control a fost eliminat. Schimbarea majoră se referă la regruparea controalelor, care în ediția din 2022 sunt plasate în 4 secțiuni, în locul celor 14 din versiunea anterioară din 2013. ISO/IEC 27001 este cel mai important și principal standard din seria ISO/IEC 27001 cu peste 80 de standarde deja operaționale. Acest standard este universal, aplicabil oriunde în lume și pentru orice tipuri de organizații, stă la baza certificării SMSI, este un standard sistemic și central – toate celelalte sunt concepute în jurul lui, având roluri ajutătoare specifice unor domenii, controale etc. Și **modelul M^{3}SI corespunde acestui standard actualizat în 2022**.

M^{3}SI este preconizat să ofere o flexibilitate înaltă, astfel încât să permită adăugarea, eliminarea, modificarea de noi cunoștințe structurate privind amenințările și riscurile existente, controalele și metricile preconizate pentru evaluarea nivelului de maturitate a SecInf. M^{3}SI este **însoțit de o aplicație instrumentală software**, care permite generarea profilurilor de securitate a informației:

- **Tipice unor industrii/PSITI**, e.g. educație, bănci, medicină;
- **Particularizate** conform necesităților de securitate individuală a informației/PISI **la nivel de entitate concretă**, e.g. colegiu, universitate, bancă comercială, clinică de stat sau clinică privată etc.;
- **Particularizate la nivel de zone/sfere separate sau de subdiviziuni a unei entități**, e.g. SecInf a departamentului de plăți electronice al băncii comerciale sau zona de securitate a sistemelor informatice cu cerințe specifice contextului intern/ extern;
- Cu **valori țintă** ale criteriilor de evaluare și metrici specifice de măsurare a criteriilor.

3.1.2. Conceptul modelului de maturitate multiprofil M^{3}SI

M^{3}SI înglobează setul de cunoștințe și bune practici privind cadrele de organizare, monitorizare, control și îmbunătățire continuă a SMSI și SecInf a unei entități; permite evaluarea și compararea evaluărilor SecInf a unei entități în timp, urmărind creșterea nivelului de maturitate, precum și compararea nivelurilor de maturitate a diferitelor entități tipice în cadrul unei industrii.

Avantajul abordării SecInf în baza modelului de maturitate este faptul ca acesta pune la dispoziție **un mod de lucru strict cu reguli clare și transparente** de monitorizare a fiecărui proces cu ajutorul indicatorilor de performanță/țintelor prestabilite. Ca urmare, fiecare proces poate fi îmbunătățit în mod controlabil, trecând de la o etapă la alta (de la un nivel de maturitate la altul) pentru a oferi rezultate și mai bune. Principalul dezavantaj este un timp destul de mare necesar pentru analiza și documentarea stării inițiale, cât și pentru menținerea proceselor. În continuare sunt descrise procesele și pașii necesari pentru realizarea de îmbunătățiri continue a SecInf în cadrul unei organizații concrete în baza M^{3}SI, PSITI și a profilurilor derivate PISI *(Fig. 3.1, [6])*.

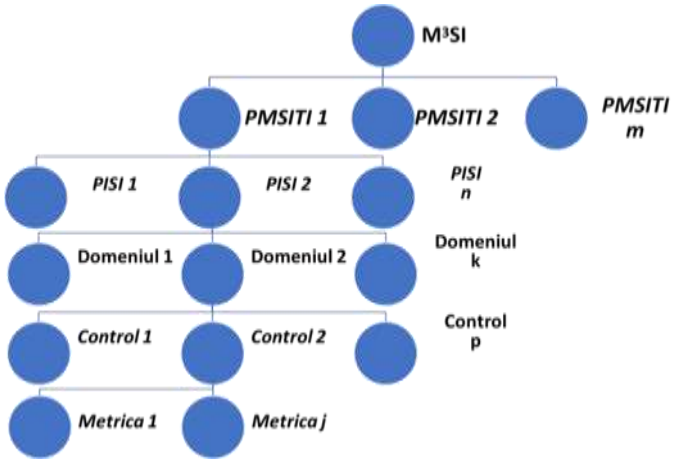


Figura 3.1. O viziune ierarhică simplificată a modelelor de maturitate în M^{3}SI

Potențialul M^{3}SI permite utilizarea sa în diferite scopuri conform ciclului PDCA *(Fig. 3.2)*.

În primul rând, M^{3}SI permite organizației să-și realizeze relativ ușor **autoevaluarea capacităților** de SecInf în mod sistematic, pentru a-și comunica convingător nivelurile de capacitate și pentru a permite prioritizarea investițiilor în securitate. În rezultatul autoevaluării organizațiile identifică lacunele/decalajele între valorile reale și valorile țintă a capacităților sale, realizează prioritizarea și elaborează planuri și proiecte pentru a elimina decalajele. Autoevaluarea poate fi repetată periodic conform cerințelor ISO/IEC 27001 și politicilor interne și/sau ca urmare a schimbării mediului și/sau a obiectivelor de afaceri, a riscurilor, a amenințărilor etc.

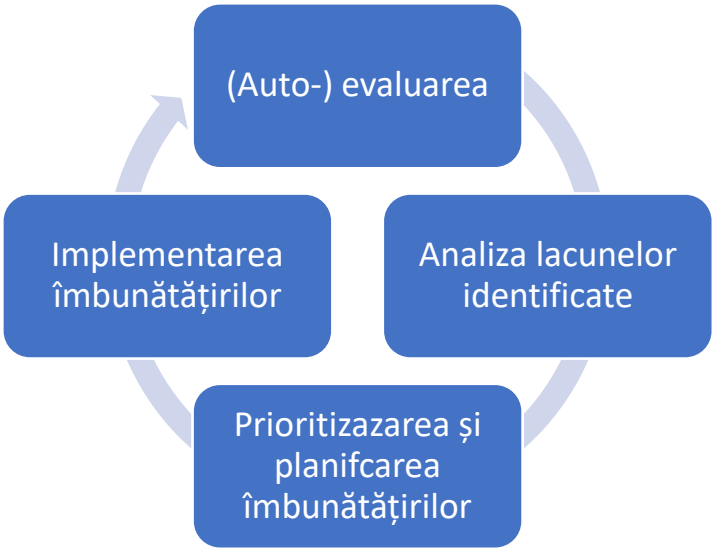


Figura 3.2. Potențialul utilizării modelului M[3]SI pentru îmbunătățire continuă

Totodată, aplicația **permite evaluarea de către controlori auditori** în baza acelorași profiluri. Răspunsurile la chestionarul generat PISI sunt alese dintr-o scară prestabilită cu 5 cinci valori, conform nivelurilor de maturitate, în funcție de cum este implementată măsura de SecInf:

1. **Inițial** (Ad-hoc/nonconformitate) controlul/practica/măsura este neimplementată, se atestă lipsa totală a acesteia;
2. **Repetabil** (Definit/conformitate inițială) – implementat parțial/incomplet, oportunitățile de îmbunătățire prevalează/sunt mult mai multe decât cele implementate;
3. **Definit** (Standardizat/conformitate de bază) – implementat incomplet, oportunitățile de îmbunătățire sunt mult mai puține decât cele implementate;
4. **Gestionat** (Optimizat/conformitate acceptabilă) – Implementat complet, dar cu careva devieri sau oportunități de îmbunătățire;
5. **Optimizat** (Conformitate *deplină)* – Implementat integral, complet, fără careva devieri sau oportunități de îmbunătățire.

După răspunsul la chestionar, aplicația calculează raportul privind punctajul acumulat, care arată lacunele în performanța SecInf. O primă analiză vizuală a diagramei-radar generate permite determinarea semnificației, importanței problemelor de soluționat. De regulă, nu este oportun, adesea nici posibil ca entitatea să atingă cel mai înalt nivel de maturitate în toate domeniile de-o dată. Entitatea ar trebui să-și identifice profilul de capacitate/nivelul de performanță dorit – **o țintă pentru fiecare domeniu sau control**, care îi permite cel mai bine să-și atingă obiectivele de afaceri conform misiunii, politicii și strategiei de SecInf. Colecția de **capabilități dorite este stabilită de PISTI, iar valorile țintă în PISI** și împreună constituie linia către care tinde entitatea**.**

După finalizarea analizei decalajului entitatea ar trebui să prioritizeze acțiunile necesare pentru implementarea completă a controalelor care permit atingerea capacității țintite în domeniile afectate de lacune. Criteriile de prioritizare trebuie stabilite în funcție de faptul cum afectează obiectivele organizației acele decalaje, costul implementării și disponibilitatea resurselor necesare pentru implementare. La stabilirea priorităților este utilă o analiză cost-beneficiu pentru lacune și activități de planificare **conform regulii Pareto** sau a curbelor pe **diagrama de echilibrare cost - securitate** a măsurilor de SecInf *(a se vedea cap. 2, Fig. 2.6)*.

După prioritizare trebuie elaborat un **plan de diminuare a decalajului** dinte valorile evaluate și valorile - țintă pentru lacunele selectate. Planificarea ar trebui să se alinieze la obiectivele strategice ale organizației, planurilor SMSI și de securitate cibernetică. Unele planuri se pot întinde săptămâni, altele luni sau ani, în funcție de amploarea îmbunătățirilor necesare pentru a elimina neconformitățile și decalajele selectate și a atinge capacitatea dorită.

În pasul 4 se realizează implementarea planurilor, după care se trece din nou la primul pas de **re-evaluare periodică** în ciclul de îmbunătățire continuă.

Pentru ca securitatea informației să aibă succes, este vital ca toți actorii implicați să împărtășească la fel înțelegerea exactă a riscurilor, a capacităților și priorităților cibernetice ale companiei, inclusiv organele externe de supraveghere și control, de certificare și acreditare etc. O asemenea viziune unificată M^3SI asupra SecInf din partea părților - cheie este primordială pentru o entitate. Viziunea M^3SI acoperă întreaga organizație, de la consiliul de administrație spre executiv, ofițer de securitate a informației, specialiști în securitate TI, SI, manageri de risc, până la toți angajații care utilizează TI, SI în activitățile lor și controlorii din partea organelor de supraveghere sau auditare. Necesitatea realizării acesteia devine din ce în ce mai mare pe măsură ce organizațiile migrează spre munca online, la distanță/telelucru, mediat de Internet și TIC moderne. Evident, fiecare actor va utiliza aceste informații în moduri diferite, în funcție de rolul său, cu concentrarea atenției pe obligațiile sale pentru reducerea celor mai mari riscuri și creșterea capacității organizației. De exemplu, actorii externi vor putea obține o viziune veridică și evolutivă a stării SecInf entității evaluate, comparabilă cu alte entități similare.

Ca urmare, M^3SI este conceput pentru a face față provocărilor de SecInf și a oferi o viziune clară, la fel înțeleasă de toți actorii implicați. M^3SI permite analiza, măsurarea, evaluarea și aprecierea SecInf nu doar pentru un anumit obiect izolat în schimbare, ci și pentru grupuri de obiecte tipice, aparținând unei industrii de-a lungul întregului ciclu de viață. Realizarea profilurilor particulare PISI include identificarea, evaluarea și abordarea nevoilor/cerințelor și constrângerilor de SecInf într-un mod consecvent, ghidat de PSITI, având la bază domeniile de SecInf *(e.g.*

oameni, procese, infrastructură TI, SI utilizate) și nivelurile de maturitate cu măsuri/metrici și ținte ale criteriilor de evaluare predefinite în PISI.

La cel mai de sus nivel M^3SI include un număr de domenii de SecInf, stabilit conform cadrelor generale de abordare corelate, e.g. ISO/IEC 27001:2022, NIST SP 800, COBIT 2019, CMMC 1.2 din 2020 [32] și altele, precum [70], [10]. Modelul multiprofil este universal, potrivit pentru diferite ramuri industriale, care, la rândul lor constau din entități tipice, e.g., sectorul financiar-bancar (*banca națională, bănci comerciale, fonduri de investiții* etc.); sănătatea publică și medicina *(spitale, clinici, laboratoare, farmacii etc.)*; ramura educației și cercetării *(instituții preșcolare, școli de diferite niveluri, universități, centre de cercetare etc.).* Pentru fiecare dintre ramurile și entitățile tipice există diferite reglementări la nivel național și local, cu cerințe specifice cazului concret, materializate în profiluri tipice PSITI e.g. constrângeri de securitate *(confidențialitate, integritate, accesibilitate, nerepudiere etc.)*, cultura informațională și resursele disponibile, soluții alternative de atenuare a riscurilor și de creștere a capacității SMSI. De exemplu, la nivel global pentru medicină – HIPAA; pentru bănci PCI DSS; la nivel național pentru bănci – conform *Cadrului legal (pct. 1.1.2)*, Domeniile de securitate și controalele specifice sunt conform cerințelor de securitate specificate fie în ISO 27001:2022 [11], fie în seria de publicații speciale NIST SP 800-53 rev.5 din 2020 [44] sau în alte cadre de abordare, incluse în cadrul aplicației.

Criteriile de evaluare sunt autoritare și fixate în bază de cunoștințe pentru ca mai mulți evaluatori să poată ajunge la aceleași rezultate în evaluarea repetată a unor practici, controale, procese definite în PISI. Caracteristicile modelului M^3SI și a profilurilor rezultante PSITI și PISI, expuse în continuare, permit dezvoltarea inteligentă a unui PISI în baza PSITI și a bazei de cunoștințe M^3SI, care este foarte utilă și necesară pentru marea majoritate a utilizatorilor atât pentru înțelegerea mai bună a controalelor, cât și pentru modificarea acestora de către experți cu adăugarea în baza de date a noilor cunoștințe. M^3SI are următoarele proprietăți:

- **Flexibilitate** – procesele sunt definite în concordanță cu obiectivele propuse în diverse cadre, inclusiv combinate din două sau mai mute cadre;
- **Modularitate** – modelul este împărțit pe arii și niveluri ierarhice distincte;
- **Scalabilitate** – modelul poate fi folosit în diverse industrii și entități, indiferent de tip, forma de proprietate, dimensiune, amplasare în teritoriu etc.;
- **Comprehensibilitate** – o bună integrare a noilor ediții de standarde, modele, metode etc.;
- **Parcurs evolutiv** – procesele sunt implementate incremental, pe etape/niveluri de maturitate, în funcție de dimensiunea organizației, țintele și aspectele pe care aceasta se focusează la momentul respectiv.

3.1.3. Profiluri de maturitate tipice și individuale

Profilul tipic PSITI pentru activitatea bancară în RM și a modelului de maturitate individual PISI pentru o entitate sunt realizate conform *Regulamentului cu privire la sistemele de control intern în bănci* [18], *Recomandărilor cu privire la obiectivele de control și măsurile de securitate ale SMSI* [13], *Regulamentului cu privire la cardurile bancare* [91], *Regulamentului privind cerințele minime pentru Sistemele Informaționale și de Comunicare ale Băncilor* [92] și altele, aprobate de către BNM ca organ superior de supraveghere a băncilor comerciale.

Modelele PSITI țin cont de bunele practici, sunt organizate pe **domenii-controale-obiective-niveluri de maturitate** ale SecInf (*Fig. 3.3).* În literatura de specialitate domeniile SecInf mai sunt numite **zone** sau **arii**. Fiecare domeniu este o grupare logică a bunelor practici/controalelor de SecInf. Practicile din cadrul unui domeniu sunt grupate în funcție de obiective-țintă și ordonate pe niveluri conform valorii nivelului de maturitate.

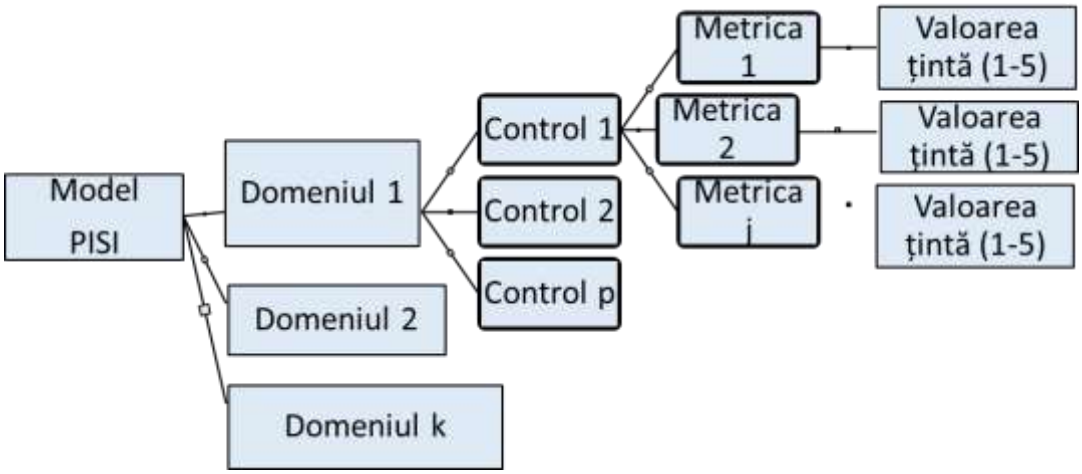


Figura 3.3. Elementele PSITI pe domenii reprezintă o structura ierarhică

Un **model de maturitate individual** permite **analiza decalajelor și evaluarea** unui obiect aflat în schimbare, care trece prin mai multe etape ale ciclului de viață, cu diferite valori/niveluri de maturitate. În acest sens, definirea anumitor etape sau niveluri de maturitate ale SMSI sunt utile, de exemplu, pentru a lua decizii primare privind posibilitatea utilizării SMSI pentru atingerea obiectivelor sau decizii secundare, privind creșterea maturității/îmbunătățirii performanței obiectului. Ca obiective ale evaluării maturității conform profilurilor particulare pot servi: proiectarea unui nou SMSI adecvat circumstanțelor și mediului particular al unei organizații; evaluarea maturității unui SMSI existent; operaționalizarea modificărilor; automatizarea operațională *(evitarea controlului manual)*; adoptarea unor inovații, dezvoltări/îmbunătățiri și altele. De exemplu, obiectivele evaluării maturității pot fi *SMSI în ansamblu, diferite subsisteme/domenii ale SMSI (e.g. rețeaua intranet, extranet) sau procese*

separate (e.g. acces la distanță, copieri backup); Analize privind performanța SMSI, efectuate de management cu scopul de îmbunătățiri; Pre (audit) de certificare etc.

Indiferent de modul de utilizare – **ariile SMSI și profilurile PISI sunt adaptabile, flexibile**, fiecare nivel de maturitate acoperă un anumit set prestabilit de procese cu **„țintele" dorite**, iar nivelurile de maturitate descriu valori concrete ale consistenței SecInf.

Definirea NM în chestionarele de evaluare constituie aportul personal al autorului.

În concluzie, dacă în abordarea veche SecInf era realizată ad-hoc, centrată pe sisteme cu valoarea adăugată preponderent la etapa de utilizare *(a se vedea Tabelul 2.1, Fig. 2.1, Cap. 2)*, în prezent se impune realizarea SecInf gestionată strategic de-a lungul ciclului de dezvoltare, cu **posibilități de îmbunătățire continuă** (PDCA) și cu **valoarea incorporată a SecInf** în toate fazele de dezvoltare și de operare a afacerii.

Acest deziderat poate fi atins prin profiluri individuale de SecInf, generate de M^{3}SI. Raportul evaluării conform PISI **reflectă sfera și starea curentă a SecInf, precum și riscurile și amenințările specifice și sugerează țintele recomandate de îmbunătățire.**

În *Tabelul 3.1* este prezentat un exemplu de PSITI cu 12 domenii și 41 de controale, o primă versiune a modelului, realizată în baza experienței activității în sistemul bancar în fișiere Excel. Noua versiune a modelului are la bază NSIT SP-800.53, versiunea din 2020, care corelează mai bine cu ISO/IEC 27001:2022 și cu cadrul legislativ în vigoare din RM, cu reglementările BNM și tendințele moderne ale SecInf. Conținutul complet al bazei de cunoștințe a modelului M^{3}SI, profilurile PSITI și PISI explorate pot fi consultate/explorate în web aplicația de suport cu acces controlat de către autor, disponibilă la adresa *https://www.m3-si.eu/*.

Noul **PSITI pentru activitatea bancară** este folosit pentru evaluarea și monitoriza BC de către BNM, **dar poate fi utilizat în direct de către fiecare dintre bănci**. Totodată, atât PSITI cât și PISI pot fi adaptate. De exemplu, pentru o bancă procesatoare de carduri bancare pot fi adăugate domenii specifice și controale noi conform PCI DSS, prezentate în *compartimentul 3.2.2*. **Adaptabilitatea profilurilor nu este în niciun fel limitată.** Este la discreția entității ce să adauge sau ce să scoată din PSITI și/sau PISI, oferite implicit de aplicație, principala condiție fiind conformitatea cu cadrul legislativ și de reglementare în vigoare.

De regulă, profilurile individuale stabilesc niveluri de maturitate țintă pentru domenii și controale. Maturitatea conform PISI evaluează cât de bine îndeplinesc procedurile, standardele și ghidurile corporative cerințele PISI, cât de bine ating țintele stabilite. Un exemplu de evaluare conform unu profil PISI controale a se vedea în *Tabelul 3.2*.

Tabelul 3.1. Exemplu de domenii și controale de SecInf pentru activitatea bancară

Aria/Zona	ID	Nume control
Cadrul de organizare a securității informației/CO	CO.1	Politica de securitate a informației
	CO.2	Organizarea SMSI
	CO.3	Relația cu terțele părți
	CO.4	Externalizarea serviciilor TI
Managementul resurselor informaționale/MR	MR.1	Responsabilitatea pentru resurse
	MR.2	Clasificarea informației
	MR.3	Managementul riscurilor
Securitatea resurselor umane/RU	RU.1	Înainte de angajare
	RU.2	Instruirea
	RU.3	Pe perioada angajării
	RU.4	Încetarea contractului sau schimbul locului de muncă
Securitatea fizică și a mediului de lucru/SF	SF.1	Zone de securitate
	SF.2	Securitatea echipamentelor
Managementul comunicațiilor și operațiunilor/MC	MC.1	Proceduri operaționale și responsabilități
	MC.2	Managementul serviciilor terțelor părți
	MC.3	Planificarea și acceptanța sistemelor TI
	MC.4	Protecția contra softului cu potențial dăunător
	MC.5	Copii de rezervă
	MC.6	Securitatea rețelelor de comunicații electronice
	MC.7	Gestionarea suporturilor de informație
	MC.8	Schimbul de informație
	MC.9	Gestiunea mijloacelor criptografice
	MC.10	Managementul vulnerabilităților
	MC.11	Monitorizarea
Controlul accesului la resursele informaționale/CA	CA.1	Politica de control al accesului
	CA.2	Managementul accesului utilizatorilor
	CA.3	Responsabilitățile utilizatorilor
	CA.4	Controlul accesului la rețea
	CA.5	Controlul accesului la sistemele de operare
	CA.6	Accesul la aplicații și informații
	CA.7	Mediile virtualizate
Achiziționarea, dezvoltarea și mentenanță sistemelor de aplicații/AD	AD.1	Cerințele de securitate pentru sistemele aplicative
	AD.2	Procesarea corectă a datelor în cadrul aplicațiilor
	AD.3	Securitatea fișierelor de sistem
	AD.4	Securitatea în procesul de dezvoltare și de suport
Managementul incidentelor SecInf/MI	MI.1	Identificarea și raportarea incidentelor
	MI.2	Reacțiunea la incidentele de securitate
Managementul continuității activității/MCA	MCA.1	Planificarea continuității afacerii
	MCA.2	Restabilirea sistemelor TI
Conformitatea/C	C.1	Conformitatea cu cerințele legale și regulatorii
Auditul intern al securității informației/AI	AI.1	Planificarea și organizarea auditului

Tabelul 3.2. Exemplu de profil PISI cu ținta stabilită și scorul real măsurat

Domenii și controale	Scor țintă	Scor Real
CO.1-Politica de securitate a informației	3,00	2,00
CO.2-Organizarea SMSI	3,00	1,20
CO.3-Relația cu terțele părți	3,00	3,00
CO.4-Externalizarea serviciilor TI	3,00	4,00
MR.1-Responsabilitatea pentru resurse	3,00	2,00
MR.2-Clasificarea informației	3,00	3,00
MR.3-Managementul riscurilor	3,00	1,00
RU.1-Înainte de angajare	3,00	3,00
RU.2-Instruirea	3,00	3,00
RU.3-Pe perioada angajării	3,00	1,00
RU.4-Încetarea contractului sau schimbul locului de muncă	3,00	4,00
SF.1-Zone de securitate	3,00	2,00
SF.2-Securitatea echipamentelor	3,00	5,00
MC.1-Proceduri operaționale și responsabilități	3,00	2,00
MC.2-Managementul serviciilor terțelor părți	3,00	3,00
MC.3-Planificarea și acceptanța sistemelor TI	3,00	2,00
MC.4-Protecția contra softului cu potențial dăunător	3,00	4,00
MC.5-Copii de rezervă	3,00	5,00
MC.6-Securitatea rețelelor de comunicații electronice	3,00	2,00
MC.7-Gestionarea suporturilor de informație	3,00	2,00
MC.8-Schimbul de informație	3,00	3,00
MC.9-Gestiunea mijloacelor criptografice	3,00	3,00
MC.10-Managementul vulnerabilităților	3,00	3,00
MC.11-Monitorizarea	3,00	3,00
CA.1-Politica de control al accesului	3,00	2,00
CA.2-Managementul accesului utilizatorilor	3,00	4,00
CA.3-Responsabilitățile utilizatorilor	3,00	5,00
CA.4-Controlul accesului la rețea	3,00	2,00
CA.5-Controlul accesului la sistemele de operare	3,00	2,00
CA.6-Accesul la aplicații și informații	3,00	3,00
CA.7-Mediile virtualizate	3,00	3,00

3.2. Particularitățile modelelor tipice și individuale

Modelele tipice reflectă specificul unei (sub) ramuri industriale, iar modelul individual – specificul unei entități concrete. PSITI limitează SecInf de jos, cât de mic poate fi SMSI. PISI generat în baza PSITI limitează SecInf și de sus, ținând cont de specificul entității, strategiile de afaceri, politicile de securitate și nivelul de maturitate atins în procesul de măsurare a SecInf, cazul particular de măsurare etc. În esență PSITI este doar un cadru. PISI este și un cadru și un instrument de măsurare, evaluare, raportare și afișare a rezultatelor, realizat în baza chestionarelor cu cele 5 niveluri de maturitate. Evaluările se realizează periodic, minim o dată în an și ori de câte ori apar schimbări în infrastructura TI, sistemele informaționale ale entității, riscuri noi etc., de fiecare dată în baza unor PISI existente sau adaptate cazului de utilizare.

În general un **PISI poate fi echivalat cu o evaluare** conform unei misiuni concrete.

3.2.1. Particularitățile modelelor tipice unor industrii PSITI

De regulă, nucleul controalelor PSITI este în baza cerințelor de bază ale unui standard de bune practici, e.g. NIST SP 800.x, ISO/IEC 27001, PCI DSS etc. La care trebuie adăugate cerințele specifice de SecInf pentru diversele industrii, formulate în standarde și reglementări industriale, specifice *e.g. PCI DSS* pentru activitatea bancară; *HIPAA* aplicabil pentru instituții medicale; regulamentele BNM și alte reglementări locale ale organelor de supraveghere pentru bănci; regulamentele Ministerului Educației și Cercetării pentru instituții de învățământ; regulamentele Ministerului Sănătății pentru spitale, clinici, laboratoare, farmacii etc. Profilul de maturitate **PSITI specifică cerințele organelor superioare și/sau de supraveghere** pentru satisfacerea necesităților managementului.

De exemplu, necesitatea includerii controalelor PCI DSS în profilurile tipice activității bancare PSITI și/sau a profilurilor individuale PISI poate fi determinată conform *(Fig. 3.4).*

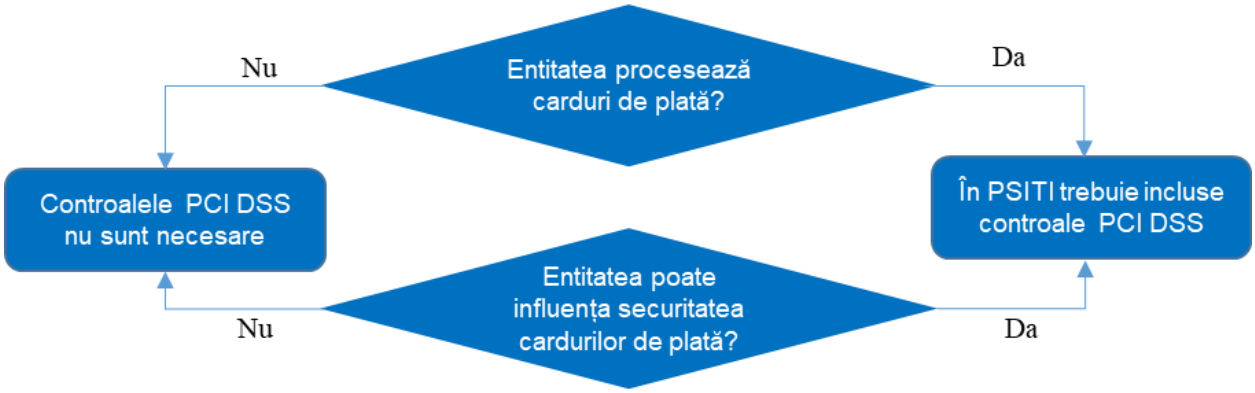


Figura 3.4. Decizia privind includerea controalelor PCI DSS în profiluri tipice/individuale

Modelul PSITI nu este menit să ofere răspunsul definitiv la întrebarea cât de bun este un SMSI individual, ci servește ca **suport de structurare a unui SMSI** individual sau a **unui profil** individual. De fapt PSITI stabilește cât de mic/mare trebuie să fie SMSI, pentru a justifica investițiile și respectiv PISI pentru evaluări concrete particularizate de SecInf sau pentru **compararea maturității diferitelor entități tipice**, care aparțin unei industrii *(e.g. bancară, medicină)* și unui tip concret de afacere *(e.g. bănci, spitale, clinici, farmacii)* cu funcții similare, comparabile.

Controalele sunt recomandate de bunele practici. PSITI sunt generate în baza acestora și respectiv, PISI în baza PSITI, conțin riscurile asociate, definirea nivelurilor de maturitate și țintele urmărite. Tocmai **prin aceste definirii diferă profilurile PISI de PSITI și PSITI de standardele** de bune practici.

Modelul/profilul PSITI este construit în regim de dialog prin selectarea controalelor din diferitele seturi de bune practici, potrivite cadrului legislativ și de reglementare în vigoare și/sau prin clonare-importare și redactare. Ca bază pentru alcătuirea PSITI poate servi unul din seturile global recunoscute, e.g. ISO/IEC 27002 și altele asociate din familia ISO27k *(e.g. Securitatea în Cloud, securitatea în rețea)*, CIS Controls v.8, NIST SP 800.x, COBIT 2019, PCI DSS v 4.x etc., dar fără a se limita la un set. Or, în cadrul unui PSITI pot intra controale din diferite seturi, dacă acestea diferă *(în multe cadre diferite există o parte de controale identice)*. Descrierea completă a modelului PSITI cu descrierea controalelor și a nivelurilor, a maturității pe fiecare control și alte detalii a se vedea în aplicație. **Riscurile posibile asociate cu fiecare control,** e.g. cu cele 114 din ISO/IEC 27001/27002:2013 sau cele 93 din ISO/IEC 27001/27002:202 pot fi foarte specifice și adaptate/precizate în PSITI pentru fiecare industrie și în PISI pentru fiecare entitate. Adaptarea acestora depinde mult de industrie, afacere, contextul, mărimea și specificul organizației.

Astfel, în PSITI și PISI chestionarele aferente sunt oferite **ca exemple generice, reprezentative** ale riscurilor asociate pentru anumite arii/domenii de control și controalele recomandate pe niveluri de maturitate. Chestionarele și definirea nivelurilor constituie sintezarea de către autor a celor mai bine practici ISO/IEC 27001/2 și altor standarde a familiei ISO27k, a seriei NIST SP 800.x, O-ISM3, PCI DSS și altele.

3.2.2. Particularitățile profilurilor individuale de maturitate PISI pentru bănci

Deoarece controalele securității și măsurările sunt derivate din situațiile statice și/sau dinamice concrete de funcționare ale organizației și misiunii evaluării, PISI particularizează un profil PSITI sau un PISI al unei entități similare. Orice entitate concretă își creează propriul profil PISI conform contextului său specific, care va ține cont de aria SMSI, scopul misiunii de

evaluare și țintele stabilite. De regulă, organele de supraveghere stabilesc un model PISI unic pentru toate entitățile supravegheate. De exemplu, PSITI BNM stabilește un cadru unic PISI pentru băncile supravegheate. Însă fiecare bancă poate exploata și alte diferite profiluri particulare PISI, cu alte liste extinse/restrânse de controale și alte chestionare, potrivite pentru alte misiuni, e.g. audit intern de performanță al SMSI sau pre-audit de certificare SMSI etc.

În afară de cerințele generice universale ale ISO/IEC 27001:2022 privind asigurarea SecInf prin prisma implementări unui SMSI, cerințele Legii RM 133 privind protejarea datelor cu caracter personal și GDPR pentru conformitatea cu contextul extern și interesele persoanelor externe cu care entitatea relaționează, la nivelul entității există cerințe specifice de context intern, determinate de misiunea, viziunea, strategiile și politicile interne ale entității, tipul și mărimea entității, volumul afacerii etc.

De exemplu, conformitatea cu standardul internațional de securitate a datelor din industria plăților cu carduri bancare PCI DSS este o **cerință obligatorie** pentru toate organizațiile care **stochează, procesează tranzacții** cu carduri bancare și **este benevolă** pentru altele, care doar utilizează sisteme de plăți electronice. În RM avem ambele tipuri de bănci. **Baza de cunoștințe a aplicației conține cadrul general recomandat PCI DSS conform [20],** care poate fi adaptat și aplicat pentru bănci**.**

În afară de domenii, controale și chestionare profilul PISI mai conține și **nivelurile de maturitate așteptat-identificat, lista de probe și argumente** de rigoare atașate care documentează nivelul de maturitate identificat. Descrierea completă a modelului PISI pentru o bancă cu descrierea controalelor și a nivelurilor, a maturității pe fiecare control și alte detalii a se vedea în aplicație.

În ultimă instanță, rezultatul evaluării conform PISI permite identificarea decalajelor, planificarea etapelor/pașilor de îmbunătățire continuă a securității informației. Totodată, flexibilitatea profilurilor permite acumularea istoricului privind domeniile și îmbunătățirile incrementale, care pot apărea în entitatea analizată de la un trimestru/semestru la altul sau de la un an la altul, în funcție de frecvența impusă de cerințele afacerii.

3.3. Arhitectura aplicației M^{3}SI

Există diverse instrumente/șabloane EXCEL, concepute pentru a face față provocărilor și complexității SecInf, multe dintre ele cu versiuni gratuite, altele sunt versiuni proprietare cu plată. De exemplu, Instrumentul de autoevaluare a controalelor *Controls Self-Assessment Tool de la Center of Internet Security (CIS CSAT [31]),* promovat de centrul CIS și Institutul SANS pentru controalele lor cu versiunea 8 din 2020, conține o listă dinamică a măsurilor de securitate, care

permite organizațiilor să evalueze și să urmărească implementarea controalelor în vederea conformității în funcție de mărimea organizației și propriul său SMSI *(IG1, IG2, IG3 [30]).*

În multe cazuri, asemenea instrumente pot satisface necesitățile organizației. De ce atunci a trebuit să mai realizăm un instrument/o aplicație originală? Aplicația M^{3}SI diferă calitativ de aceste instrumente amintite și altele similare prin:

a) **Sintezarea și sistematizarea** cunoștințelor despre diverse cadre de SecInf și instrumente/chestionare de evaluare, inclusiv pe cinci niveluri de maturitate într-o singură bază de date cumulativă adaptabilă și extensibilă;

b) **Aplicabilitatea universală a aplicației**, de exemplu pornind de la Top 20 CIS Controls, orientate preponderent spre Internet; CMMC, orientate preponderent spre securitatea cibernetică; cu adăugarea PCI DSS, orientate spre tranzacțiile cu carduri bancare; cu migrarea spre controalele ISO/IEC 27001:2022, NIST sau altele care pot fi arbitrar extinse/restrânse/modificate.

c) **Acumularea istoricului** evaluării nivelurilor de maturitate ale entității conform unor PISI și misiuni particularizate, urmărirea progresului, dinamicii;

d) **Comparabilitatea evaluărilor** diferitelor entități din contul formalizării criteriilor de evaluare și a metricelor de SecInf definite în PSITI.

Pentru a utiliza aplicația ce integrează modelul generic M^{3}SI, PSITI și PISI, utilizatorul trebuie:

1. Să definească **aria de aplicabilitate a SMSI** sau **a misiunii de evaluare**, pornind de la modelul tipic industriei, prin eliminarea, adăugarea, modificarea unor controale specifice în toate sau în oricare dintre modelele M^{3}SI, PSITI, PISI, dictată de necesitățile și constrângerile organizației, a misiunii de evaluare etc.;
2. Să **genereze profilul individualizat** de maturitate a securității informației PISI. Eventual prin identificarea unui PISI similar/apropiat, clonarea și adaptarea lui sau prin construirea inițială PISI prin combinarea domeniilor de control și controalelor aferente în conformitate cu riscurile și amenințările caracteristice pentru industria și entitatea dată;
3. **Să completeze chestionarele/listele de întrebări și/sau metricile** criteriilor respective *(prin selectarea valorilor constante prestabilite din meniurile derulante de pe paginile fiecărui control, inclus în PISI).* În baza răspunsurilor la fiecare întrebare și/sau a alegerii unor opțiuni din listele derulante și/sau a introducerii rezultatelor măsurărilor criteriilor de evaluare, aplicația determină în mod automat scorurile nivelului de maturitate conform metricilor furnizate pe domenii și controale, după care

afișează **Raportul rezultant al evaluării cu diagrame de tip radar sau cu bare.** Raportul și diagramele sunt afișate **integral, conform profilului PISI** și **detaliat** pe domenii separate. De exemplu, pentru compararea stării curente cu obiectivele-țintă ale indicatorilor și/sau pentru analiza decalajelor pe domenii concrete de control conform scării/culorilor matricei de analiză a riscurilor [5] etc.

4. **Să elaboreze recomandările și/sau planurile** de îmbunătățire bazate pe evaluarea realizată/raportul rezultant. Scorurile obținute pot fi utilizate fie pentru a măsura progresul organizației, fie pentru a formula obiective/sarcini de îmbunătățite, fie pentru a diminua riscurile conform nevoilor și constrângerilor clienților și ale organizației, fie pentru a asigura trecerea evolutivă în trepte de la un efort ad-hoc individual (nivelul inițial al maturității) la o abordare organizațională consistentă și optimizabilă de îmbunătățire continuă a SecInf spre cel mai înalt nivel de maturitate.

3.3.1. Baza de date a aplicației

Baza de date a modelului M^3SI întrunește cunoștințele despre cele mai bune practici, modele, standarde, instrumente de SecInf care se aplică atât la nivel global, național cât și local, în cadrul diferitelor medii de afaceri, permițând organizațiilor să creeze în mod inteligent un model multiprofil M^3SI, care să corespundă nevoilor generale și specifice de îmbunătățire a performanței.

Conținutul principal al BD îl constituie cunoștințele despre ariile și controalele de SecInf/SC, preluate și adaptate din cele mai bune practici/cele mai răspândite cadre de abordare a SecInf, precum O-ISM3:2018, NIST SP:2018, familia ISO27k, inclusiv ISO/IEC 27001:2022, ISO/IEC 27004:2016, ISO/IEC 27032:2023, ISO/IEC 27033 partea 1-7 (2010-2023), PCI DSS versiunea 4.x din 2023, COBIT:2019, ISO/IEC 20000-1:2018, ITIL versiunea 4 din 2019; harta structurată a amenințărilor conform (ENISA, 2020 [71]), nomenclatoare de vulnerabilități și cataloage de risc recunoscute la nivel global (e.g. ISO/IEC 27005:2022 [28], CVE:2021 [72] , CIS Controls v8 (2020) [6]) etc. la fel adaptate de autor pentru necesitățile aplicației. În afară de adaptare și sintezare, aportul important al autorului în realizarea conținutului informațional al bazei de cunoștințe constă în definirea criteriilor pe cele 5 niveluri de maturitate.

Baza de date a aplicației constă din șapte fișiere relaționate între ele prin atribuite-cheie așa cum este ilustrat în *Figura 3.5*:

1. Lista Entităților care utilizează aplicația,
2. Utilizatori,
3. Date de Logare,
4. Baza de cunoștințe a aplicației (nucleul informațional al aplicației),

5. Standarde și/sau PISITI,
6. Controale grupate pe arii,
7. Chestionare de control, care conțin țintele stabilite de entitate și notele atribuite de evaluatori pentru misiunile de evaluare realizate.

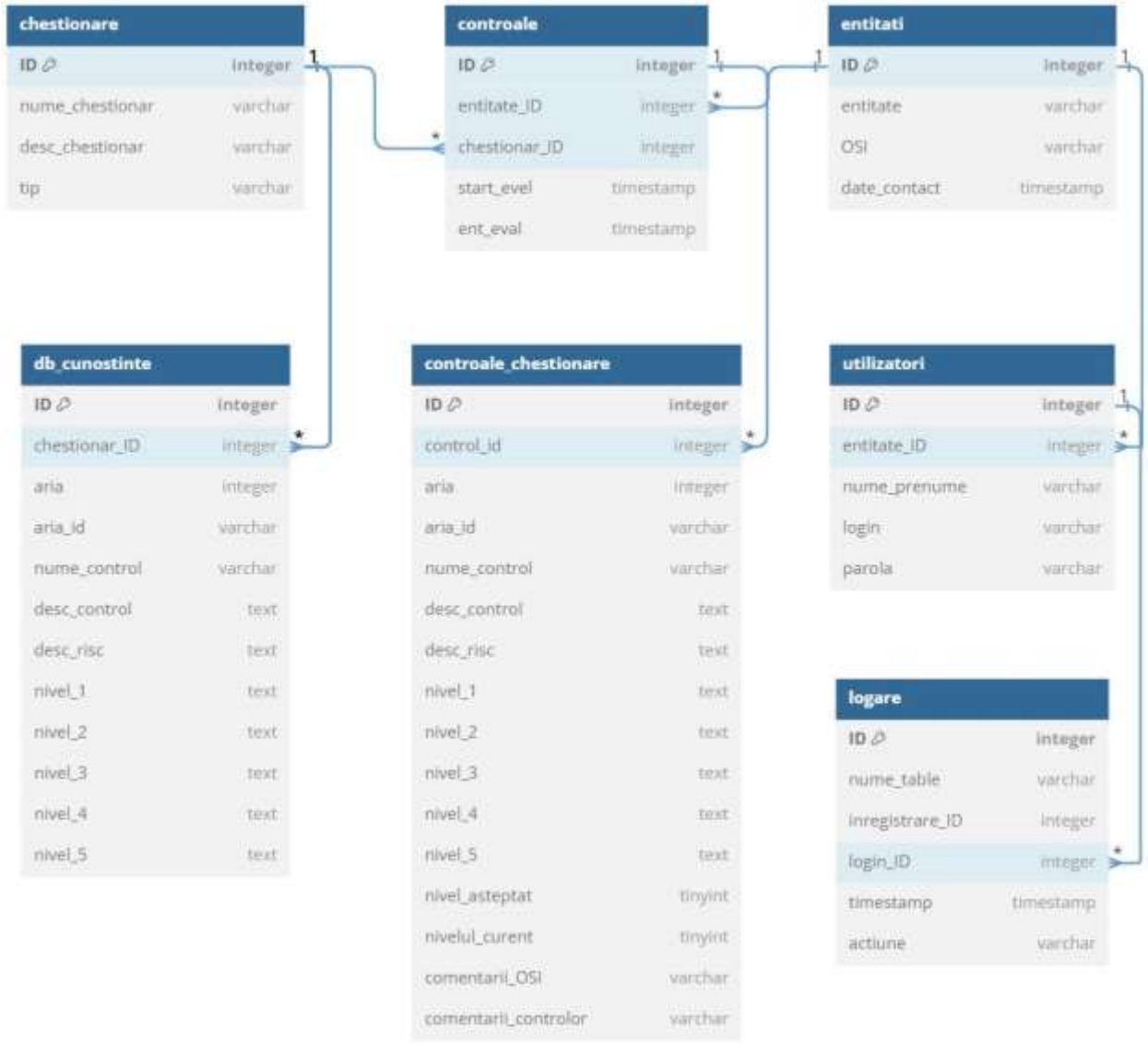


Figura 3.5. Schema info-logică a bazei de date a aplicației M3-SI

Utilizatorii aplicației pot completa fișierele BD manual, câte o înregistrare. Dar volumele mari de date, precum standardele de bune practici, cu cartografierea relațiilor dintre controalele de SecInf cu referire la clauzele respective ale cadrelor mapate, pot fi importate direct din fișiere Excel, prealabil pregătite. De exemplu, mapările controalelor ISO/IEC 27001:2022 cu controalele versiunii precedente ISO/IEC 27001:2013 se conțin direct în denumirile controalelor ISO/IEC 27001:2022. Cartografierile ajută la o mai bună înțelegere și justificare a controalelor incluse în model, determinarea dacă acestea funcționează în concordanță cu standardele independente

existente și recomandările de securitate, dacă pot asigura comparabilitatea maturității diferitelor entități cu diferite profiluri PISI și altele. Cele mai multe cartografieri sunt realizate în CIS Controls v8. Acestea sunt asociate cu ISO27k și cu mai mult de o duzină de standarde industriale, inclusiv HIPAA, NIST, PCI DSS etc.

Actual baza de date a aplicației conține cadrul de control și chestionarul de audit ISO/IEC 27001:2013, ISO/IEC 27001:2022, PCI DSS, un model PSITI mai vechi pentru activitatea bancară și un model PSITI actualizat, necesar și utilizat în prezent de către BNM pentru evaluarea și compararea SecInf a băncilor supravegheate, realizarea unor controale/verificări specifice a unor bănci în baza unor modele particularizate PISI.

Dar **conținutul BD nu a fost un scop în sine pentru teză, nu este în niciun fel limitat** și **poate fi continuu adăugat, dezvoltat, adaptat** conform necesităților entității. Rolurile respective din aplicația M3-SI pot adăuga noi cadre, noi profiluri PSITI și PISI, pot realiza noi evaluări.

3.3.2. Interfața aplicației M^{3}SI și scenariul de utilizare

Aplicația de suport a modelului M^{3}SI este găzduită pe domeniul Internet de nivel superior al Uniunii Europene „.eu”, care este dotat cu un sistem avansat de protecție împotriva înregistrărilor abuzive pentru a permite organizațiilor să își protejeze numele de domeniu.

Mediul de dezvoltare al aplicației este Apache, PHP, MYSQL, Java script, HTML.

În esență, aplicația este un sistem de administrare a bazei de cunoștințe, a profilurilor tipice unor ramuri industriale PSITI în baza cadrelor de bune practici și generare a profilurilor individuale PISI, destinate pentru evaluarea securității informației într-o entitate și o misiune concretă. Este o aplicație de tip web **cu acces controlat de către autor**, disponibilă la adresa *https://www.m3-si.eu*. Dar aplicația poate fi găzduită pe orice alt server web proprietar al entității, care satisface condițiilor mediului de dezvoltare al aplicației. După culegerea adresei de lansare *https://www.m3-si.eu* apare meniul de autentificare, prezentat în *Figura 3.6*. Detalii privind funcțiile aplicației a se vedea capturile de ecran din *Anexa 2*.

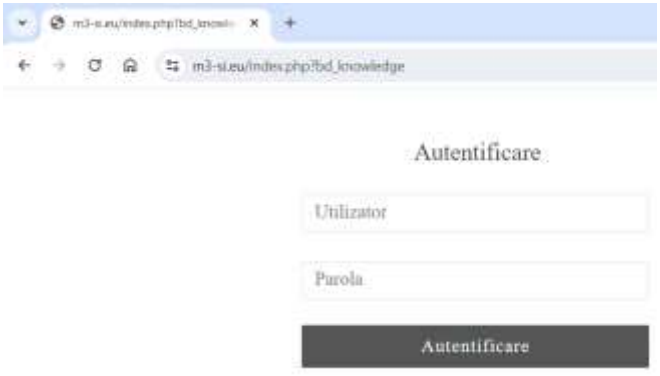


Figura 3.6. Fereastra de autentificare în aplicație

Utilizatorul trebuie să-și cunoască **numele de logare** și **parola de acces**, obținute de la administrator. Rolurile în sistem și lista utilizatorilor sunt definite doar de către administrator. În afară de administrator aplicația permite și alte clase de utilizatori, fiecare cu drepturile sale tranzitive de sus în jos și asimetrice: utilizatorii de nivel superior pot realiza orice manipulări accesibile utilizatorilor de pe nivelurile inferioare, dar nu și invers.

1. **Administratorul sau Evaluatorul** administrează baza de date a aplicației, profilurile PSITI, PISI, listele de evaluări și de utilizatori. Acesta este un **utilizator privilegiat,** care poate crea profiluri PSITI, PISI fie prin clonarea unuia dintre cele existente, fie prin selectarea și redactarea controalelor din unul sau mai multe cadre de abordare.
2. **Utilizator evaluator sau utilizator evaluat** – poate introduce date/evalua SecInf în baza unor profiluri PISI asociate și poate genera – afișa rapoarte de evaluare. De exemplu, un asemenea utilizator poate fi ofițerul de securitate a informației din entitatea evaluată, care poate introduce date și genera rapoarte de autoevaluare și de documentare a raportului pentru profilurile asociate. Acești utilizatori au acces doar la Evaluări și Diagrame din entitățile din care fac parte.

După autentificarea în aplicație apare interfața cu meniul implicit activat *„Baza de cunoștințe”* (*https://www.m3-si.eu/index.php?bd_knowledge/*). Înseși interfața este intuitivă, ușor de utilizat și după lansare afișează două zone de operare, *Zona 1* și *Zona 2* care, la rândul său, este structurată în trei *subzone 2.1-2.3 (Fig. 3.7).*

Figura 3.7. Viziune de ansamblu a interfeței M³SI

Aplicația permite *adăugarea unui exemplar nou al obiectului selectat, clonarea unui obiect existent pentru o nouă utilizare, ștergerea* sau *editarea datelor de identificare a obiectului.*

Prima zonă (din stânga) conține o listă a meniurilor funcționale. Opțiunile meniurilor pot fi activate în mod tradițional: plasarea cursorului pe opțiunea dorită și un dublu ***Click*** când cursorul este plasat pe obiectul selectat sau tastarea ***Enter***. Obiectul selectat este evidențiat prin text de

culoare albastră (în Fig. 3.7. Baza de cunoștințe, colțul din stânga-sus). Aceste meniuri permit adăugarea, eliminarea, editarea listei entităților, listei utilizatorilor, listei evaluărilor și/sau a profilurilor tipice PSITI, realizarea de noi evaluări/misiuni de control, revizuirea unor evaluări deja efectuate.

Operarea cu meniurile este transparentă și intuitivă:

- **Baza de cunoștințe** – permite manipularea cu datele cadrelor global recunoscute de abordare a SecInf (standarde), care servesc ca sursă de alcătuire a profilurilor tipice (PSITI), care la rândul lor servesc pentru crearea/clonarea și editarea profilurilor individuale PISI;
- **Entități –** listează numele entităților ce utilizează sistemul;
- **Evaluări PISI –** listează perioadele misiunilor de control/evaluări conform profilurilor individuale PISI create și asociate unor utilizatori din entitățile respective. Permite introducerea prin activarea acțiunii „Completează", după care urmează selectarea nivelului de maturitate curent și comentariile OSI pentru controalele stabilite în PISI. Comentariile OSI pot fi nume de documente/dovezi confirmative sau trimiteri către acestea. Este posibilă completarea parțială și/sau modificarea repetata a datelor;
- **Diagrame –** permite selectarea și afișarea unor rapoarte de evaluare în cadrul misiunilor cu rezultatele sumare ale evaluării și lista riscurilor reziduale;
- **Utilizatori –** conține lista pe roluri și drepturile lor de operare cu obiectele asociate;
- **Manual** de utilizare – afișează instrucțiuni succinte de operare în aplicație.

Zona 2, este locul principal de lucru pe ecran, în care se afișează exemplarele obiectului selectat și posibilitățile de manipulare cu acesta. Zona 2 are trei subzone: *2.1-2.3 (Fig. 3.7).* Posibilitățile de manipulare includ ***adăugarea*** *unui nou obiect* **și acțiuni** cu obiectul selectat, precum ***clonarea, ștergerea, editarea,*** evidențiate prin culoare *(zona 2.3, Fig. 3.7, partea dreaptă)*: Este posibilă **Editarea** numelui, tipului obiectului prin selectarea pictogramei de culoare verde sau  **Ștergere** de culoare roșie sau  clonare toate  situate în partea dreaptă a ecranului sub titlul „**Acțiuni"**. Tot în această zonă pot fi editate înregistrările, atributele cadrelor de bune practici, pot fi introduse datele de evaluare etc. prin activarea butonului de culoare albastră cu numărul de înregistrări al obiectului selectat *(zona 2.2, Fig. 3.7).*

Manipularea cu exemplarul obiectului trebuie confirmată prin **activarea/Click** pe butonul respectiv, de exemplu pentru obiectele „*Bazei de cunoștințe"* acestea sunt butonul „**Editează chestionar**", amplasat în partea de jos a zonei de lucru și **„Confirmați înregistrarea datelor?"**, afișată în partea de sus a ecranului *(Fig. 3.8).*

Baza de cunoștințe conține Cadre/Standarde de abordare a SecInf și Profiluri PSITI. Aici pot fi adăugate cadre noi, pot fi editate cadre deja existente, pot fi eliminate/șterse cadre care nu mai sunt utile. Actualizarea cadrelor de abordate a SecInf, a profilurilor PSITI și PISI trebuie realizată înaintea oricărei funcții de evaluare. În teză este realizat un PSITI real și un PISI real pentru activitatea bancară, altele fiind arbitrare.

Aplicația permite *adăugarea unui exemplar nou al obiectului selectat, clonarea unui obiect existent pentru o nouă utilizare, ștergerea lui.* Editarea datelor de identificare a obiectelor este diferită de editarea cunoștințelor despre acel obiect, e.g. nivel de maturitate, valori țintă.

Figura 3.8. Exemplu de editare a unui obiect din Baza de cunoștințe

Posibilitatea de manipulare în interiorul obiectului ***(Acțiuni:*** pictogramele *Edit, Delete)* în partea dreaptă a ecranului, la fel evidențiate prin culoare, așa cum se vede în *(Fig. 3.9).*

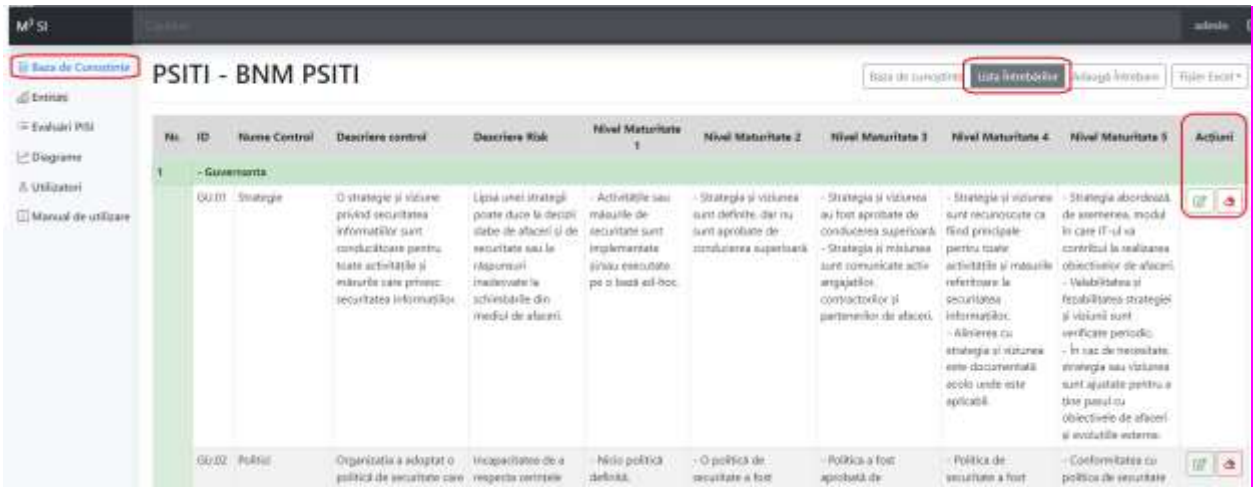


Figura 3.9. Exemplu de editare a conținutului unui PSITI selectat

Scenariul general de utilizare a aplicației presupune existența cel puțin a unui cadru de abordare sau PSIITI, din care pot fi create profiluri individuale PISI și realizate controale conform acestor profiluri.

Un exemplu de editare a unui cadru standard a se vedea *(Fig. 3.10).* În Figura 3.10 se poate observa diferența dintre standarde și PSITI – atribuitele cu valoarea TBD nu au valorile definite.

Figura 3.10. Un fragment al ecranului de editare a unui standard

Pentru detalii a se explora web aplicația de suport, disponibilă la adresa [https://www.m3-si.eu/.](https://www.m3-si.eu/)

. Standardele și profilurile sunt aplicabile pentru toate băncile din RM, supravegheate de către BNM. Dar evaluările concrete semnifică aprobarea profilului PSITI de către BNM, a profilului PISI de către BNM și entitatea respectivă. Sau, fiecare entitate/BC își poate particulariza profilurile PISI, destinate unor misiuni speciale de audit intern și/sau de evaluare a performanței SMSI cu scopul de analiză a decalajelor pentru îmbunătățiri ulterioare și/sau de justificare a proiectelor de investiții în SecInf. După aprobare BC vor raporta BNM în baza acestor profiluri.

Exemplificarea funcției de introducere a datelor de evaluare a se vedea în (*Fig. 3.11).* Funcțiile de operare sunt realizate de către persoane autorizate împuternicite numite de către top managementul entității/OSI. Evaluarea rezumă în colectarea probelor și dovezilor conform cerințelor stabilite și aprobate de către entitate și introducerea valorilor în PISI. Aplicația permite selectarea profilului și evaluarea conform acestui profil de către persoana autorizată împuternicită în baza drepturilor, care pot fi modificate doar de către administrator. Persoana autorizată, eventual OSI, introduce valorile caracteristicilor de evaluare/răspunde la întrebările chestionarului, după care aplicația calculează raportul de evaluare și afișează diagramele solicitate de utilizator.

Figura 3.11. Un fragment al ecranului de evaluare conform PISI pentru banca „Alfa”

Rezultatele evaluărilor sunt afișate în diagrame de diferite forme *(Fig. 3.12)* și lista riscurilor reziduale identificate *(Fig. 3.13)*, care pot fi prioritizate, filtrate, tratate conform politicilor, scopurilor, necesităților.

Figura 3.12. Moduri de afișare grafică sumară a evaluării BC „Alfa”

Aplicația afișează raportul de evaluare în formă integrală *(toate ariile de control pe o digramă)* sub formă de diagrame radar cu 2 linii *(scor țintă – scor curent)* diagramă tip bare verticale și sub formă de linii frânte, fiecare utilă în funcție de scopul urmărit. De exemplu,

compararea pe domeniile SMSI, analiza decalajelor, urmărirea progresului, justificarea deciziilor, analiza/compararea între entități diferite ale aceleiași industrii, evoluția în timp (creșterea maturității).

Riscuri de securitate identificate

#	ID	Aria	Nume control	Descriere risc	Risc inerent
1	GU.02	Guvernanta	Politici	Incapacitatea de a respecta cerințele legislative, regulatorii și/sau interne de IT (securitate) din cauza unui cadru de politici ineficient care susține strategia IT și securitatea informațiilor.	Mic
2	GU.03	Guvernanta	Plan / Foaie de parcurs	Organizația nu oferă îndrumare și suport pentru securitatea informațiilor în conformitate cu obiectivele de afaceri, riscurile și cerințele de conformitate.	Mic
3	GU.04	Guvernanta	Arhitectura	O viziune incompletă asupra arhitecturii actuale și țintă poate duce la creșterea costurilor, complexității și incapacității de a răspunde în timp util la provocările determinate de schimbările din afaceri.	Mediu
4	OR.02	Organizare	Segregarea responsabilitatilor	Acțiuni unilaterale (de exemplu, accesul neautorizat la date) ar putea avea loc în procesele cheie de IT, ceea ce ar putea duce la un impact negativ asupra proceselor de afaceri, de exemplu, riscul de utilizare neglijentă sau deliberată a sistemului.	Mic

Figura 3.13. Un fragment al listei riscurilor remanente

Cele două suprafețe colorate pe diagrama radar semnifică scorul țintă (albastru) și scorul/ nivelul de maturitate curent de culoare violetă, razele semnifică ariile de control. Culorile au aceeași semnificație pe diagramele cu bare verticale și pe diagramele cu segmente de linie frântă.

Raportul în formă grafică este util în toate cazurile misiunilor de audit al SecInf *(intern de performanță, pre-audit de certificare)* pentru analiza vizuală a decalajelor și de planificare a îmbunătățirilor sub forma unei viziuni integratoare, pe o pagină.

Totodată, pe fiecare dintre ariile/domeniile de control sunt afișate diagrame grafice de tip bare. Acestea sunt utile pentru analize punctuale separate, e.g. pentru justificarea unor proiecte de îmbunătățire a managementului accesului în baza analizei decalajelor. În *Figura 3.14* sunt afișate două asemenea domenii, fiecare cu câte cinci controale, barele de culoare albastră reflectând valorile țintelor iar de culoare roșie valorile reale ale controalelor. După cum se poate observa din *(Fig. 3.14),* entitatea are mari rezerve de îmbunătățire pe controlul *ID.03. Super utilizatori* al domeniului *Managementul accesului* și rezerve moderate pe domeniul *Guvernanță,* controalele *GU.01 Strategie; GU.02 Politici; GU.03 Plan/Foaie de parcurs* și *GU.04 Arhitectura* informațiilor întreprinderii.

Pentru alte detalii privind rapoartele de evaluare și afișările grafice a se explora aplicația.

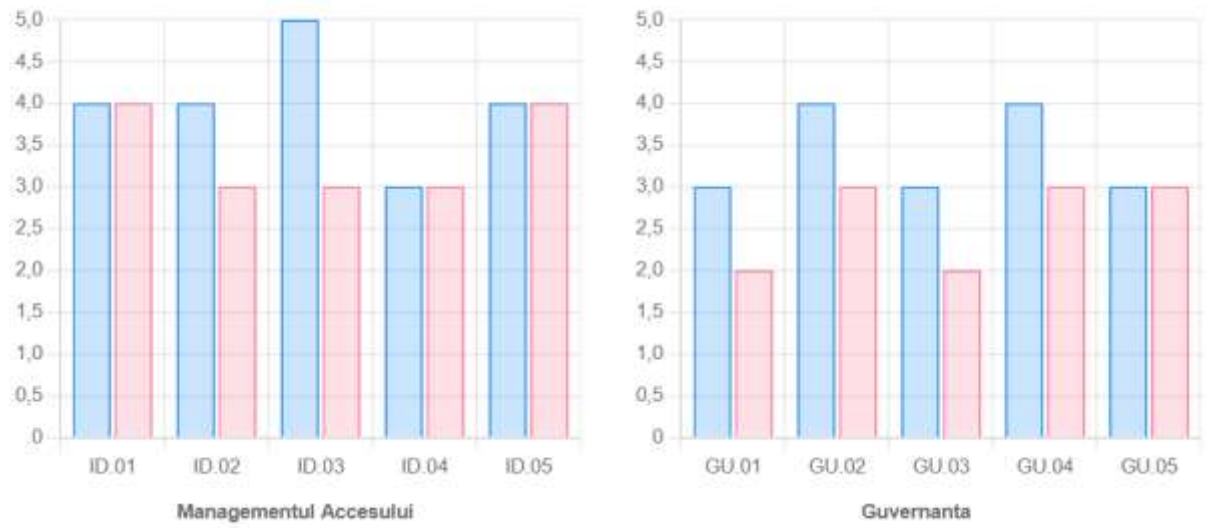


Figura 3.14. Detalii privind nivelurile de maturitate pe domenii/arii separate

Aplicația M3-SI permite **importarea/exportarea cadrelor de abordare și a chestionarelor elaborate** sub forma unor fișiere Excel *(Fig. 3.15).* Această oportunitate este deosebit de utilă la elaborarea inițială a cadrelor și/sau a chestionarelor pentru operarea cu toate liniile tabelului, verificarea sintaxei, corectarea masivă a conținutului, precizarea controalelor, riscurilor și metricilor etc.

Fișierele Excel trebuie să aibă valori de intrare în fiecare celulă, nu se admite divizarea sau îmbinarea celulelor, nu se admit semne speciale precum &, @, întrerupere forțată de linie, semne de operare, de concatenare și alte semne cu destinație specială în Excel. În cazul importului unui PSITI și lipsei valorilor nivelurilor de maturitate 1-5 acestea obțin valori implicite: *Inițial*, *Repetabil*, *Definit*, *Gestionat/Măsurabil*, *Îmbunătățire continuă.*

Figura 3.15. Ilustrarea oportunității de import/export a standardelor/chestionarelor

Liniile de Excel în care lipsește cel puțin o valoare a unuia dintre atributele obligatorii nu se vor importa, despre care fapt utilizatorul este informat *(Fig. 3.16).*

Figura 3.16. Informarea privind numărul de controale importate

3.3.3. Ilustrarea evaluării nivelului de maturitate pentru un profil concret PISI

Fie că entitatea este interesată de evaluarea SecInf pe 6 domenii, identificate de A la F, fiecare cu un oarecare număr de subdomenii și controale identificate de la A1 la An, B1 – Bn etc.

Cadrul de organizare al SecInf (domeniul A):

A1. Managementul asigură orientarea generală și sprijinul pentru SecInf în conformitate cu cerințele afacerii, legislația și actele normative aplicabile.

A2. Organizarea internă este adecvată pentru managementul securității informației.

A3. Este asigurată SecInf în relația cu terțe părți care prestează sau beneficiază de servicii, ce implică informația entității.

A4. Este asigurată securitatea și continuitatea serviciilor și externalizate către furnizori externi de servicii.

Managementul comunicațiilor și operațiunilor (domeniul B):

B1. Este asigurată operarea corectă și în condiții de securitate a sistemelor de procesare a informației (SPI).

B2. Software-ul și informația entității sunt protejate de activitatea malițioasă a virușilor.

B3. Este asigurată integritatea și disponibilitatea informației entității și a SPI.

B4. Este asigurat schimbul securizat de informație și pachete software cu terțe părți, precum și în interiorul entității.

B5. Este realizată prevenirea existenței vulnerabilităților pentru resursele entității.

B6. Activitățile neautorizate de accesare a informației și de utilizare a resurselor informaționale sunt identificate în timp util.

Managementul și securitatea resurselor umane (domeniul C):

C1. Este asigurat faptul că noii angajați sunt corespunzător verificați înainte de acordarea accesului la resursele entității, iar responsabilitățile pentru securitatea informației sunt adecvat stabilite, comunicate și asumate.

C2. Este asigurat faptul că cerințele de SecInf sunt cunoscute și respectate necondiționat de către angajați, iar responsabilitățile și răspunderea lor juridică sunt stabilite și conștientizate corespunzător.

C3. Este asigurat faptul că angajații încetează relația cu entitatea într-o manieră controlată din punct de vedere al riscurilor de securitate.

Managementul proceselor (domeniul D):

D1. Asigurarea implementării Managementului incidentelor de securitate.

D2. Asigurarea implementării Managementului continuității activității.

D3. Asigurarea conformității cu cerințele legale.

Securitatea infrastructurii TI (domeniul E):

E1. Asigurarea stabilirii și asumarea responsabilității pentru protecția corespunzătoare a resurselor informaționale ale entității.

E2. Asigurarea faptului că informația beneficiază de un nivel de protecție adecvat, proporțional importanței ei, reglementărilor aplicabile și amenințărilor aferente.

E3. Asigurarea stabilirii și realizării politicii de control al accesului la resursele informaționale ale entității.

Securitatea fizică și a mediului de lucru (domeniul F):

F1. Asigurarea prevenirii accesului fizic neautorizat, distrugerii și pătrunderii în interiorul entității, precum și al accesului la resursele informaționale și definirea zonelor de securitate.

F2. Asigurarea prevenirii pierderii, distrugerii, furtului sau compromiterii echipamentelor TIC și întreruperea proceselor de activitate ale entității.

Nivelul fiecărui domeniu de SecInf în parte și Nivelul de maturitate integrat al SecInf este apreciat conform scărilor aduse în Tabelul 3.3.

Tabelul 3.3. Scări de apreciere a Domeniilor și a Nivelului de maturitate al SecInf

Valoare	**Nivel operațional**		
0	Inexistent	**Interval valori**	**Nivel de maturitate**
1	Inițial	0 – 1.5	1 - Nonconformitate
2	Repetabil intuitiv	1.6 – 2.5	2 - Conformitate inițială
3	Proces definit	2.6 – 3.5	3 - Conformitate de bază
4	Gestionat și măsurabil	3.6 – 4.5	4 - Conformitate acceptabilă
5	Optimizat	4.6 – 5	5 - Conformitate deplină

Un exemplu de evaluare a SecInf pe domenii, de determinare și afișare a nivelului de maturitate a se vedea în *Figura 3.17*. În partea stângă a *Figurii 3.17* sunt indicate valorile

indicatorilor, iar în partea dreaptă putem observa vizual nivelul de maturitate în forma unei diagrame de tip radar. Pentru analiză, comparare, evaluare valoarea numerică a nivelului de maturitate poate fi exprimată ca aria suprafeței hexagonului.

Aria hexagonului ca valoare integrată a nivelului de maturitate poate fi ușor calculată în mod analitic, ceea ce permite evaluarea repetată și/sau continuă în mod automatizat în cadrul unei entități pentru observarea dinamicii prin compararea ariilor hexagoanelor respective și/sau compararea nivelurilor de maturitate pentru diferite entități tipice în cadrul unei industrii.

Domeniu	**Nota**	**Domeniu**	**Nota**	**Domeniu**	**Nota**
A	**3,25**	**B**	**3,33**	**C**	**3,33**
A1	3	B1	3	C1	3
A2	3	B2	3	C2	3
A3	4	B3	4	C3	4
A4	3	B4	3		
		B5	4		
		B6	3	*	3
D	**3,6**	**E**	**4,0**	**F**	**4,5**
D1	4	E1	3	F1	4
D2	3	E2	4		
D3	4	E3	5		
		F1	4	F1	4

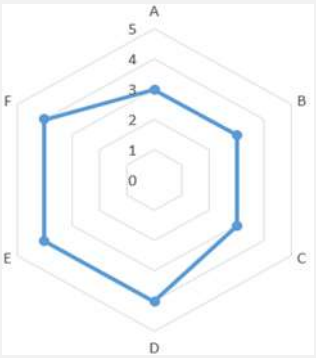


Figura 3.17. Exemplu de evaluare a SecInf pe 6 domenii

Evaluarea conform PISI permite entității să se pronunțe asupra modului în care funcționează SMSI și SecInf, precum și identificarea punctelor slabe și planificarea remedierii eventualelor deficiențe. Totodată, PISI furnizează o evaluare unică, în urma căreia este posibilă nu doar compararea internă și dinamică în timp a nivelurilor de maturitate pe domeniile/procesele SMSI și controalele SecInf, ci și compararea externă a maturității SMSI între organizații tipice. Profilul particular PISI permite o evaluare utilă a funcționării întregului SMSI sau a unei părți a acestuia, în funcție de aspectele pe care entitatea decide să le analizeze pe durata funcționării sale. Evaluarea vizează clasificarea performanței SMSI pe baza criteriilor și dovezilor documentate obținute fie în cadrul supravegherii sau analizei efectuate de management, fie în cadrul unui audit tematic intern sau extern.

Un exemplu al raportului de evaluare pentru o altă bancă Alfa sau o altă misiune ilustrează flexibilitatea modelului M^3SI, profilul PISI conținând deja nu șase, ci 15 domenii, numărul acestora fiind stabilit de entitate în baza modelelor PSITI elaborate în acord cu bunele practici/cadre de abordare și aprobate de entitate *(Fig. 3.18).*

Figura 3.18. O altă evaluare a SecInf/conform altui PSITI și PISI

Fiecare PSITI și PISI poate avea propriile sale metrici/chestionare, preluate din PSITI și adaptate/orientate spre atingerea obiectivelor specifice. Iar determinarea maturității se bazează pe revizuirea documentației SMSI, intervievarea personalului, efectuarea unor măsurători în cadrul auditului de performanță a SecInf, a unor analize a decalajelor dintre țintele și valorile măsurate pentru fiecare dintre domeniile și controalele de securitate incluse în PISI**.**

De exemplu, pentru pre-audituri de certificare măsurătorile de bază ale SMSI în PSITI și profilurile PISI trebuie și pot fi adaptate conform celor stabilite de ISO/IEC 27004:2016 [47]: Ce trebuie monitorizat *(Clauza 6.2);* Ce trebuie măsurat *(Clauza 6.3);* Ce trebuie monitorizat, măsurat, analizat și evaluat *(Clauza 6.4);* Cine trebuie să monitorizeze, măsoare, analizeze și evalueze *(Clauza 6.5).* Tot în acest standard sunt sugerate tipurile de măsurări *(Clauza 7.2. Măsurări de performanță; Clauza 7.3. Măsurări de eficacitate)*. Procesele sunt descrise în Clauza 8 a standardului, iar anexele prezintă modele de măsurare a securității informației *(Anexa A)*, exemple de constructe de măsurare *(Anexa B, Anexa C).*

Entitatea este în drept să-și aleagă de sine stătător modelele, indicatorii, procesele, metricile etc. conform necesităților misiunilor sale concrete, cerințelor legale globale și industriale, bunelor practici, tradiții și instrumente utilizate precum O-ISM3 [8], CMMC 2.0 [37], C2M2 [72], CIS Controls v8/CSAT [31], COBIT [35], NIST SP 800.x [36] etc.

Evaluarea nivelurilor pe domenii și controale se realizează conform criteriilor elaborate/metricilor fixe ale modelului. În cazul când criteriul specificat are mai multe metrici și

acestea au fost apreciate cu valori diferite, scorul sumar poate fi apreciat, de regulă, la nivelul metricii cu valoarea cea mai scăzută, fie cu o valoare medie.

3.4. Concluzii

Platforma M3-SI (cadrul de abordare a împreună cu aplicația) posedă o serie de **avantaje și caracteristici inovative:**

a. Este o **platformă integrată multinivel** (model generic – profil tipic PSITI – profil individual PISI – arii de control – controale – niveluri de maturitate) și multidimensional de **concepere, dezvoltare, evaluare și îmbunătățire continuă a SecInf**;

b. Este o **metodă practică și un instrument de determinare a riscului de SecInf** și de măsurare obiectivă a capacității de a atenua cele mai importante riscuri prin identificarea decalajelor dintre capacitățile actuale ale organizației și nivelul de maturitate necesar stabilit de cadrul legal, de politicile și strategiile entității;

c. Aplicația de suport **generează rapoarte și diagrame vizuale** privind starea, obiectivele și necesitățile de îmbunătățire a SecInf, bazate pe dovezi documentate. Afișarea rezultatului evaluării sub formă de diagrame **înlesnește analiza decalajelor.** În baza acestora consiliul de conducere, auditorii etc. pot obține informații obiective, consistente, calitative asupra stării SecInf și pot justifică deciziile sale;

d. Organizațiile pot alege să aibă profiluri multiple conform nevoilor individuale, aliniate la anumite componente și/sau misiuni;

e. **Ofițerii și echipele de profesioniști** de Securitate a informației, TI, SI, Cibernetică etc. **pot elimina o mare parte a rutinei** privind colectarea, documentarea și aprecierea nivelului de maturitate al SecInf pentru planificarea sarcinilor de viitor; pot determina cu ușurință, vizual, cât de bine capacitățile organizației se aliniază cadrelor/reglementărilor de securitate comune și propriilor politici de securitate în baza diagramelor ce reflectă starea dorită și starea reală, de-facto și pot genera o foaie de parcurs pentru îmbunătățirea securității informației entității.

f. Platforma M3-SI permite **acumularea istoricului, evoluției controalelor și domeniilor de SecInf și a îmbunătățirilor incrementale**, care pot apărea în entitatea analizată ori de câte ori apare necesitatea, frecvența fiind impusă de cerințele afacerii;

g. Platforma M3-SI **permite analiza comparativă a maturității entităților tipice**, precum bănci, universități, spitale etc.

CONCLUZII FINALE ȘI RECOMANDĂRI

Simultan cu migrarea masivă a diverselor afaceri în spațiul cibernetic virtual global (e-educație, e-guvernare, e-distracții, jocuri electronice, e-comerț etc.) și creșterea conectivității la Internet, crește dependența de infrastructura TIC, **a crescut esențial și continuă să crească volumul informațiilor sensibile** care circulă pe Internet, **au crescut simțitor și amenințările, riscurile** aferente de SecInf prin folosirea informațiilor cu rea-intenție, furturi de identitate, fraudă, extorcare/stoarcere ilicită de bani și alte infracțiuni. Criminalitatea cibernetică rămâne a fi o amenințare perpetuă pentru interesele entităților, iar securitatea informației a devenit esențială, atât pentru persoane fizice și juridice, cât și pentru societate și stat în întregime, ca componentă semnificativă a securității naționale și regionale. Aceste concluzii au fost convingător demonstrate în teză prin analiza diverselor statistici și tendințe moderne ale SecInf/SC în *Introducere* și *Capitolul 1*, în special în *subcapitolul 1.3. Importanța, provocări și probleme majore de SecInf în activitatea bancară*.

În cadrul tezei a fost analizată **starea actuală a SecInf** în diferite entități, au fost identificate unele probleme, legate în principal de **complexitatea SecInf** și **multitudinea cadrelor de abordare**. Au fost analizate cadrul legal și principalele cerințe de SecInf, diverse cadre global recunoscute de abordare a SecInf cu scopul de a sinteza și justifica rolul și locul SMSI în cadrul entității *(subcapitolul 1.1, 1.2).*

Aportul de bază a primului capitol constă în elucidarea unor **probleme actuale** și **dificultăți majore** în abordarea SecInf, precum: *domeniul SecInf este continuă schimbare; amenințările cibernetice sunt în permanentă evoluție; angajații reprezentă o vulnerabilitate majoră, fiind impusă educația și conștientizarea continuă a personalului; entitățile utilizează o varietate de sisteme, rețele și aplicații, gestionarea, actualizarea constantă și securizarea cărora este relativ dificilă; lucrul de la distanță, utilizarea dispozitivelor mobile BYOD în cadrul organizației crește riscul de pierdere sau furt de date; entitățile trebuie să se asigure că sunt în concordanță cu reglementările privind SecInf, dar demonstrarea conformității este dificilă și costisitoare; ca urmare a subaprecierii semnificației SecInf și celor menționate mai sus, adesea bugetele unor entități pentru SecInf sunt restrânse și SecInf este încălcată, compromisă.*

În capitolul II au fost analizate diverse **cadre global recunoscute, principii și instrumente de abordare a SecInf** cu scopul de a sinteza și justifica un model integrator/o bază comună de cunoștințe, care să permită utilizarea tuturor celor mai bune practici. Printre cele mai bune practici global acceptate au fost examinate COBIT de la ISACA, ISO27k de la ISO, seria NIST SP 800.x, PCI DSS, abordarea bazată pe riscuri și altele.

Pentru a conserva confidențialitatea, integritatea și disponibilitatea informațiilor valoroase ale entității în condițiile în care acestea circulă nu doar în interiorul său, ci și în spațiul cibernetic, pe Cloud Computing, pe Internet și Web, **organizațiile trebuie să adopte noua paradigmă de abordare a SecInf prin prisma unui SMSI și instrumentelor de suport**, să implementeze diverse politici, proceduri, controlul accesului și monitorizarea activităților, gestionarea riscurilor, gestionarea accidentelor, conștientizarea și formarea continuă a personalului, investirea în soluții IDS, IPS, SIEM etc. Abordarea tehnică-tehnologică doar la nivel de criptare, autentificare, setări, configurări nu mai face față provocărilor moderne cauzate de dezvoltarea vertiginoasă TIC și de e-transformarea continuă a afacerilor prin migrarea acestora pe Internet și Web *(subcapitolul 2.1. Paradigme, principii și cadre de abordare a SecInf).*

Multe dintre diversele cadre analizate de abordare a SecInf prin prisma unui SMSI pot fi recomandate ca bază pentru lansarea SMSI, e.g. NIST SP 800.x, COBIT, ISO/IEC 27001:2022. Dar cel mai recomandat rămâne a fi ISO/IEC 27001:2022. Printre argumentele forte de implementare a unui SMSI bazat pe ISO/IEC 27001 sunt de menționat:

- Adoptarea SMSI în cadrul organizației oferă un mediu unic global recunoscut în care sunt îndeplinite toate cerințele de securitate a informației. Totodată, **SMSI conform ISO27k conține toate mecanismele necesare** pentru autocorectare și îmbunătățire.
- Standardele pereche ISO/IEC 27001↔ISO/IEC 27002 formează **baza universală a controalelor necesare pentru înțelegerea și gestionarea adecvată** și eficientă a riscurilor, activelor, resurselor informaționale valoroase pentru entități, indiferent de apartenența sectorului privat, public sau individual, mărime, localizare etc.
- **Standardele ISO27k** sunt de circulație internațională și **acoperă toate tipurile de entități**, indiferent de tip, mărime, industrie, specificând cerințe flexibile pentru implementarea, operarea, revizuirea, menținerea și îmbunătățirea continuă a SMSI.
- La moment, în afară de standardul formator de sistem ISO/IEC 27001, **familia ISO27 k conține cca 80 de standarde operaționale care acoperă tot spectrul de activități**, ghiduri și linii directoare privind implementarea, operarea, revizuirea, auditarea, menținerea și îmbunătățirea continuă a securității informației, inclusiv pentru industrii specifice, cum ar fi telecomunicații, sectorul bancar, sectorul energetic etc.

Evident, în funcție de țară, tradiții, preferințe, industrii, contexte specifice etc. vor fi utilizate și alte cadre de reglementare. De exemplu, seria de publicații speciale NIST SP 800.x este pe larg utilizată în toată lumea, nu doar în S.U.A. Și PCI DSS este utilizat în toată lumea în industria de plăți cu carduri. **Aceste standarde nu contravin standardelor ISO27k** sau altor bune

practici internaționale privind organizarea și monitorizarea SMSI, dar le **precizează** și completează pentru a spori nivelul de securitate a informației pentru anumite regiuni, industrii etc.

Produsele gen CIS Controls v.8, CIS Controls Self-Assessment Tool (CIS CSAT, 2022), Cybersecurity Maturity Model Certification v.1.02 (CMMC 1.2, 2020) și altele **pot simplifica esențial lansarea inițială rapidă a SMSI pentru asigurarea securității cibernetice**. Dar pentru certificarea SMSI oricum SecInf trebuie abordată conform ISO/IEC 27001:2022, iar **pentru urmărirea și gestionarea progresului SecInf este foarte utilă platforma M3-SI**.

Fiecare din abordările SecInf bazată pe risc, pe standarde de bune practici și pe modele de maturitate pot fi utilizate separat. Dar ele **nu se exclud una pe alta**; **mai degrabă sunt complementare** și **utilizarea lor comună permite sporirea nivelului de maturitate** a securității informației. În realitate multor entități le este greu să obțină o viziune unică, obiectivă, comprehensibilă a tuturor acestor abordări, este nevoie de mult timp, de competențe și expertize speciale, de care entitățile nu totdeauna dispun. **Complexitatea rămâne încă a fi un factor foarte important în realizarea unei viziuni unice și obiective a riscurilor și capacităților de SecInf.** Inclusiv și pentru că riscurile sunt în creștere continuă, cauzată de integrarea noilor aplicații TIC, de apariția noilor vulnerabilități, noilor amenințări, atacuri etc. Inclusiv și pentru că gestiunea riscurilor SecInf este un proces continuu. Inclusiv și de felul în care informațiile privind securitatea cibernetică sunt colectate, gestionate, raportate/difuzate către rolurile respective din entități pentru monitorizarea și suportul SecInf în timp real. Este extrem de dificilă nu doar colectarea de date și evaluarea SecInf, ci și actualizarea și păstrarea consistenței numeroaselor documente pentru obținerea unei imagini coerente asupra tuturor aspectelor securității informației și compararea și analiza evoluției în timp pentru o entitate și/sau compararea între entități etc. **Pentru combaterea acestor dificultăți poate di utilă platforma M3-SI.**

Aportul de bază al Capitolului doi **este orientarea spre M^{3}SI**, motivată de *cerințe complexe de SecInf/SC; multiple și diverse cadre de abordare cu multiple controale; instrumente; securitatea informației/securitatea cibernetică trebuie privită ca proces continuu într-un mediu în continuă schimbare al afacerilor, riscurilor, provocărilor; utilizarea bunelor practici standardizate și acceptate la nivel global este crucială pentru asigurarea securității informației/securității cibernetice.*

Ideea principală ce trebuie desprinsă de aici este că un standard național este bun, un standard european este mai bun iar un standard global este cel mai bun. Dar obligativitatea aplicării lor este tocmai inversă: aplicarea standardelor internaționale este benevolă, a celor europene de dorit, iar a celor naționale obligatorie. Și dacă abordarea SecInf bazată pe standardele de bune practici internaționale și instrumente general acceptate constituie abece-ul procesului, atunci

maturitatea constituie restul alfabetului în scenariul PDCA de măsurare, evaluare, analiză și îmbunătățire continuă a SecInf, indiferent de care standarde sunt utilizate la etapele inițiale de start, de începere a tratării SecInf.

Pentru depășirea multor dintre problemele și provocările menționate ale SecInf, în teză a fost propus și realizat **un cadru mixt** *(Capitolul III)* materializat în **modelul generic multiprofil M^{3}SI cu o aplicație-suport M3-SI de generare-administrare a bazei de cunoștințe**, **a profilurilor tipice industriei și individuale** de evaluare a maturității SecInf, **adecvate pentru gestionarea securității informațiilor** de-a lungul întreg ciclului de viață într-o entitate.

În esența sa platforma M^{3}SI este un prototip de SMSI pentru planificarea-evaluarea SecInf în baza **profilurilor tipice PSITI și profilurilor individuale PISI**, cu criterii prestabilite de evaluare. Arhitectural M^{3}SI reprezintă **o bază de date generică, cumulativă, adaptabilă și extensibilă** *(subcapitol 3.1,3.2)* privind cunoștințele despre cadrele de abordare, zonele, controalele, criteriile și țintele de SecInf, din care sunt generate profiluri tipice unor industrii PSITI (e.g. educație, sănătate, bănci), care, la rândul lor servesc ca bază pentru construirea/generarea de profiluri particulare PISI, bazându-se inclusiv și pe acumularea experienței entităților similare, cu profiluri similare. Profilurile PISI servesc pentru măsurarea proceselor SMSI și SecInf, permit adaptarea, îmbunătățirea lor continuă la mediul schimbător și alinierea la cerințele legale.

Pe de o parte, contextele interne și externe pot diferi esențial pentru diverse entități și, ca urmare, nu poate exista un singur model de evaluare a maturității. Fiecare model PISI urmărește propriile obiective și rezolvarea propriilor probleme în cadrul unor misiuni specifice. Pe de altă parte, este dificil să se aplice modele de maturitate personalizate fără a înțelege modelul de bază/enunțul general al problemei, profilurile tipice industriei și modurile de abordare. Concepute pentru a optimiza performanța securității unei entități într-un mediu global în continuă schimbare, modelul multiprofil M^{3}SI, profilurile tipice unor industrii PSITI, profilurile particulare PISI de evaluare a SecInf și aplicația aferentă, **oferă îndrumare și suport organizației pentru îmbunătățirea proceselor de SecInf,** inclusiv capacitatea de gestionare, dezvoltare, achiziționare și întreținere a controalelor, instrumentelor, produselor și serviciilor de SecInf.

Modelul M^{3}SI, profilul tipic PSITI și profilurile individuale PISI de evaluare a SecInf sunt susținute de o aplicație informatică originală, elaborată de autor *(subcapitol 3.3).*

Aplicația M3-SI permite **afișarea rezultatului evaluării în diagrame de tip radar, diagrame cu bare** și **linii**, la diferite niveluri de agregare/detaliere conform necesităților utilizatorului potrivite cu scopul măsurării maturități, precum urmărirea dinamicii în timp sau auditul intern de performanță sau pre-audit de certificare etc. *(subcapitol 3.4).*

Aplicația M^{3}SI posedă o serie de avantaje și caracteristici inovative, enumerate în concluziile la capitolul 3 *(subcapitol 3.5).*

Toate acestea fac gestionarea și asigurarea SecInf în cadrul entităților sau unor conglomerate de entități din același domeniu de activitate mai **transparentă, mai simplă și mai ușor de înțeles și de aplicat**; **ajută organizația la evaluarea nivelului de maturitate, la stabilirea priorităților de îmbunătățire și punerea în aplicare a acestor îmbunătățiri în contexte și procese specifice unei entități.**

Cu ajutorul M^{3}SI și instrumentului suport elaborat, **maturitatea poate fi evaluată sistematic și după necesitate,** mai larg și/sau mai concret, pentru a identifica, sesiza „punctele de plecare" și a aplica modelul la o gamă mai largă de sarcini, situații, inclusiv pentru a planifica schimbările într-un mod mai coordonat și mai rezonabil, inclusiv pentru a compara nivelurile de maturitate la diferite momente de timp și/sau nivelurile de maturitate ale diferitelor entități cu activități similare etc.

În realitate cele 5 niveluri de maturitate semnifică **etape de evoluție prin care trece și se maturizează un SMSI lansat**. Criteriile destinate pentru aprecierea (măsurarea-evaluarea) și/sau pentru îmbunătățirea continuă a SMSI, răspund atât propriilor nevoi și politici particulare de securitate a informației specifice organizației, cât și celor globale, stabilite în baza bunelor practici. Aplicația aferentă modelului M^{3}SI oferă suport inteligent de generare a profilurilor de evaluare consistentă pentru maturizarea SecInf prin îmbunătățirea continuă.

Abordarea **„model multiprofil – profil tipic industriei – profil particular specific entității"** și aplicația respectivă M3-SI de suport automatizat este utilă atât pentru rolurile specifice de securitate, care trebuie să fie la curent cu starea actuală, să întrețină documentele necesare, să asigure raportarea/informarea, cât și pentru toți cei care au nevoie de acces la informațiile de securitate, precum auditori, inspectori.

Implementarea rezultatelor. Modelul elaborat M^{3}SI și aplicația de suport-instrumental au fost implementate în BNM *(a se vedea Actul de implementare, Anexa 1),* cu ilustrarea practică pentru o bancă ipotetică „Alfa", deoarece ilustrarea în baza unei bănci reale ar fi încălcat SecInf pentru acea entitate. Dar M^{3}SI și aplicația aferentă **pot fi aplicate în mod direct** pentru orice bancă din RM, cu adaptarea necesară a profilurilor PISI, inclusiv și pentru ortice alte industrii și entități cu adaptarea BD și/sau a profilurilor PSITI și PISI.

Potențialele direcții viitoare de cercetare se referă la **colaborarea M^{3}SI cu alte modele și instrumente similare**, gen CIS Controls v8, CIS CSAT etc., pornind de la actualizarea controalelor, cartografierii cadrelor și terminând cu importul/exportul de date în/din M3-SI și afișarea rapoartelor integrate și detaliate obținute din datele asociate, îmbogățirea bazei de cunoștințe și altele.

BIBLIOGRAFIE

Toate sursele web, inclusiv din textul tezei, au fost verificare la data de 28.02.2024.

[1] FLECK, A. *Cybercrime expected to skyrocket in coming years. Dec 2, 2022.* Available at: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

[2] BRAGARU, T., **BRICEAG, V.,** MALCOCI, V., GALAICU V. (2019). *Securitatea informației vis-a-vis de securitatea informațională.* Revista Studia Universitatis Moldaviae, 2(122), seria „Științe exacte și economice", CEP USM, 2019, pp. 38-47. ISSN 1857-2073; ISSN online 2345-1033

[3] *ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary*

[4] *ISO/IEC 27032:2023 Cybersecurity – Guidelines for Internet security*

[5] **BRICEAG, V.,** BRAGARU, T. *Evaluarea riscului securității cibernetice.* Revista Economica, 2(122), SEP ASEM, 2021, pp. 138-147. ISSN 1810-9136

[6] **BRICEAG, V.** *Model Multiprofil de Maturitate a Securității Informației (M3SI).* Revista Română de Informatică și Automatică (RRIA), ISSN 1220-1758, vol. 32, nr. 1, pp. 99-112. ICI București, 2022. Disponibil la: https://rria.ici.ro/en/vol-32-no-1-2022. ISSN 1220-1758

[7] BRAGARU, T., **BRICEAG, V.** *Evaluarea securității informației organizației în baza unui model de maturitate*. IN: Materialele conferinței științifice-practice internaționale „Teoria și practica administrării publice", Chișinău, AAP, 22 mai 2020, pp.248-252. ISBN 978-9975-3240-9-0

[8] The Open Group. *Open Information Security Management Maturity Model (O-ISM3, 2017), Version 2.0.* Available at: https://www.opengroup.org/forum/security/infosecmanagement/

[9] MILOSLAVSKAYA, N., TOLSTAYA, S. *Information Security Management Maturity Models.* 2022 Annual International Conference on Brain-Inspired Cognitive Architectures for Artificial Intelligence: The 13th Annual Meeting of the BICA Society. 2022, Procedia Computer Science 213 (2022) 49–57. Available at: www.sciencedirect.com

[10] RABII, A., ASSOUL, S., OUAZZANI TOUHAMI, K., ROUDIES, O. *Information and Cyber Security Maturity Models: A Systematic Literature Review*. Inf. Comput. Secur. 2020, 28, pp. 627–644.

[11] *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements*

[12] *SM ISO 690:2022 – Information and documentation – Guidelines for bibliographic references and citations to information resources* (identic cu standardul internațional ISO 690:2021(E))

[13] *Recomandări cu privire la obiectivele de control și măsurile de securitate ale SMSI.* Aprobate de Guvernatorul BNM în 2010 cu modificări din 01.07.2015. Disponibil la: https://www.bnm.md/ro/content/recomandari-cu-privire-la-obiectivele-de-control-si-masurile-de-securitate-ale-sistemului-de

[14] *Lege Nr. LP133/2011 din 08.07.2011 privind protecția datelor cu caracter personal, adoptată de Parlamentul RM, cu modificări LP52 din 12.03.20.* MO84/14.03.20 art.88; în vigoare din 14.03.2020

[15] *Regulamentul General privind Protecția Datelor (GDPR) nr. 2016/679.* Aprobat de Parlamentul European și Consiliul UE din 27 aprilie 2016, aplicabil din 25 mai 2018. Disponibil la: https://gdpr-info.eu/

[16] *Legea cu privire la BNM nr. 548-XIII din 21.07.1995.* În vigoare din 12.10.1995, cu modificări ulterioare prin Legea Nr. LP32/2020 din 27.02.2020. În vigoare din 02.04.2020

[17] *Legea privind activitatea băncilor nr.202 din 06 octombrie 2017.* În vigoare din 01.01.2018

[18] *Regulament cu privire la sistemele de control intern în bănci.* Aprobat de BNM prin Hotărârea nr. HBN96/2010 din 30.04.2010, cu modificări din 01.07.2017, în baza Hotărârii BNM Nr. HBN146 din 07.06.17

[19] *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls*

[20] *The Complete Guide to PCI-DSS 4.0.* Available at: https://colortokens.com/blog/pci-dss-4-0/

[21] *Securitizare.* Accesibil https://asfromania.ro/en/a/943/securitizare/

[22] CURRAS, E. *Information as the fourth vital element and its influence on the culture of peoples.* Journal of Information Science, vol. 13, 3: pp. 149-157. First Published Jun 1, 1987.

[23] BRAGARU, T. *Dezvoltarea și implementarea sistemului de management al securității informației (în baza ISO/IEC 27001).* USM, 2021, Tipogr. „Foxtrot", 113 p. ISBN 978-9975-89-204-9

[24] *Okinawa Charter on Global Information Society.* Okinawa, G8, 2000. Available at: https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html/

[25] *Ransomware Report: Latest Attacks and News*. Available at: https://cybersecurityventures.com/ransomware-report/

[26] MD HARIS UDDIN SHARIF, MEHMOOD ALI MOHAMMED. *A literature review of financial losses statistics for cyber security and future trend. 2022.* Available at: https://www.researchgate.net/publication/362363620/].

[27] Verizon Reports. *DBIR 2023 data breach investigations report.* Available at: https://www.verizon.com/business/ resources/Tbf7/reports/2023-data-breach-investigations-report-dbir.pdf

[28] *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks*

[29] Compendiu de audit. *Securitatea* cibernetică în UE și în statele membre ale acesteia. Disponibil la: https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_RO.pdf/

[30] CIS Controls Version 8. (CIS/SANS TOP 20 Security Controls) Available at: https://www.cisecurity.org/controls/v8/?utm_source=website&utm_medium=email&utm_campaign=v8_release/

[31] CIS Controls Self-Assessment Tool or CIS CSAT. Available at: https://csat.cisecurity.org

[32] Cybersecurity Maturity Model Certification v.1.02 (2020). (CMMC 1.2, 2020). Available at: https://www.acq.osd.mil/cmmc/draft.html/

[33] *Standards by ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection.* Available at: https://www.iso.org/committee/45306/x/catalogue/

[34] ISO27k. *About the ISO27k standards.* Available at: https://www.iso27001security.com/html/iso27000.html/

[35] *COBIT® 2019 Framework: Governance and Management Objectives*. ISACA, 2019. -300 p. Available at: https://www.iso27001security.com/html/iso27000.html

[36] National Institute of Standards and Technologies. *Special Publication 800 series, Computer security.* Available at: https://csrc.nist.gov/publications/sp800

[37] *Cybersecurity Maturity Model Certification v.2.0, 2021*. Available at: https://www.itgovernance.co.uk/cybersecurity-maturity-model-certification?promo_name=megamenu-cybersecurity&promo_id=info-cmmc

[38] MALIK SALEH. *Information Security Maturity Model.* Available at: https://www.researchgate.net/publication/216462795

[39] MUNEER, A. et al. *A Balanced Information Security Maturity Model Based on ISO/IEC 27001:2013 and O-ISM3. International Journal of Innovative Science and Research Technology, Volume 8, Issue 6, June, 2023, p.2444-2450. ISSN No: 2456-2165*

[40] КОЛОМЫЦЕВ, М., НОСОК, С., ТОЦКИЙ, Р. *Сравнительный анализ моделей оценки зрелости*. Наукові журнали Національного Авіаційного Університету, Захист інформації, том 21, №4, жовтень-грудень 2019. Стр. 224-232. DOI: 10.18372/2410-7840.21.14337

[41] *ISO 9001:2015/EN 29000. Quality management systems. Requirements*

[42] *Cybersecurity Maturity Model Certification Guide (CMMC, 2022). Available at:* https://www.varonis.com/blog/cmmc-compliance/

[43] MAYFIELD, R., CVITANIC, J. *Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information Security*. Information Systems Control Journal, 2, 2001, ISACA. p. 32-35.

[44] *NIST SP 800-53 rev.5, 2020.* Available at: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[45] *NIST 800-207 Zero Trust Architecture, 2020.* Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[46] *ISO/IEC 27003:2017 Information technology – Security techniques – Information security management systems – Guidance*

[47] *ISO/IEC 27004:2016 Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation*

[48] *ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing*

[49] *List of ISO standards 28000–29999.* Available at: https://en.wikipedia.org/wiki/List_of_ISO_standards_28000%E2%80%9329999/

[50] *Zero Trust Core Principles.* Document No.: W210, The Open Group, 2021 (W210, 2021). Available at: https://pubs.opengroup.org/security/zero-trust-principles

[51] *ISO/IEC 27017:2015 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

[52] *ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*

[53] *ISO/IEC 27033 Information technology – Network security, part 1-7: , Part 1: Overview and concepts 2015; Part 2: Guidelines for the design and implementation of network security, 2012; Part 3: Reference networking scenarios – Threats, design techniques and control issues, 2010; – Part 4: Securing communications between networks using security gateways, 2014; Part 5: Securing communications across networks using Virtual Private Networks*

(VPNs), 2013; Part 6: Securing wireless IP network access, 2016; Part 7: Guidelines for network virtualization security, 2023

[54] **BRICEAG, V.** Intelligent support for assessing the level of maturity of information security. International Conference „Mathematics & Information Technologies: Research and Education" (MITRE - 2021). Abstracts. Chişinău: CEP USM, 2021. ISBN 978-9975-158-19-0. -p.94. Available at: https://ibn.idsi.md/vizualizare_articol/134317

[55] BRAGARU, T., **BRICEAG, V.** Sustainable cybersecurity training for modern society. Sustainable cybersecurity training for modern society. Proceeding of International Teleconference of young researchers "Creating the Society of Consciousness" (TELE-2022), 11th Edition, 18-19 March 2022. ARA Journal of Sciences, Nr. 5, 2022, pp.30-41. ISSN: 0896-1018. Available at: https://www.americanromanianacademy.org/_files/ugd/754172_0c407fa356a04c2a8a000f6a3f92bae8.pdf

[56] BRAGARU, T., **BRICEAG, V.** Sustainable cybersecurity training for modern society. The thesis of International teleconference of young researchers "Creating the Society of Consciousness" (TELE-2022), 11th Edition of 18-19 March 2022. Society. Consciousness. Computer. Volume 8 (2022). Editorial Office "Vasile Alecsandri University of Bacău", Romania, Bacău, 2022, p.32. ISSN 2359-7321. Available at: *https://ibn.idsi.md/vizualizare_articol/179237*

[57] **BRICEAG, V.**, BRAGARU, T. Sustainable Curricular assurance of the information security management course. International Conference „Mathematics & Information Technologies: Research and Education" (MITRE - 2021). Abstracts. Chişinău: CEP USM, 2021, -p.118. ISBN 978-9975-158-19-0

[58] PĂUNESCU, M. *COSO Model for* Internal *Control (I) and (II).* Available at: *https://www.ceccarbusinessreview.ro/search/coso/filter-titlu/strict/*

[59] *Complete Guide to ITIL 4 Framework.* Available at: https://www.freshworks.com/freshservice/itil/itil-4

[60] *ISO/IEC 20000-1:2018(en) Information technology – Service management – Part 1: Service management system requirements*

[61] *ISO 31000:2018(en) Risk management – Guidelines*

[62] *ISO 22301:2019/Amd 1:2024 Security and resilience – Business continuity management systems – Requirements*

[63] [NIST SP 1800]. NIST SP 1800. Cybersecurity practice guides. Available at: https://csrc.nist.gov/publications/sp1800/

[64] IEC 31010:2019 Risk management – Risk assessment techniques

[65] *Website Hacking Statistics You Should Know in 2020 (+in 2022).* Available at: https://www.webarxsecurity.com/website-hacking-statistics-2018-february/ https://patchstack.com/articles/website-hacking-statistics/

[66] MILKOVICH, Devon. 15 Alarming Cyber Security Facts and Stats. Available at: https://www.cybintsolutions.com/cyber-security-facts-stats/

[67] Webroot Reports 2019. Hook, line and sinker: Why phishing scams work. Available at: https://www.webroot.com/in/en/about/press-room/releases/employees-click-phishing-emails-atwork

[68] Diogo, P., José, B. (2018). Information Security Management Systems – A Maturity Model based on ISO/IEC 27001. In book: Business Information Systems, 2018, pp.102-114

[69] GOEL, I. Cybersecurity: A Shared Responsibility. Available at: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-39/cybersecurity-a-shared-responsibility?cid=edmi_3000179&Appeal=edmi&utm_source=sfmc&utm_medium=email&utm_campaign=AtISACA_20211124&utm_term=article-cyber-shared-responsibility&utm_id=154374&sfmc_id=97796656/

[70] Bilge, Y. O., Sonny van Lingen & Marco, S. (2021). The Cybersecurity Focus Area Maturity (CYSFAM), 2021. Available at: www.mdpi.com/journal/jcp.

[71] Amenințări generice la adresa securității cibernetice, ENISA (2020). Disponibil la: https://dnsc.ro/vezi/document/amenintari-generice-securitate-cibernetica/

[72] CVE (Common Vulnerabilities and Exposures, 2021). Available at: https://cve.mitre.org/

[74] 2022 Top Routinely Exploited Vulnerabilities. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a /

[74] *Cybersecurity Capability Maturity Model (C2M2, version 2.1, 2022).* Available at: https://c2m2.doe.gov/C2M2%20Version%202.1%20June%202022.pdf

[75] ISO/IEC TS 27100:2020 Information technology – Cybersecurity – Overview and concepts

[76] ISO/IEC TS 27110:2021 Information technology, cybersecurity and privacy protection – Cybersecurity framework development guidelines

[77] ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection – Governance of information security

[78] PCI DSS Certification. Available at: https://www.imperva.com/learn/data-security/pci-dss-certification/

[79] 239 Cybersecurity Statistics (2023). Available at: https://www.packetlabs.net/posts/239-cybersecurity-statistics-2023/

[80] Cele mai bune teste antivirus gratuite 2024. Disponibil la: https://top10programeantivirus.com/cel-mai-bun-antivirus-gratuit/

[81] *What is SIEM, Why is it important and how does it work?* Available at: https://www.exabeam.com/explainers/siem/what-is-siem/

[82] *SIEM Tools: Top 6 SIEM Platforms, Features, Use Cases and TCO.* Available at: https://www.exabeam.com/explainers/siem-tools/siem-buyers-guide/

[83] *Free assessment of your cyber security defences.* Available at: https://www.itgovernance.co.uk/free-assessment-of-your-cyber-security-defences

[84] *The NIST Cybersecurity Framework (CSF) 2.0 (2024).* Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf/

[85] *Gartner Magic Quadrant.* Available at: *https://www.gartner.com/en/research/methodologies/magic-quadrants-research*

[86] BRAGARU, T. *Auditul sistemului de management al securității informației.* USM, 2021, Tipogr. „Foxtrot", 110 p. ISBN 978-9975-89-203-2

[87] *Cum se efectuează un audit de securitate cibernetică: un ghid în 3 pași (XONTECH, 2023).* Disponibil la: https://xontech.md/news/cum-se-efectueaza-un-audit-de-securitate-cibernetica-un-ghid-in-3-pasi/

[88] *Open Web Application Security Project (OWASP).* Available at: https://www.techtarget.com/searchsoftwarequality/definition/OWASP/

[89] *ISO 27001 Implementation Guide: Checklist of Steps, Timing, and Costs involved.* Available at: *https*://advisera.com/27001academy/knowledgebase/iso-27001-implementation-checklist

[90] *ISO 27001 certification - Everything you need to know about getting ISO 27001 certified.* Available at: https://advisera.com/27001academy/iso-27001-certification/

[91] *Regulamentului cu privire la cardurile bancare din 24.02.2005, cu modificări HBN19 din 31.01.13. Disponibil la: http://lex.justice.md/document_rom.php?id=518876C0:64AFD799*

[92] *Regulamentului privind cerințele minime pentru Sistemele Informaționale și de Comunicare ale Băncilor, aprobat prin HCE al BNM nr.47 din 14 martie 2018.* Disponibil la: https://www.bnm.md/ro/content/regulament-privind-cerinte-minime-pentru-sistemele-informationale-si-de-comunicare-ale

[93] Peter F. Drucker. *The Effective Executive: The Definitive Guide to Getting the Right Things Done", 2006.* Available at: https://dtleadership.my/wp-content/uploads/2019/05/Drucker-2006-The-Effective-Executive-The-Definitive-Guide-to-Getting-the-Right-Things-Done.pdf

ANEXE

Anexa 1. Act de implementare a rezultatelor tezei

Banca Națională a Moldovei

Act de implementare

Stimate Domnule / Stimată Doamnă

Prezentul act atestă faptul că aplicația "M3SI – Model Multi-profil de Măsurare a Nivelului de Maturitate a Sistemului de Management al Securității Informației" dezvoltată de dl Briceag Valentin este implementată în regim pilot în cadrul Băncii Naționale a Moldovei, Direcția Managementul Continuității Activității, Securității Informației și Supraveghere în TI. Această aplicație este folosită in cadrul misiunilor de control la Băncile Comerciale din Republica Moldova și a misiunilor de audit în cadrul BNM. Identificarea cerințelor pentru aplicație au fost elaborate de către dl Briceag Valentin împreună cu angajații responsabili de implementare din cadrul BNM.

Totodată BNM interzice divulgarea și partajarea datelor folosite în aplicație care ar putea duce la identificarea Băncilor Comerciale. Se permite doar anonimizare și modificarea datelor statistice în scop demonstrării al funcționalului aplicației M3SI.

Cu respect,

BANCA NAȚIONALĂ A MOLDOVEI SECRETARIAT GENERAL

Victor CIUBOTARU
Șef de direcție, Direcția Managementul Continuității Activității, Securității Informației și Supraveghere în TI

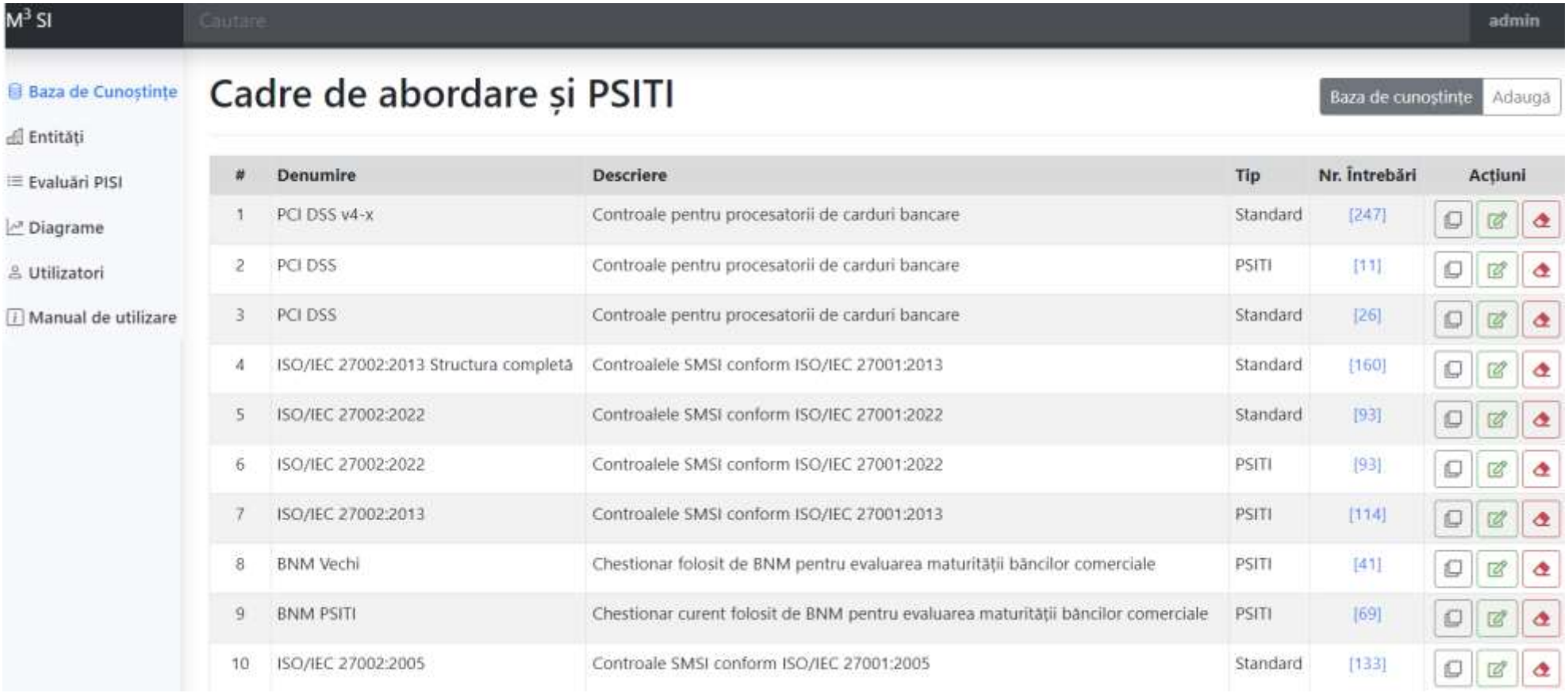
Ștefan DĂNILĂ
Șef-adjunct de direcție, Direcția Managementul Continuității Activității, Securității Informației și Supraveghere în TI

Tel.: +373 69 194121
E-mail: victor.ciubotaru@bnm.md
Tel.: +373 69 040677
E-mail: stefan.danila@bnm.md

Adresa: Bulevardul Grigore Vieru nr. 1,MD-2005, Chișinău, Republica Moldova
Tel: (+373) 22 822 606, Fax: (+373) 22 220 591, email: official@bnm.md, web: www.bnm.md

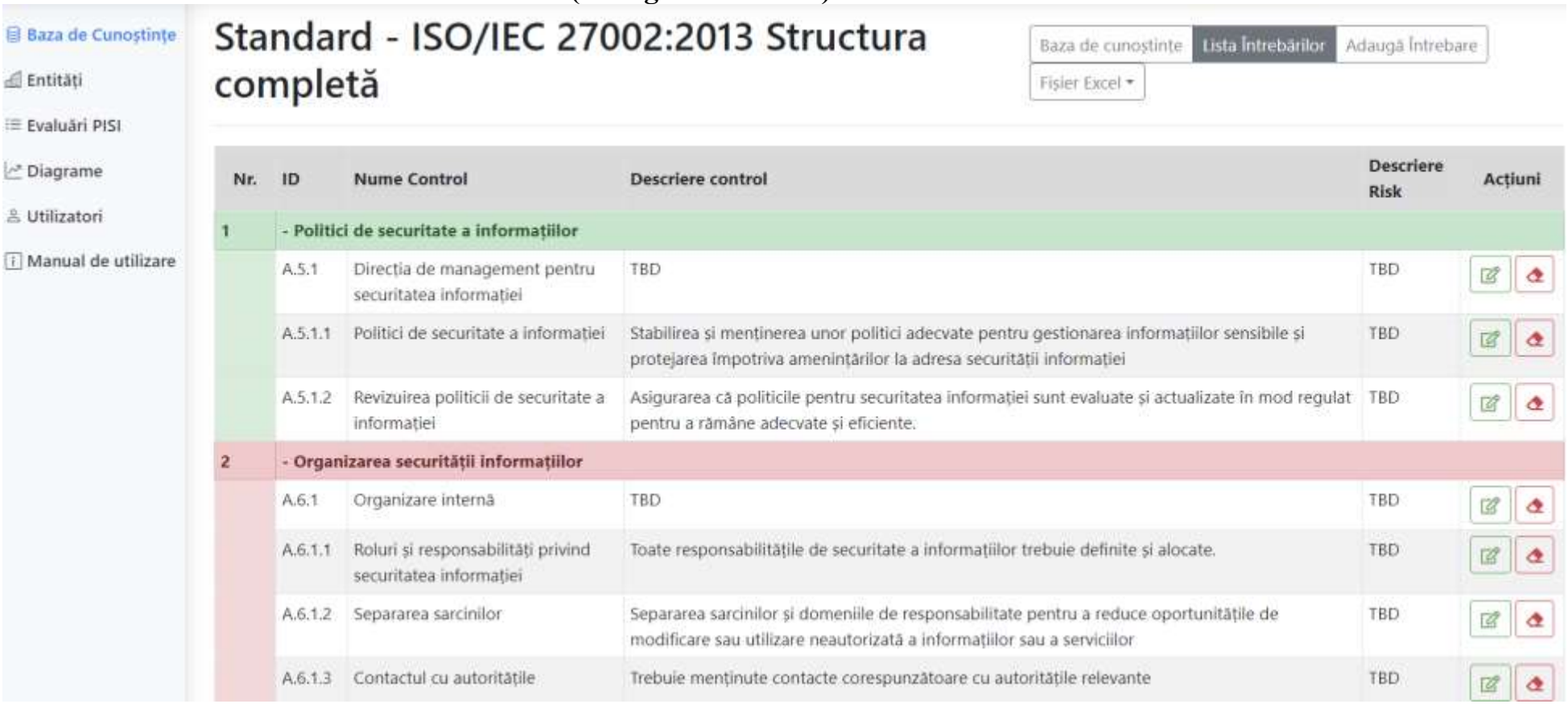
Anexa 2. Capturi de ecran cu ilustrarea funcțiilor aplicației M3-SI

A2.1. Lista cadrelor de abordare și a modelelor PSITI



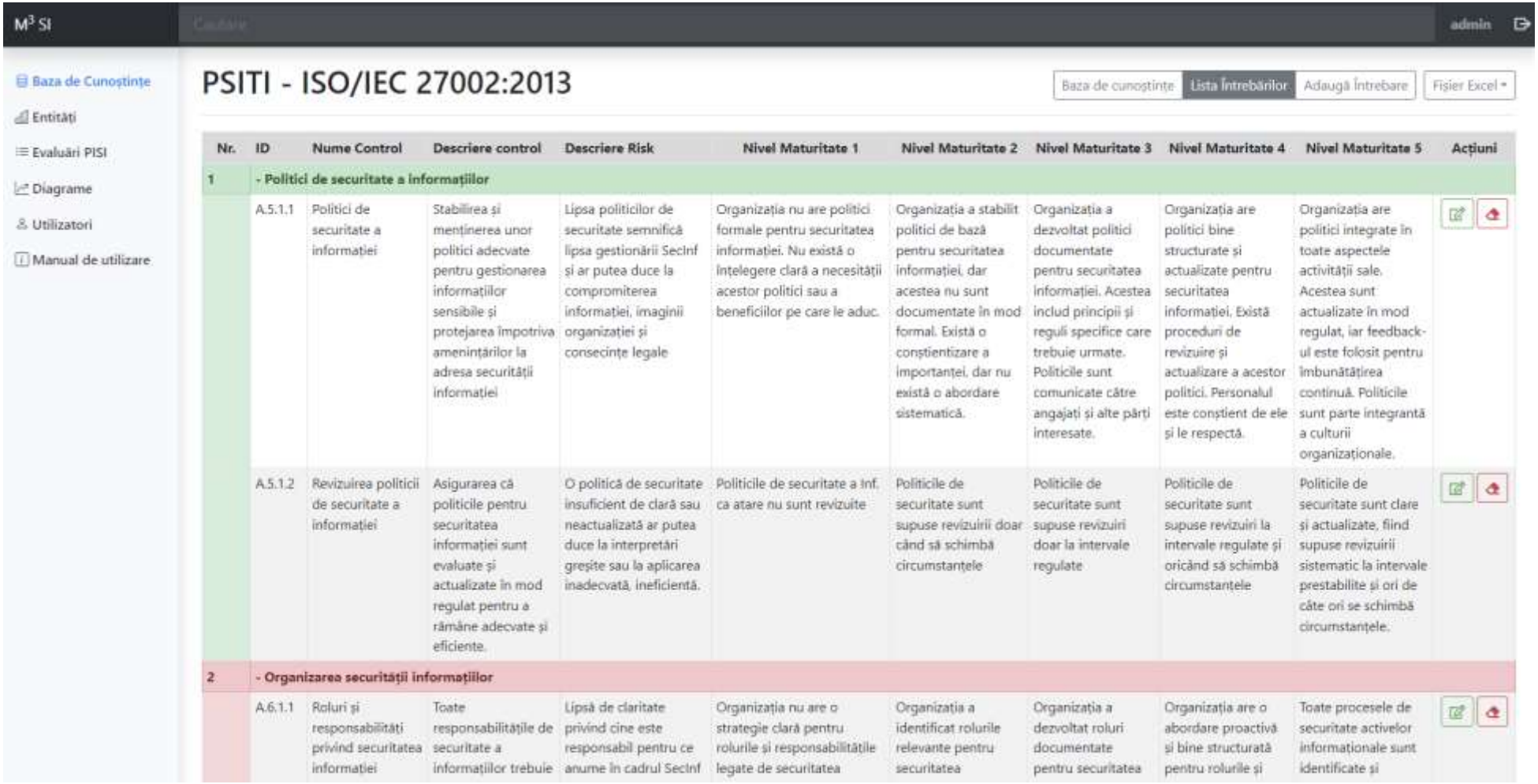
#	Denumire	Descriere	Tip	Nr. Întrebări	Acțiuni
1	PCI DSS v4-x	Controale pentru procesatorii de carduri bancare	Standard	[247]	
2	PCI DSS	Controale pentru procesatorii de carduri bancare	PSITI	[11]	
3	PCI DSS	Controale pentru procesatorii de carduri bancare	Standard	[26]	
4	ISO/IEC 27002:2013 Structura completă	Controalele SMSI conform ISO/IEC 27001:2013	Standard	[160]	
5	ISO/IEC 27002:2022	Controalele SMSI conform ISO/IEC 27001:2022	Standard	[93]	
6	ISO/IEC 27002:2022	Controalele SMSI conform ISO/IEC 27001:2022	PSITI	[93]	
7	ISO/IEC 27002:2013	Controalele SMSI conform ISO/IEC 27001:2013	PSITI	[114]	
8	BNM Vechi	Chestionar folosit de BNM pentru evaluarea maturității băncilor comerciale	PSITI	[41]	
9	BNM PSITI	Chestionar curent folosit de BNM pentru evaluarea maturității băncilor comerciale	PSITI	[69]	
10	ISO/IEC 27002:2005	Controale SMSI conform ISO/IEC 27001:2005	Standard	[133]	

A2.2. Editarea unui cadru de abordare (de regulă standard)



Nr.	ID	Nume Control	Descriere control	Descriere Risk	Acțiuni
1	- Politici de securitate a informațiilor				
	A.5.1	Direcția de management pentru securitatea informației	TBD	TBD	
	A.5.1.1	Politici de securitate a informației	Stabilirea și menținerea unor politici adecvate pentru gestionarea informațiilor sensibile și protejarea împotriva amenințărilor la adresa securității informației	TBD	
	A.5.1.2	Revizuirea politicii de securitate a informației	Asigurarea că politicile pentru securitatea informației sunt evaluate și actualizate în mod regulat pentru a rămâne adecvate și eficiente.	TBD	
2	- Organizarea securității informațiilor				
	A.6.1	Organizare internă	TBD	TBD	
	A.6.1.1	Roluri și responsabilități privind securitatea informației	Toate responsabilitățile de securitate a informațiilor trebuie definite și alocate.	TBD	
	A.6.1.2	Separarea sarcinilor	Separarea sarcinilor și domeniile de responsabilitate pentru a reduce oportunitățile de modificare sau utilizare neautorizată a informațiilor sau a serviciilor	TBD	
	A.6.1.3	Contactul cu autoritățile	Trebuie menținute contacte corespunzătoare cu autoritățile relevante	TBD	

A2.3. Editarea unui model PSITI

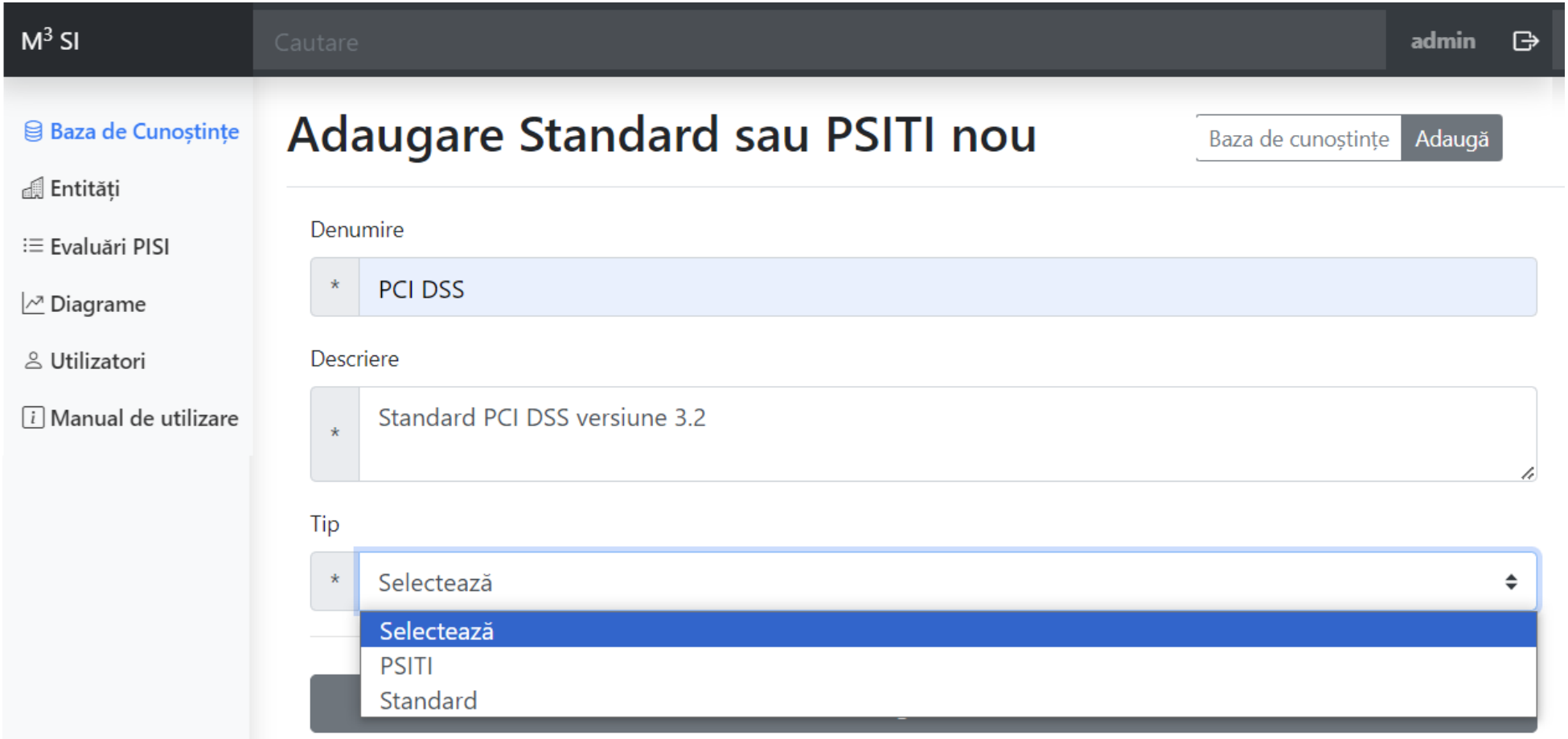


Nr.	ID	Nume Control	Descriere control	Descriere Risk	Nivel Maturitate 1	Nivel Maturitate 2	Nivel Maturitate 3	Nivel Maturitate 4	Nivel Maturitate 5	Acțiuni
1	- Politici de securitate a informațiilor									
	A.5.1.1	Politici de securitate a informației	Stabilirea și menținerea unor politici adecvate pentru gestionarea informațiilor sensibile și protejarea împotriva amenințărilor la adresa securității informației	Lipsa politicilor de securitate semnifică lipsa gestionării SecInf și ar putea duce la compromiterea informației, imaginii organizației și consecințe legale	Organizația nu are politici formale pentru securitatea informației. Nu există o înțelegere clară a necesității acestor politici sau a beneficiilor pe care le aduc.	Organizația a stabilit politici de bază pentru securitatea informației, dar acestea nu sunt documentate în mod formal. Există o conștientizare a importanței, dar nu există o abordare sistematică.	Organizația a dezvoltat politici documentate pentru securitatea informației. Acestea includ principii și reguli specifice care trebuie urmate. Politicile sunt comunicate către angajați și alte părți interesate.	Organizația are politici bine structurate și actualizate pentru securitatea informației. Există proceduri de revizuire și actualizare a acestor politici. Personalul este conștient de ele și le respectă.	Organizația are politici integrate în toate aspectele activității sale. Acestea sunt actualizate în mod regulat, iar feedback-ul este folosit pentru îmbunătățirea continuă. Politicile sunt parte integrantă a culturii organizaționale.	
	A.5.1.2	Revizuirea politicii de securitate a informației	Asigurarea că politicile pentru securitatea informației sunt evaluate și actualizate în mod regulat pentru a rămâne adecvate și eficiente.	O politică de securitate insuficient de clară sau neactualizată ar putea duce la interpretări greșite sau la aplicarea inadecvată, ineficientă.	Politicile de securitate a Inf. ca atare nu sunt revizuite	Politicile de securitate sunt supuse revizuirii doar când să schimbă circumstanțele	Politicile de securitate sunt supuse revizuiri doar la intervale regulate	Politicile de securitate sunt supuse revizuiri la intervale regulate și oricând să schimbă circumstanțele	Politicile de securitate sunt clare și actualizate, fiind supuse revizuirii sistematic la intervale prestabilite și ori de câte ori se schimbă circumstanțele.	
2	- Organizarea securității informațiilor									
	A.6.1.1	Roluri și responsabilități privind securitatea informației	Toate responsabilitățile de securitate a informațiilor trebuie	Lipsă de claritate privind cine este responsabil pentru ce anume în cadrul SecInf	Organizația nu are o strategie clară pentru rolurile și responsabilitățile legate de securitatea	Organizația a identificat rolurile relevante pentru securitatea	Organizația a dezvoltat roluri documentate pentru securitatea	Organizația are o abordare proactivă și bine structurată pentru rolurile și	Toate procesele de securitate activelor informaționale sunt identificate și	

A2.4. Editarea unei întrebări a unui model PSITI

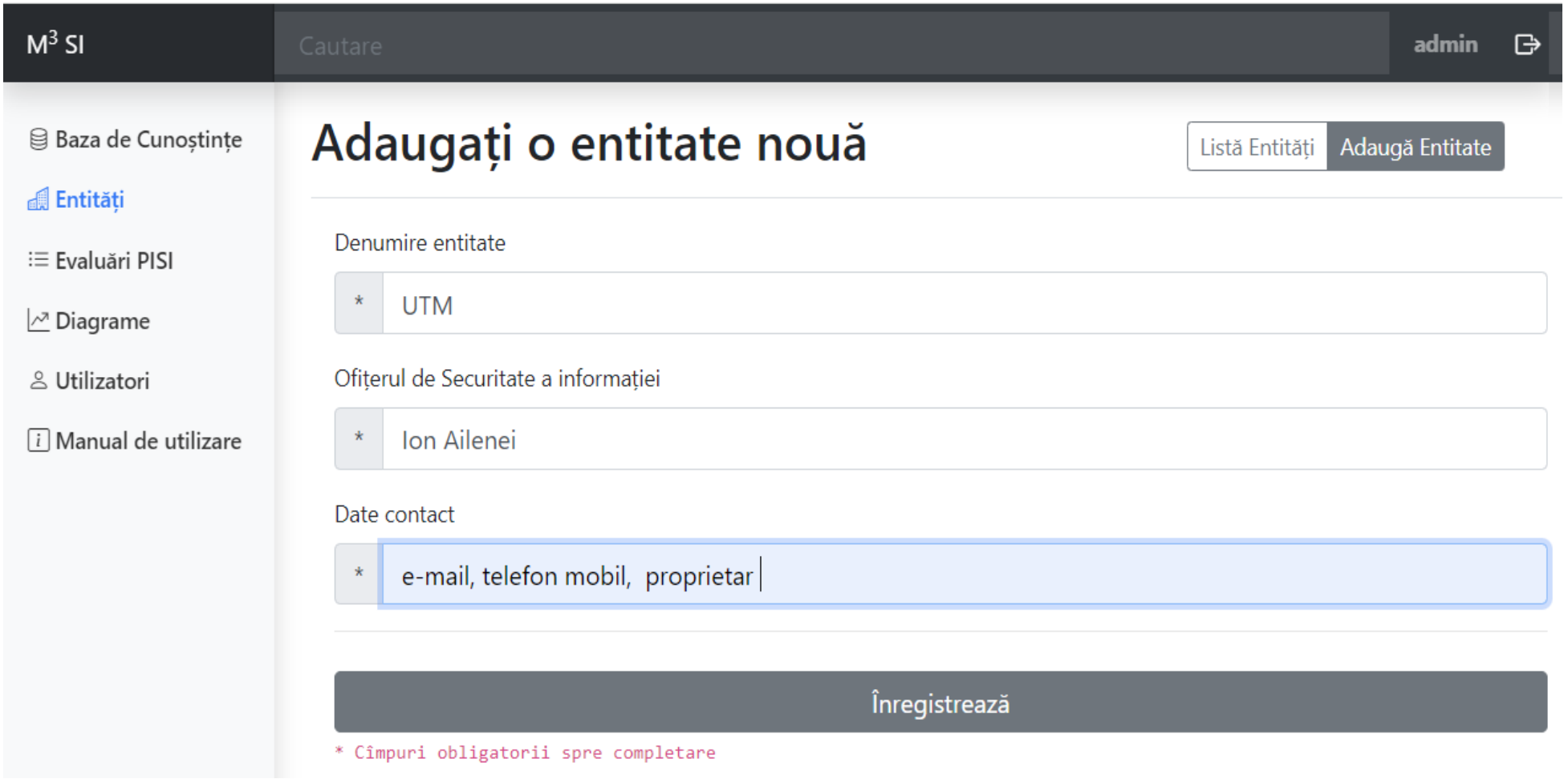
A2.5. Ștergerea unui cadru de abordare și/sau PSITI (operarea este similară)

A2.6. Adăugarea unui cadru de abordare și/sau PSITI (operarea este similară)



A2.7. Lista entităților

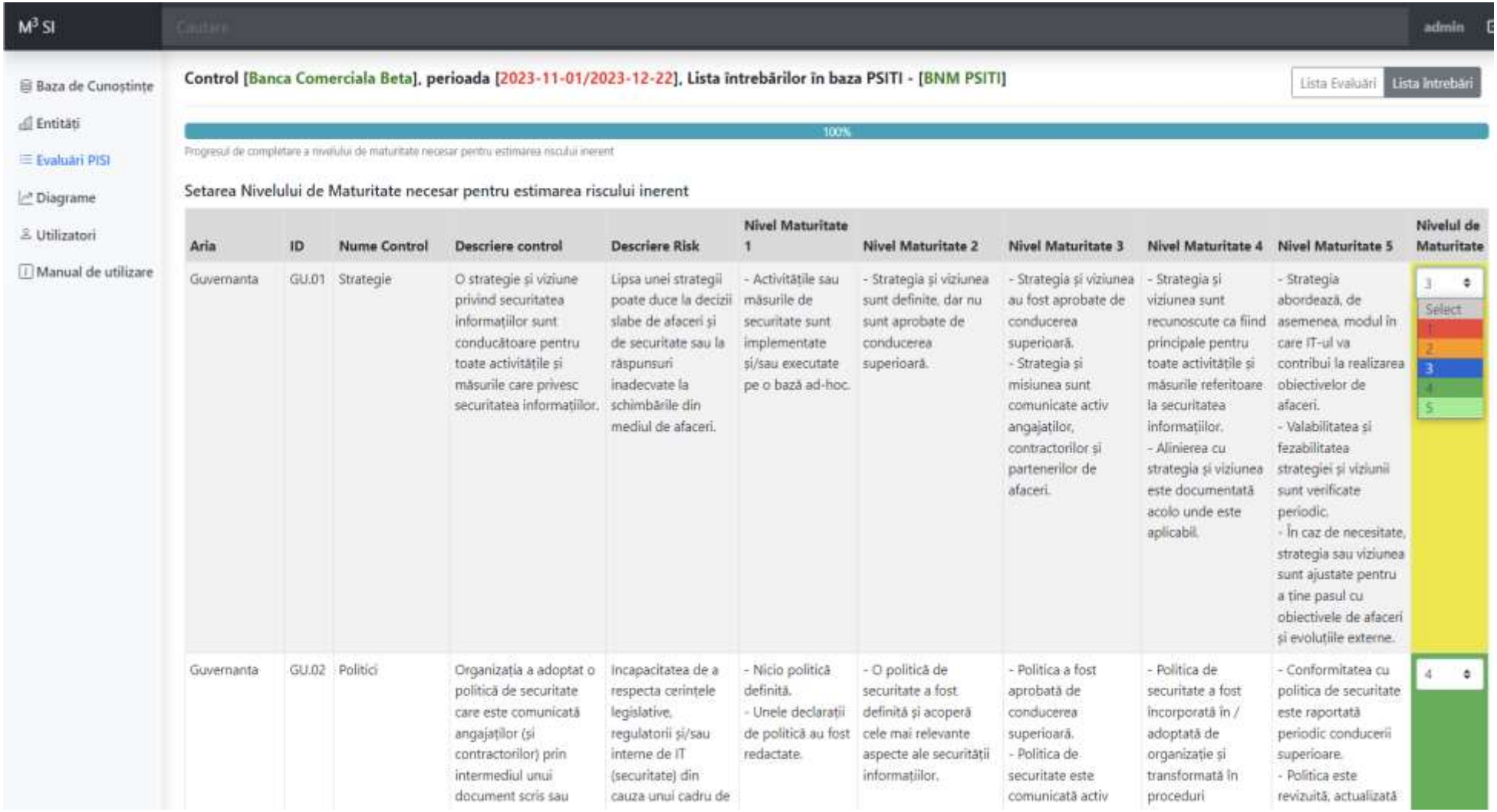
A2.8. Adăugarea unei entități noi



A2.9. Lista evaluărilor (realizate și/sau planificate)

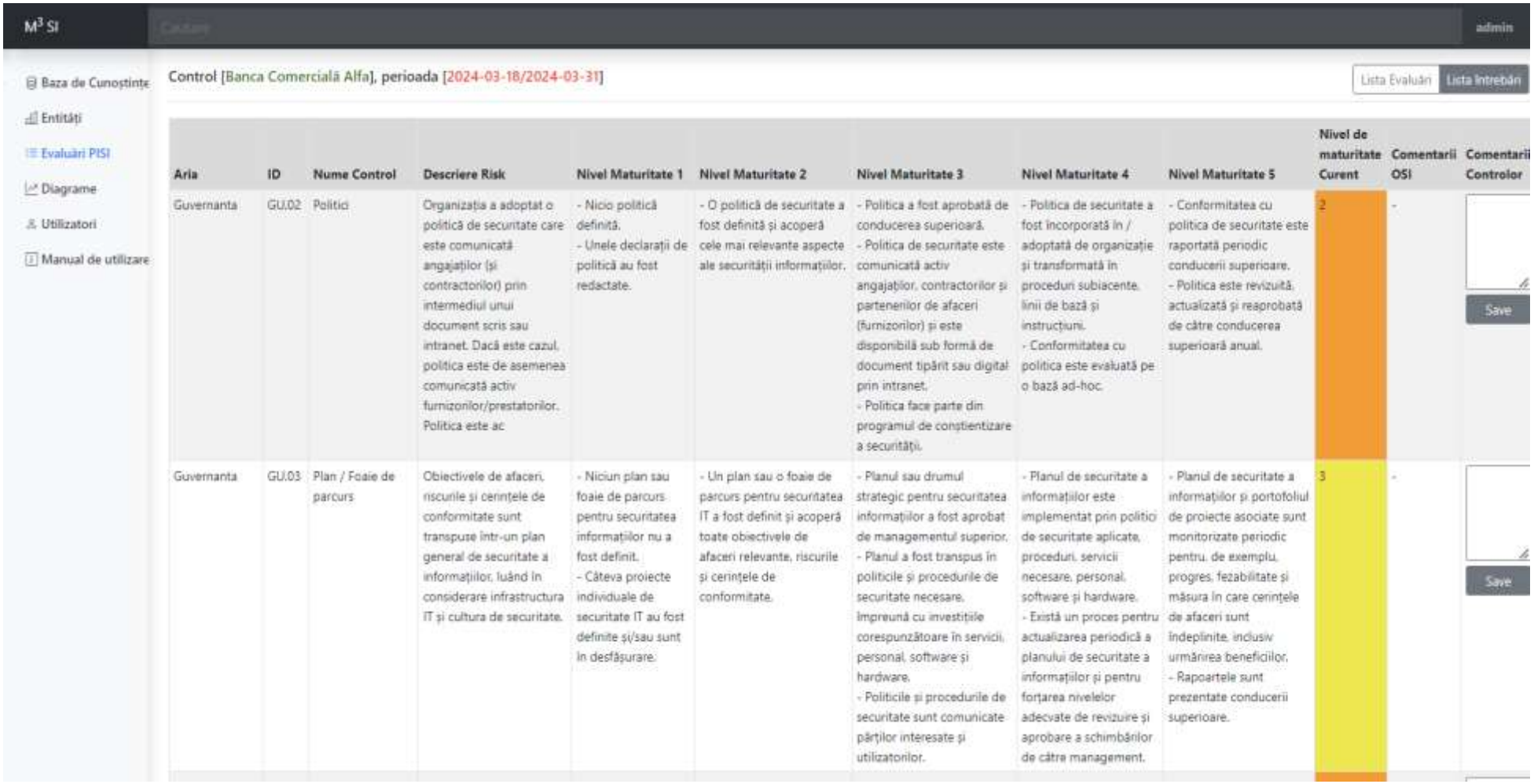
#	Entitate	PSITI/Standard	Nr. Intrebari	Perioada desfășurării controlului	Nivelul mediu așteptat	Nivelul mediu curent	Riscuri inerent	Actiuni
1	Banca Comercială Alfa	BNM PSITI	[69]	2024-04-01 - 2024-04-30	0.2	1.5	[3]	Completează
2	Universtitatea de Stat din Moldova	ISO/IEC 27002:2013	[114]	2024-03-28 - 2024-04-07	3.4	3.3	[44]	Completează
3	Banca Comerciala Beta	BNM PSITI	[69]	2023-11-01 - 2023-12-22	3.4	3	[25]	Completează
4	Universtitatea de Stat din Moldova	BNM PSITI	[69]	2024-03-14 - 2024-04-18	3.3	0.8	[56]	Completează
5	Banca Comercială Alfa	BNM PSITI	[68]	2024-03-18 - 2024-03-31	3	2.9	[29]	Completează
6	Banca Comercială Alfa	BNM Vechi	[41]	2024-03-18 - 2024-03-31	0.2	2.7	[0]	Completează
7	Banca Comercială Alfa	BNM PSITI	[69]	2024-03-12 - 2024-03-16	3.7	3.2	[25]	Completează
8	Banca Comercială Alfa	BNM PSITI	[7]	2024-03-08 - 2024-03-30	3	2.6	[4]	Completează
9	Banca Comercială Alfa	BNM Vechi	[41]	2024-03-09 - 2024-03-21	0	0	[0]	Completează
10	Banca Comercială Alfa	BNM Vechi	[14]	2024-03-08 - 2024-04-01	0	0	[0]	Completează

A2.10. Introducerea nivelului de maturitate țintă (în PSITI, nivelul planificat/așteptat)



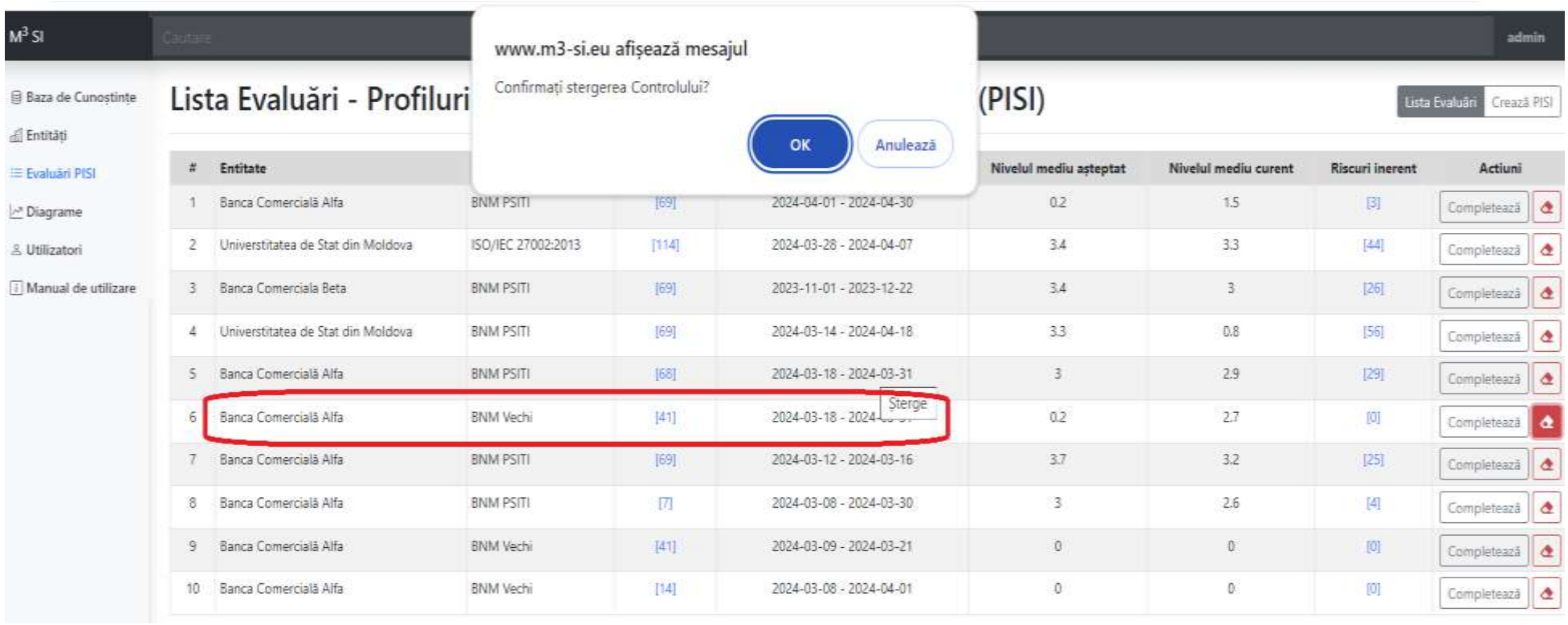
Aria	ID	Nume Control	Descriere control	Descriere Risk	Nivel Maturitate 1	Nivel Maturitate 2	Nivel Maturitate 3	Nivel Maturitate 4	Nivel Maturitate 5	Nivelul de Maturitate
Guvernanta	GU.01	Strategie	O strategie și viziune privind securitatea informațiilor sunt conducătoare pentru toate activitățile și măsurile care privesc securitatea informațiilor.	Lipsa unei strategii poate duce la decizii slabe de afaceri și de securitate sau la răspunsuri inadecvate la schimbările din mediul de afaceri.	- Activitățile sau măsurile de securitate sunt implementate și/sau executate pe o bază ad-hoc.	- Strategia și viziunea sunt definite, dar nu sunt aprobate de conducerea superioară.	- Strategia și viziunea au fost aprobate de conducerea superioară. - Strategia și misiunea sunt comunicate activ angajaților, contractorilor și partenerilor de afaceri.	- Strategia și viziunea sunt recunoscute ca fiind principale pentru toate activitățile și măsurile referitoare la securitatea informațiilor. - Alinierea cu strategia și viziunea este documentată acolo unde este aplicabil.	- Strategia abordează, de asemenea, modul în care IT-ul va contribui la realizarea obiectivelor de afaceri. - Valabilitatea și fezabilitatea strategiei și viziunii sunt verificate periodic. - În caz de necesitate, strategia sau viziunea sunt ajustate pentru a ține pasul cu obiectivele de afaceri și evoluțiile externe.	3 (Select, 1, 2, 3, 4, 5)
Guvernanta	GU.02	Politici	Organizația a adoptat o politică de securitate care este comunicată angajaților (și contractorilor) prin intermediul unui document scris sau	Incapacitatea de a respecta cerințele legislative, regulatorii și/sau interne de IT (securitate) din cauza unui cadru de	- Nicio politică definită. - Unele declarații de politică au fost redactate.	- O politică de securitate a fost definită și acoperă cele mai relevante aspecte ale securității informațiilor.	- Politica a fost aprobată de conducerea superioară. - Politica de securitate este comunicată activ	- Politica de securitate a fost încorporată în / adoptată de organizație și transformată în proceduri	- Conformitatea cu politica de securitate este raportată periodic conducerii superioare. - Politica este revizuită, actualizată	4

A2.11. Introducerea nivelului de maturitate real în timpul realizării controlului de evaluare (PISI)

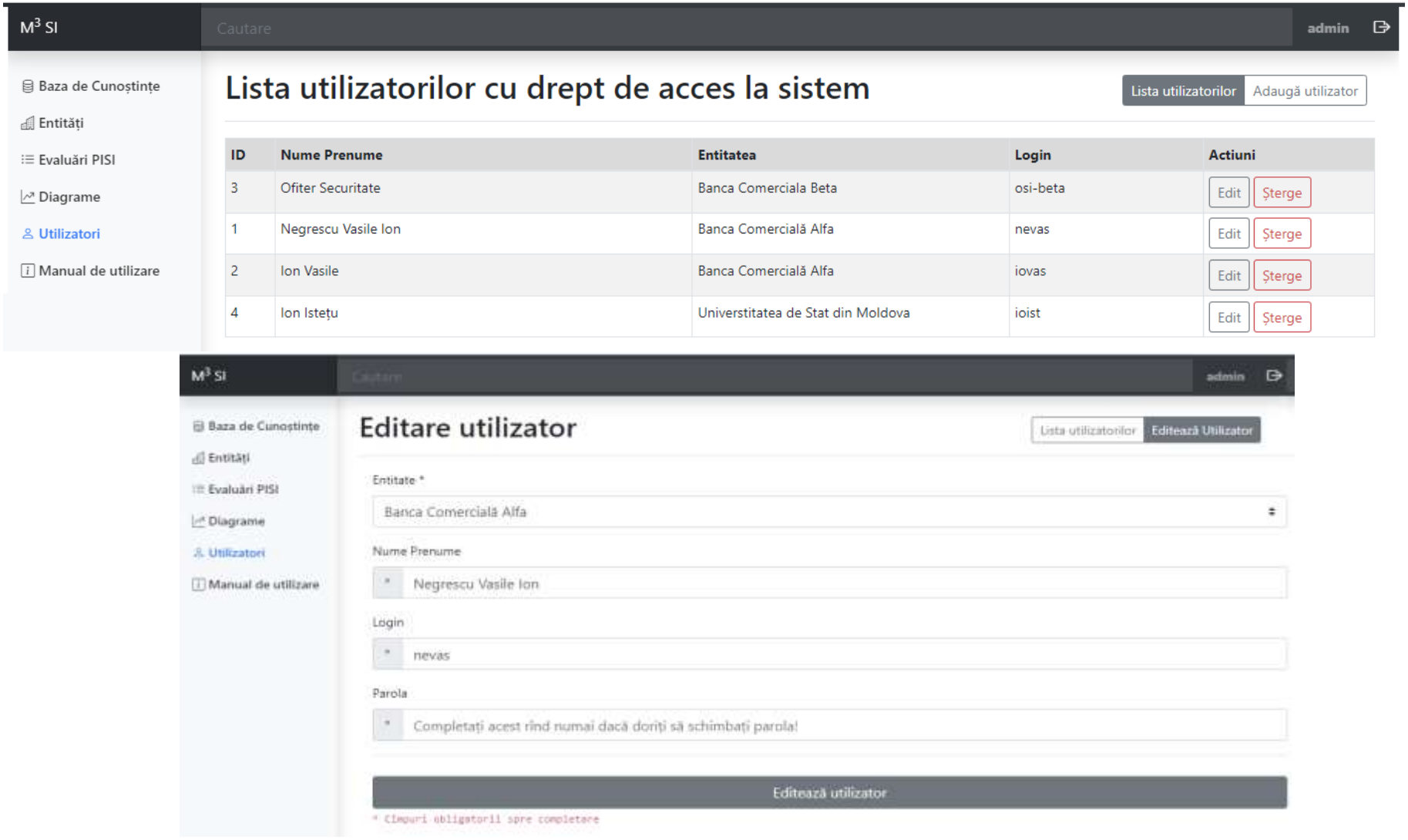


Aria	ID	Nume Control	Descriere Risk	Nivel Maturitate 1	Nivel Maturitate 2	Nivel Maturitate 3	Nivel Maturitate 4	Nivel Maturitate 5	Nivel de maturitate Curent	Comentarii OSI	Comentarii Controlor
Guvernanta	GU.02	Politici	Organizația a adoptat o politică de securitate care este comunicată angajaților (și contractorilor) prin intermediul unui document scris sau intranet. Dacă este cazul, politica este de asemenea comunicată activ furnizorilor/prestatorilor. Politica este ac	- Nicio politică definită. - Unele declarații de politică au fost redactate.	- O politică de securitate a fost definită și acoperă cele mai relevante aspecte ale securității informațiilor.	- Politica a fost aprobată de conducerea superioară. - Politica de securitate este comunicată activ angajaților, contractorilor și partenerilor de afaceri (furnizorilor) și este disponibilă sub formă de document tipărit sau digital prin intranet. - Politica face parte din programul de conștientizare a securității.	- Politica de securitate a fost încorporată în / adoptată de organizație și transformată în proceduri subiacente, linii de bază și instrucțiuni. - Conformitatea cu politica este evaluată pe o bază ad-hoc.	- Conformitatea cu politica de securitate este raportată periodic conducerii superioare. - Politica este revizuită, actualizată și reaprobată de către conducerea superioară anual.	2	-	
Guvernanta	GU.03	Plan / Foaie de parcurs	Obiectivele de afaceri, riscurile și cerințele de conformitate sunt transpuse într-un plan general de securitate a informațiilor, luând în considerare infrastructura IT și cultura de securitate.	- Niciun plan sau foaie de parcurs pentru securitatea informațiilor nu a fost definit. - Câteva proiecte individuale de securitate IT au fost definite și/sau sunt în desfășurare.	- Un plan sau o foaie de parcurs pentru securitatea IT a fost definit și acoperă toate obiectivele de afaceri relevante, riscurile și cerințele de conformitate.	- Planul sau drumul strategic pentru securitatea informațiilor a fost aprobat de managementul superior. - Planul a fost transpus în politicile și procedurile de securitate necesare. Împreună cu investițiile corespunzătoare în servicii, personal, software și hardware. - Politicile și procedurile de securitate sunt comunicate părților interesate și utilizatorilor.	- Planul de securitate a informațiilor este implementat prin politici de securitate aplicate, proceduri, servicii necesare, personal, software și hardware. - Există un proces pentru actualizarea periodică a planului de securitate a informațiilor și pentru forțarea nivelelor adecvate de revizuire și aprobare a schimbărilor de către management.	- Planul de securitate a informațiilor și portofoliul de proiecte asociate sunt monitorizate periodic pentru, de exemplu, progres, fezabilitate și măsura în care cerințele de afaceri sunt îndeplinite, inclusiv urmărirea beneficiilor. - Rapoartele sunt prezentate conducerii superioare.	3	-	

A2.12. Ștergerea unui controlului de evaluare (PISI)

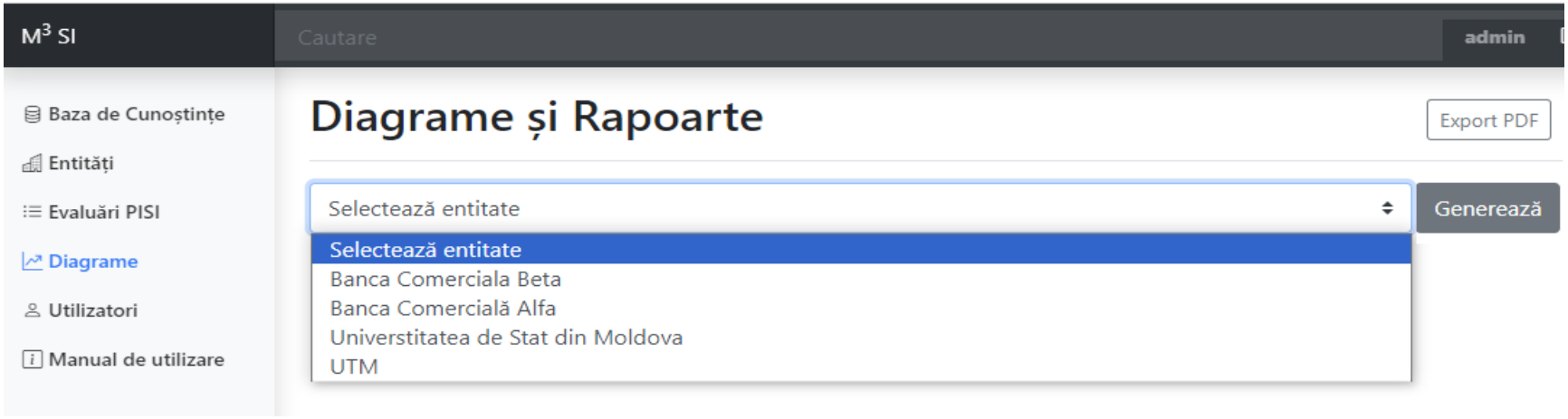


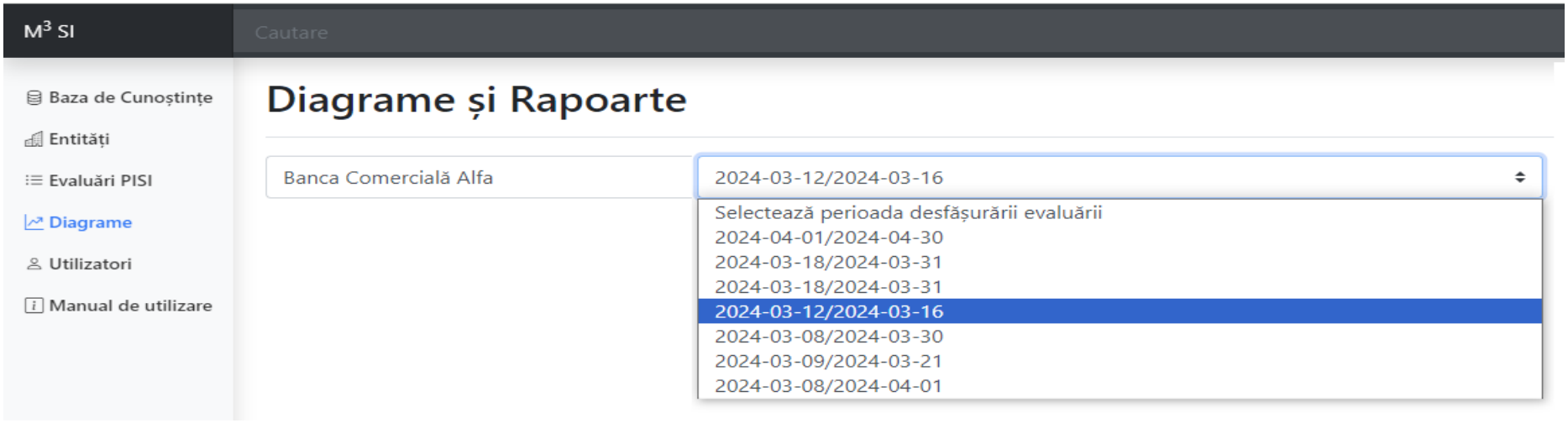
A2.13. Editarea/înregistrarea utilizatorilor în aplicația M3-SI



A2.14. Fragment de afișare a manualului de utilizare a aplicației M3-SI

A2.15. Generarea rapoartelor de evaluare (după realizarea controlului conform PISI)





A se vedea în continuare un raport de evaluare

Diagrame și Rapoarte

Export PDF

Banca Comercială Alfa

2024-03-12/2024-03-16

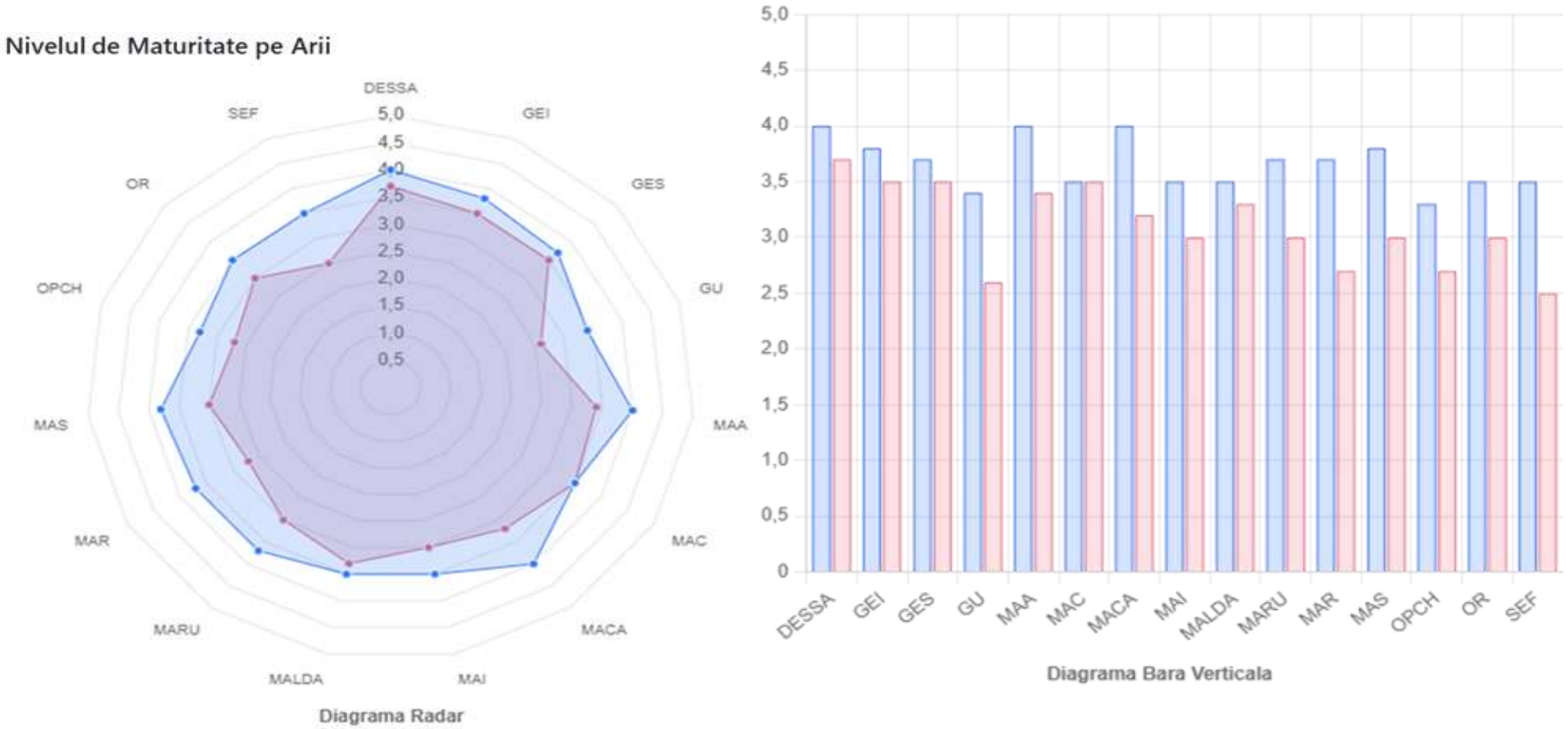
Generează

ID	Entitate	Standard / PSITI	Perioada desfășurării evaluării	Nivelul Mediu de Maturitate așteptat	Nivelul Mediu de Maturitate curent
19	Banca Comercială Alfa	BNM PSITI	2024-03-12 - 2024-03-16	3.7	3.2

NM Așteptat NM Curent

Istoricul evaluărilor

ID	Standard / PSITI	Perioada evaluării	NM așteptat	NM curent
1	BNM PSITI	2024-04-01 / 2024-04-30	0.2	1.5
2	BNM PSITI	2024-03-18 / 2024-03-31	3	2.9
3	BNM Vechi	2024-03-18 / 2024-03-31	0.2	2.7
4	BNM PSITI	2024-03-12 / 2024-03-16	3.7	3.2
5	BNM PSITI	2024-03-08 / 2024-03-30	3	2.6
6	BNM Vechi	2024-03-09 / 2024-03-21	0	0
7	BNM Vechi	2024-03-08 / 2024-04-01	0	0



Legendă : DESSA - Dezvoltarea Sistemelor si aplicațiilor; GEI - Gestionarea Informației; GES - Gestionarea Securității; GU - Guvernanta; MAA - Managementul Accesului; MAC- Managementul Configurațiilor; MACA - Managementul Continuității Activității; MAI - Managementul Incidentelor; MALDA - Managementul lanțului de aprovizionare; MARU - Managementul Resurselor Umane; MAR - Managementul Riscurilor; MAS - Managementul Schimbărilor; OPCH - Operațiuni cu horsturile; OR - Organizare; SEF - Securitatea Fizică.

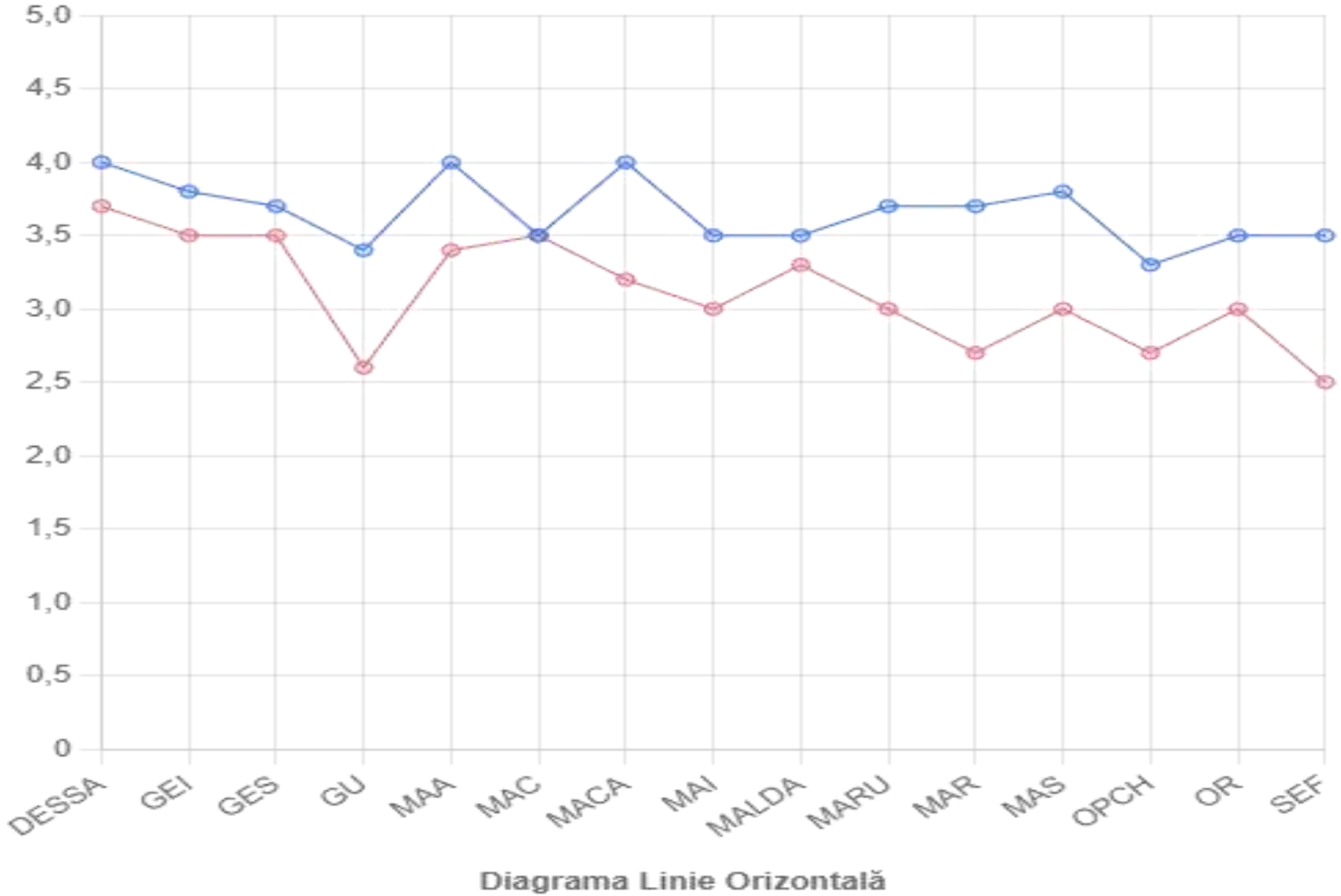
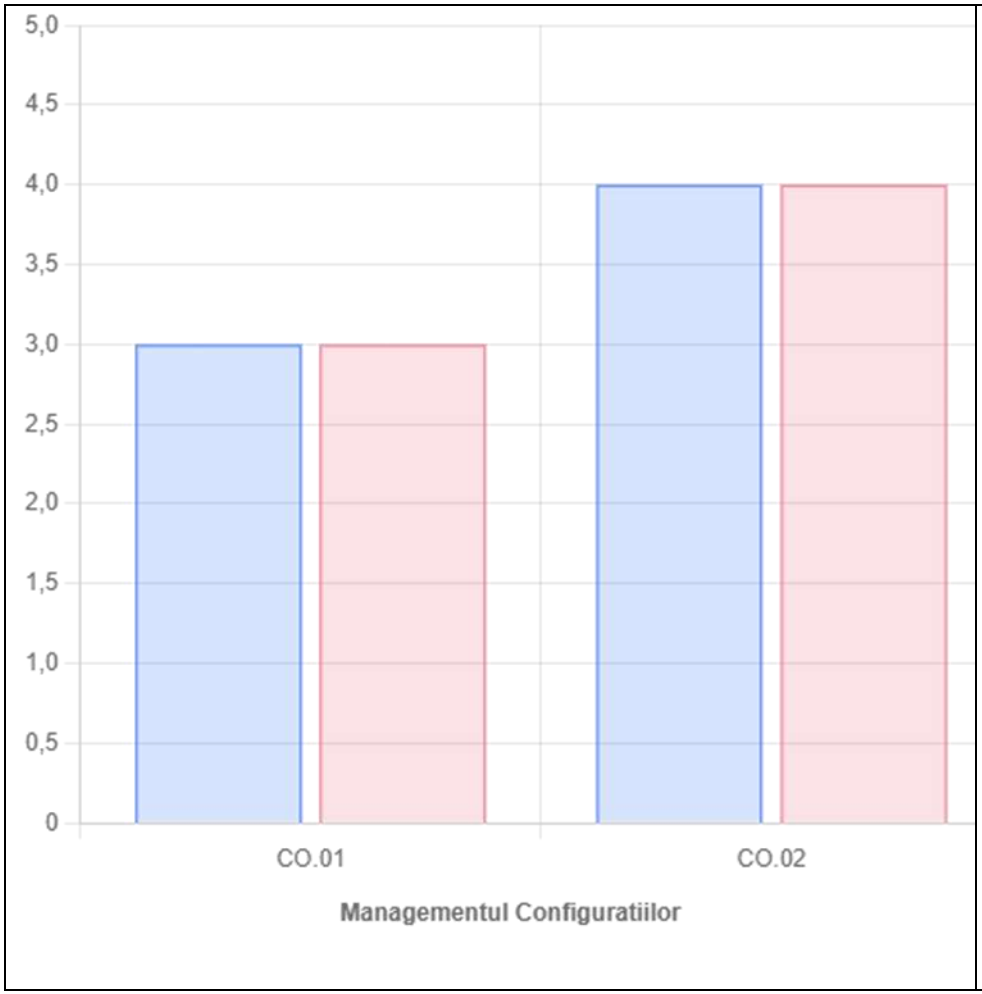
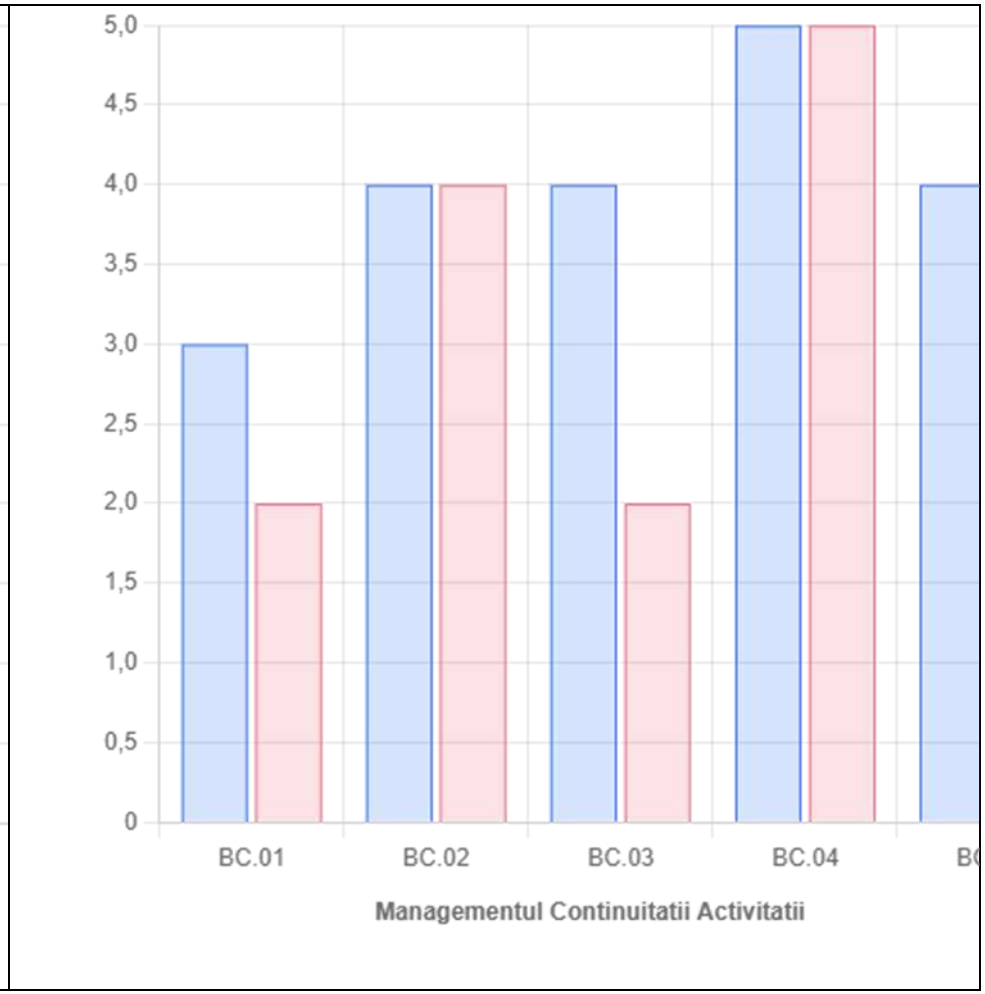
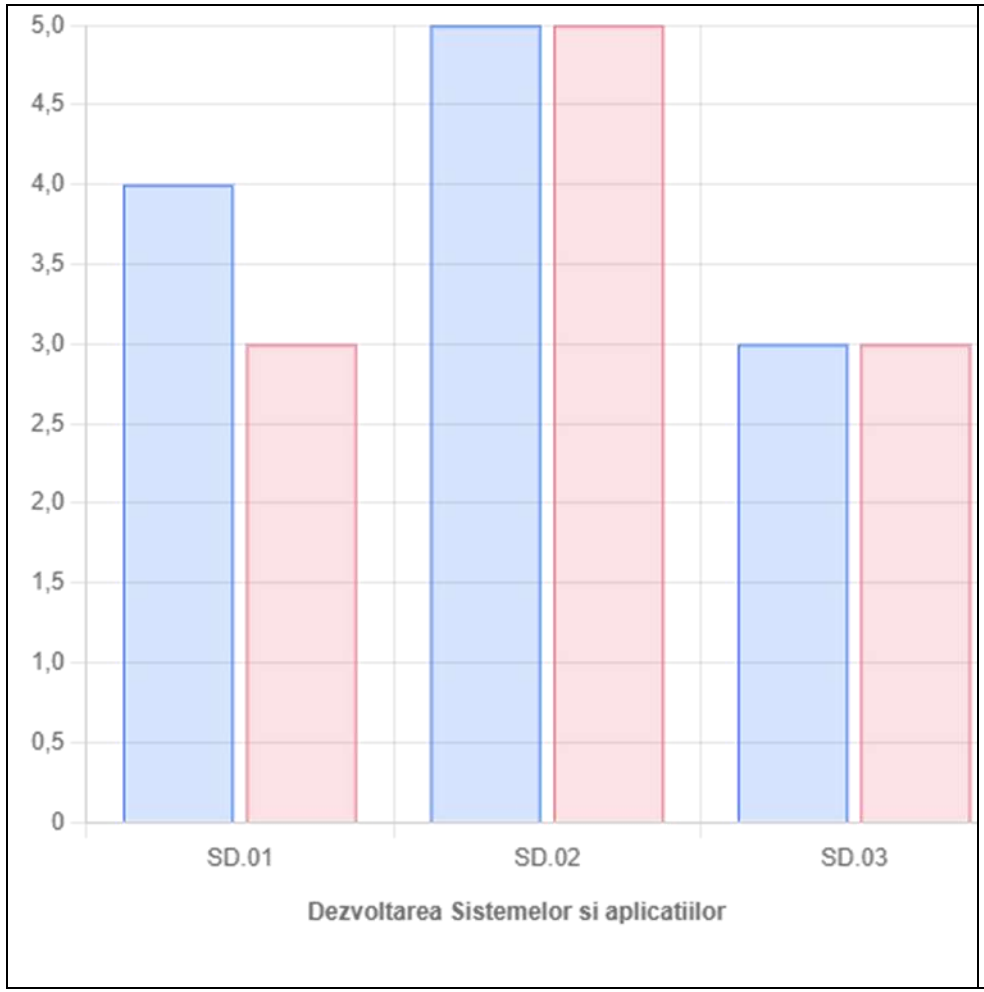
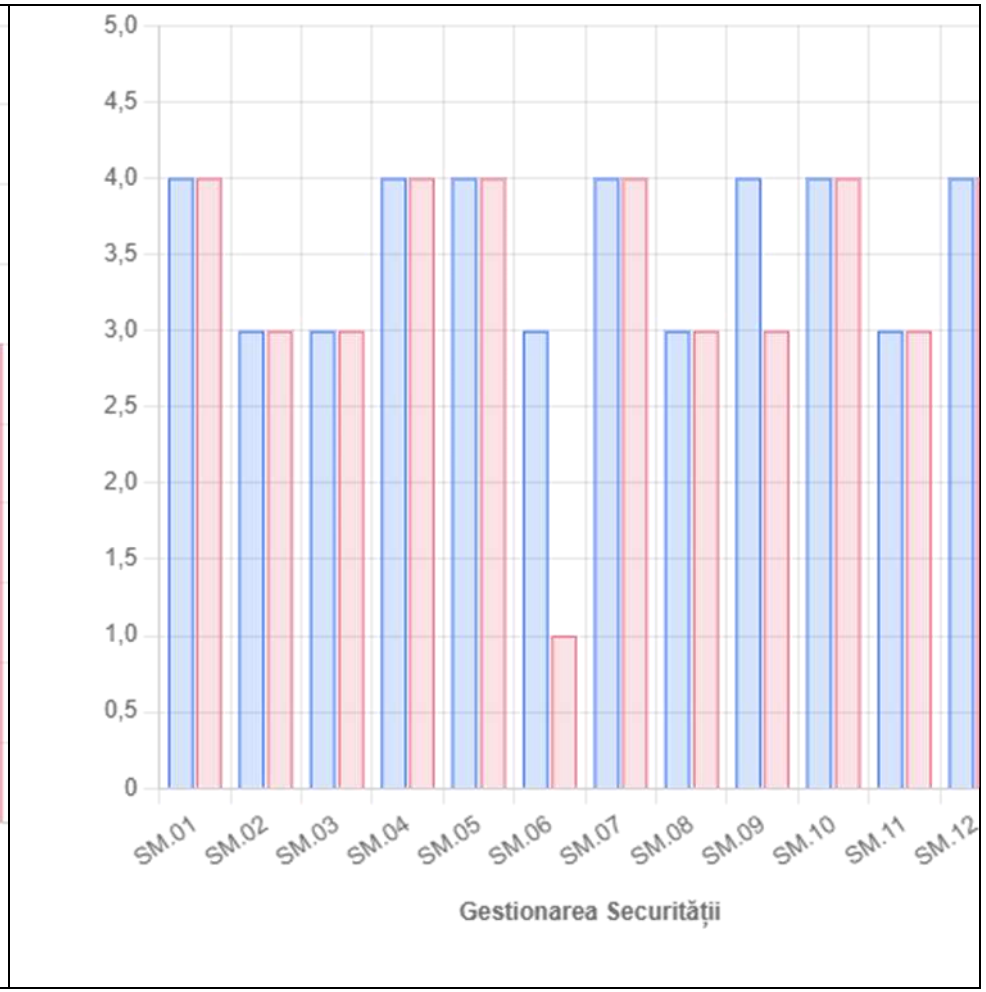


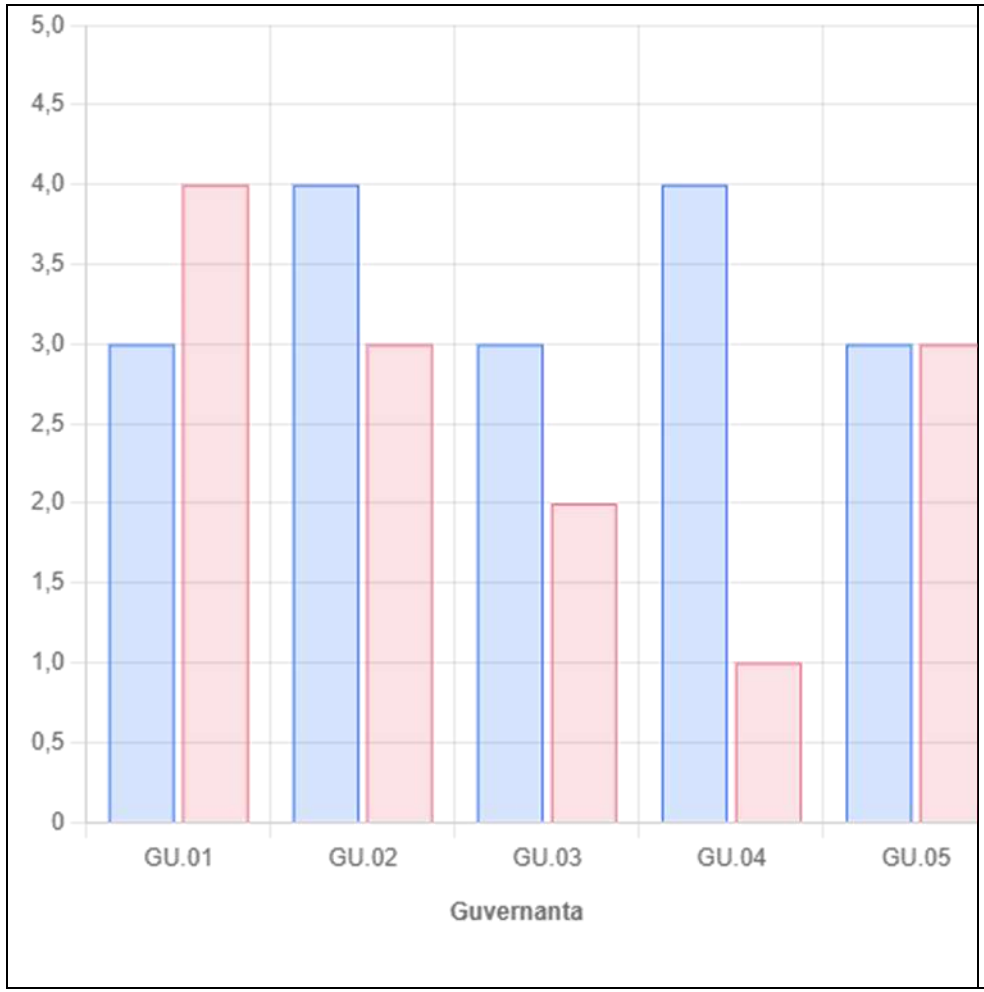
Diagrama Linie Orizontală

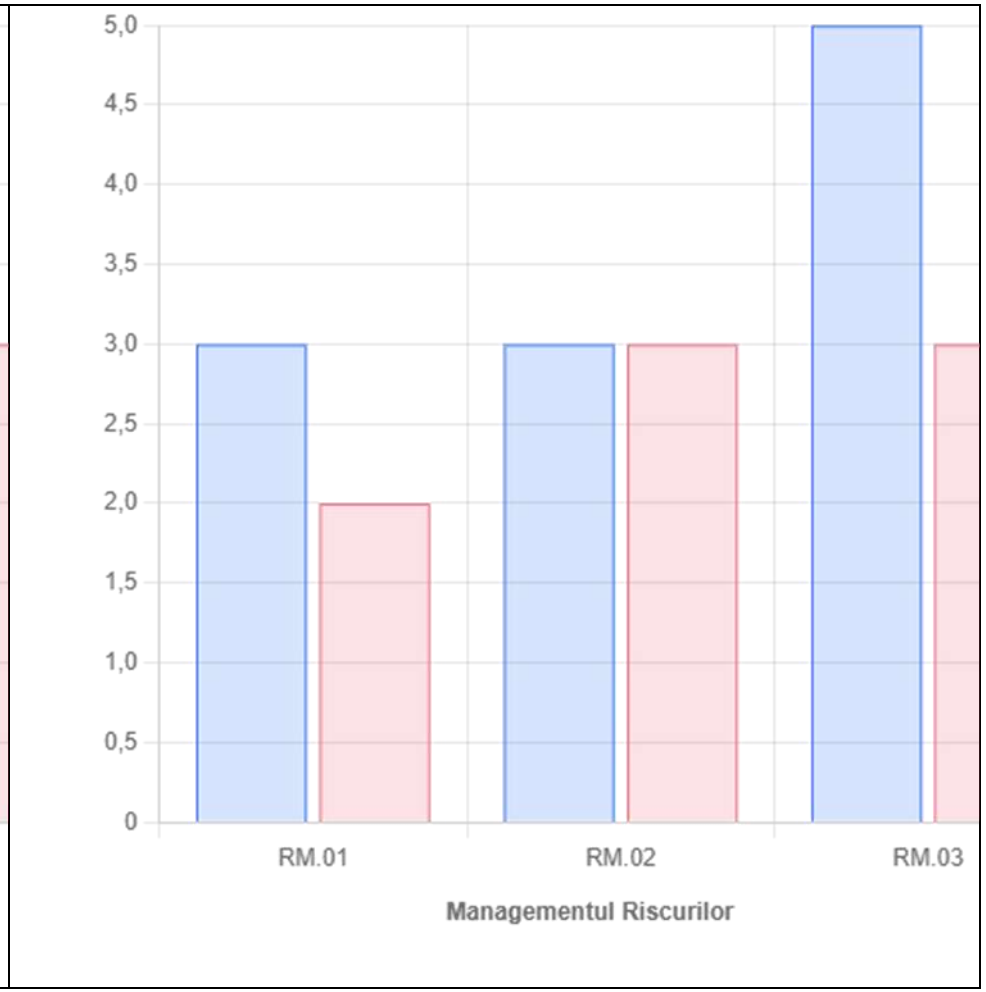

5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
CO.01
CO.02
Managementul Configuratiilor

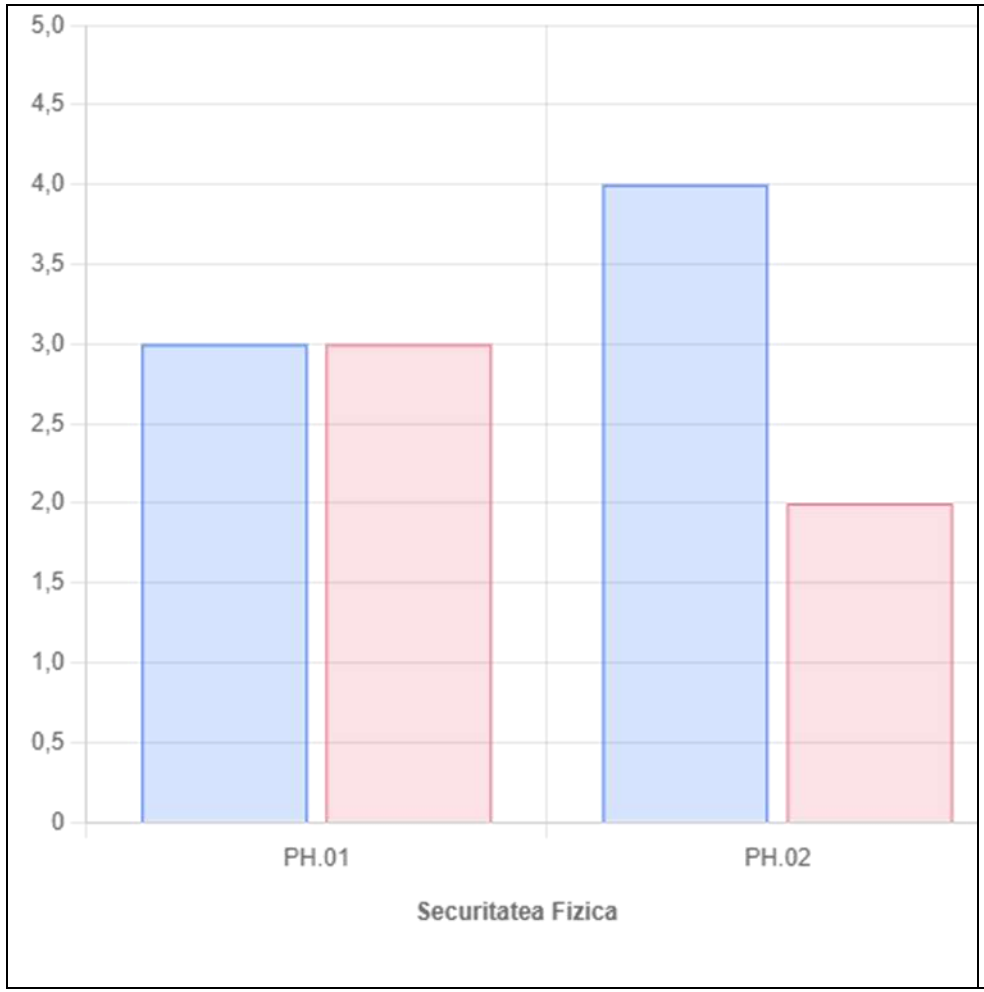

5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
BC.01
BC.02
BC.03
BC.04
Managementul Continuitatii Activitatii

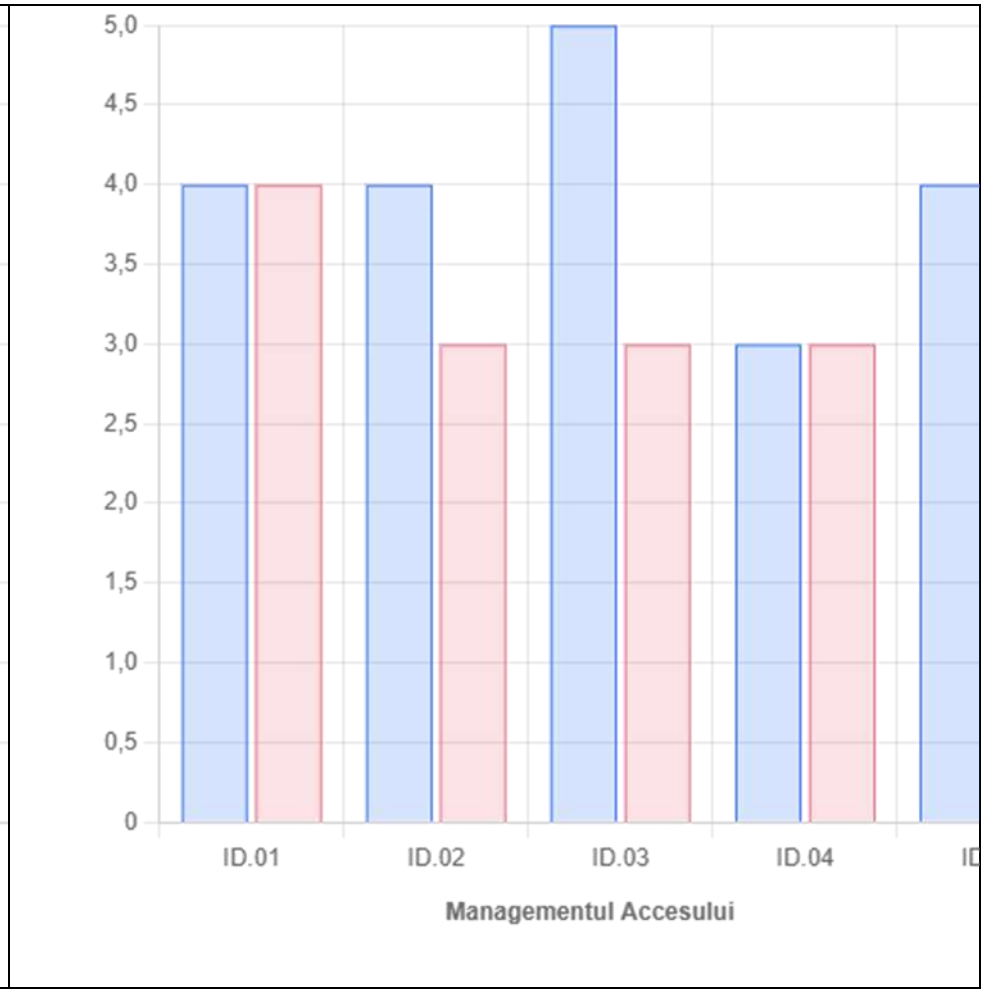

5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
SD.01
SD.02
SD.03
Dezvoltarea Sistemelor si aplicatiilor

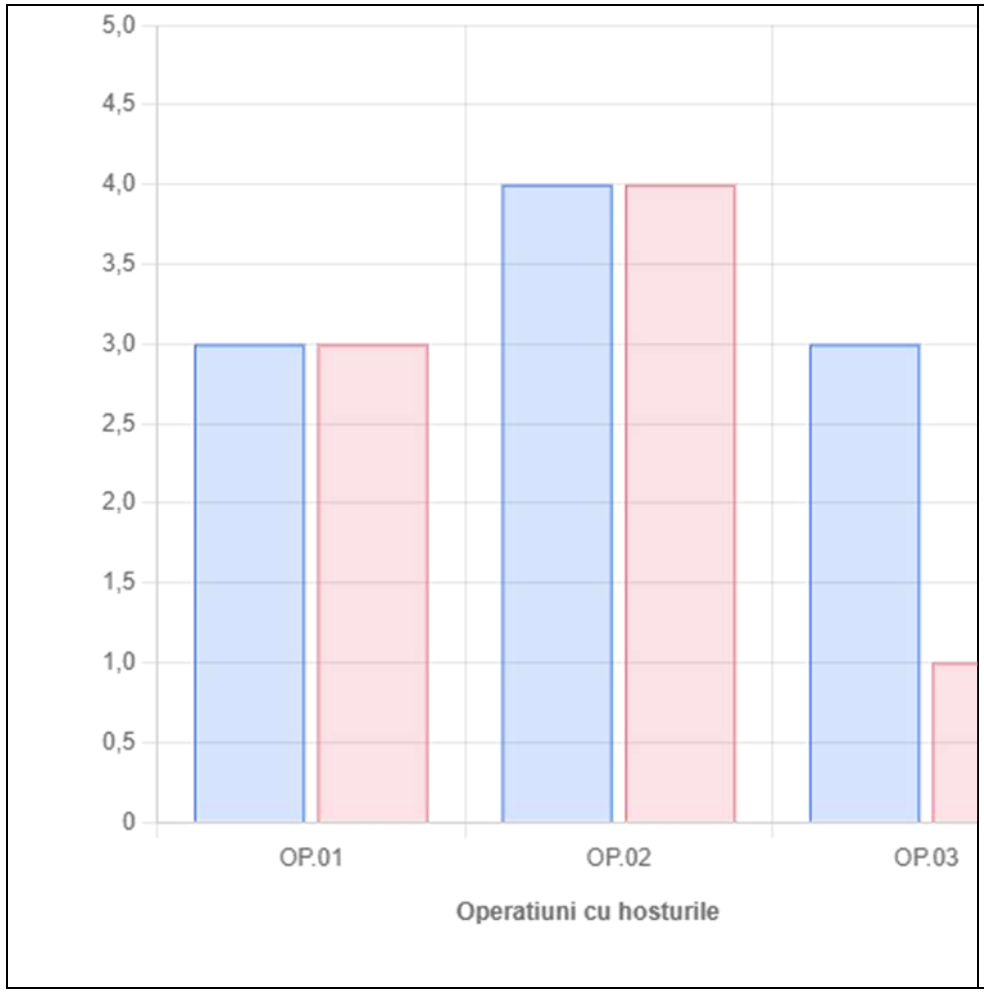

5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
SM.01
SM.02
SM.03
SM.04
SM.05
SM.06
SM.07
SM.08
SM.09
SM.10
SM.11
SM.12
Gestionarea Securității

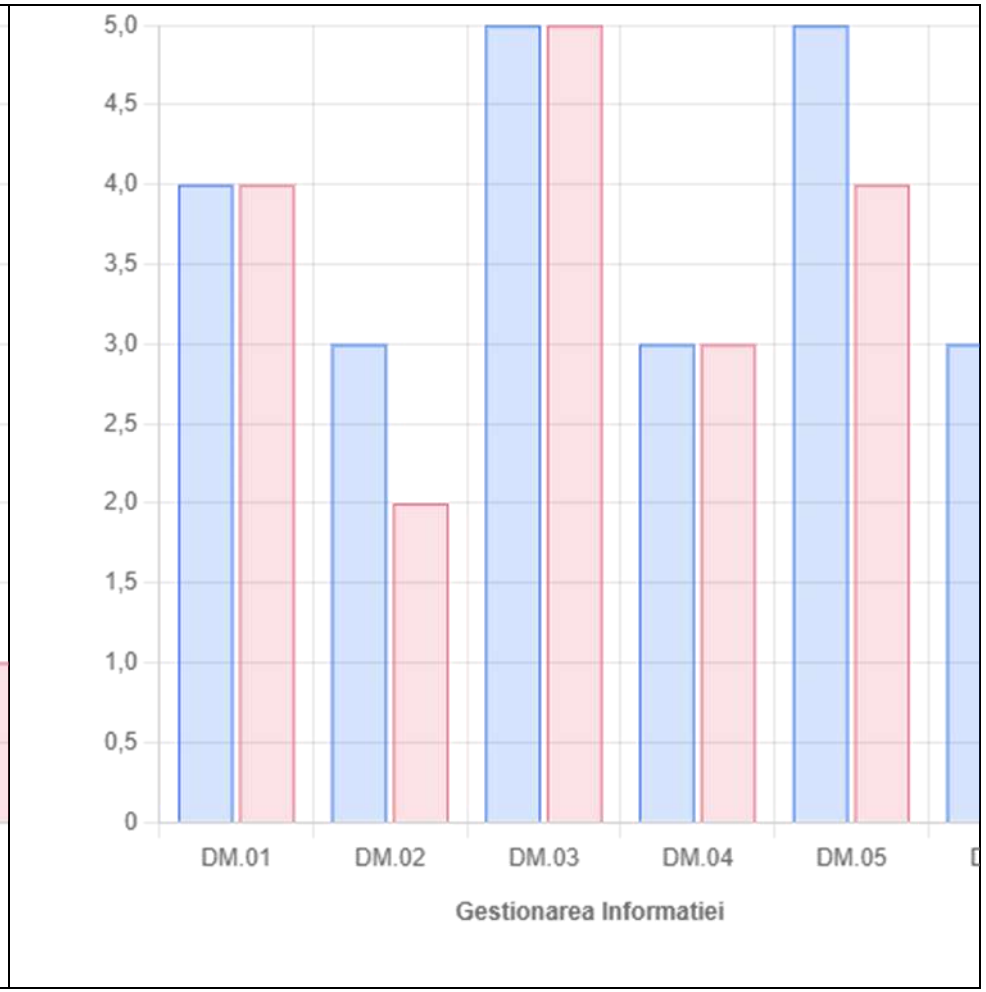

5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
GU.01
GU.02
GU.03
GU.04
GU.05
Guvernanta

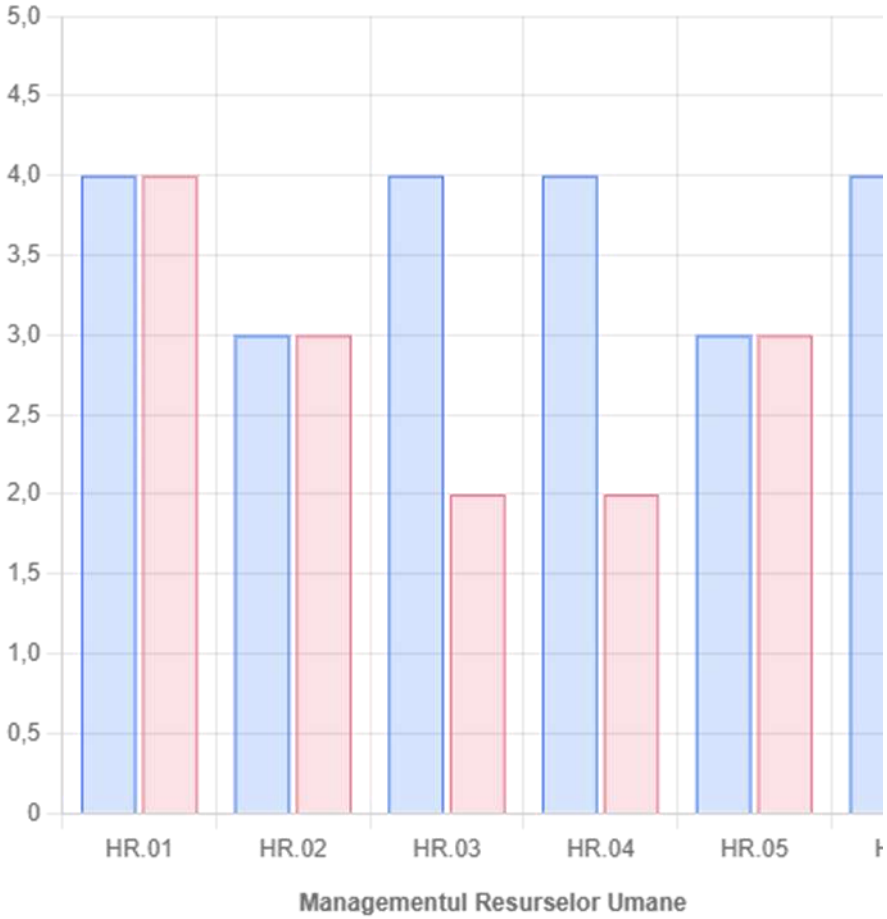

5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
RM.01
RM.02
RM.03
Managementul Riscurilor

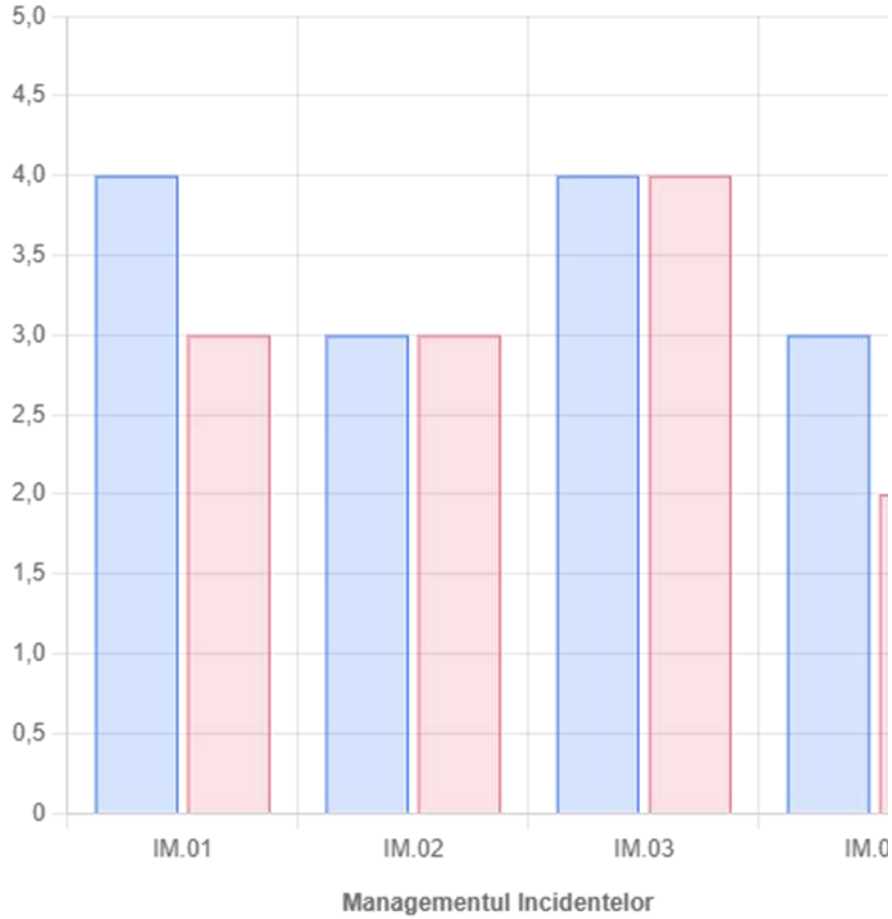

5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
PH.01
PH.02
Securitatea Fizica

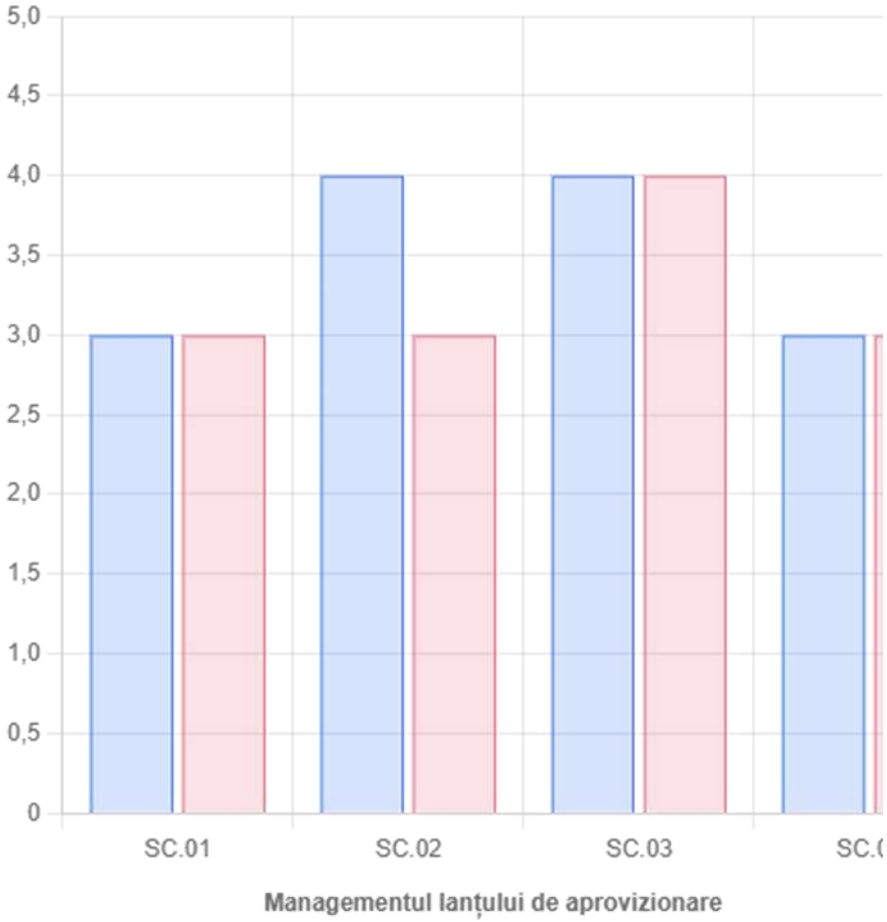

5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
ID.01
ID.02
ID.03
ID.04
Managementul Accesului

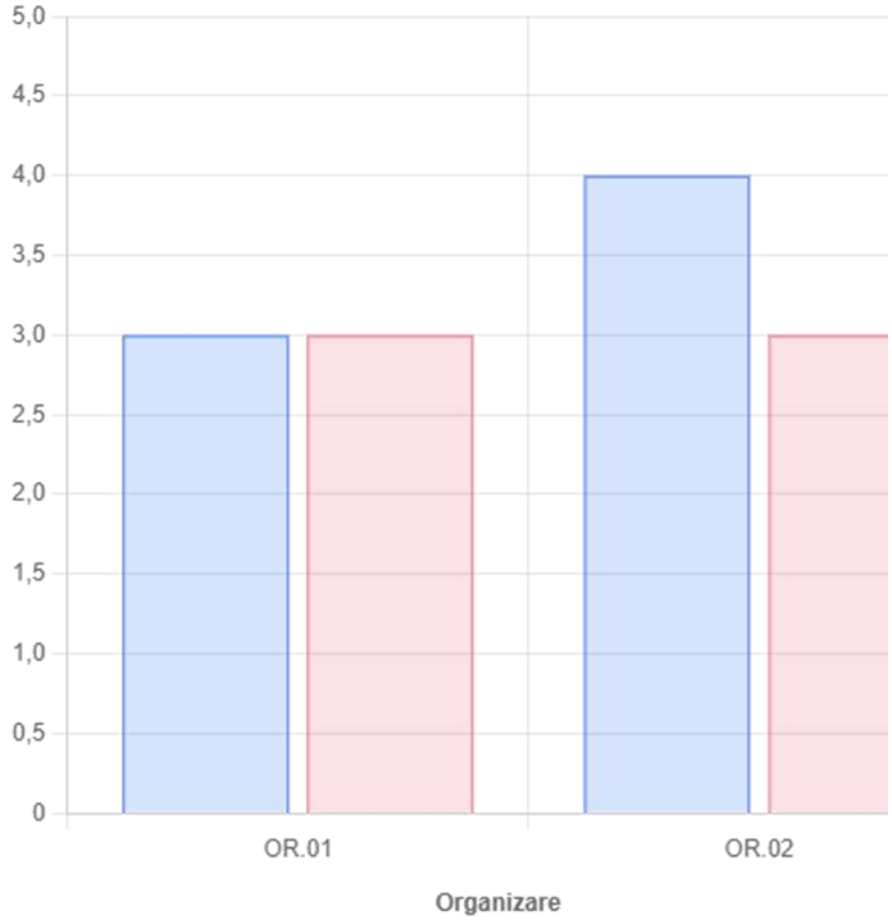

5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
OP.01
OP.02
OP.03
Operatiuni cu hosturile

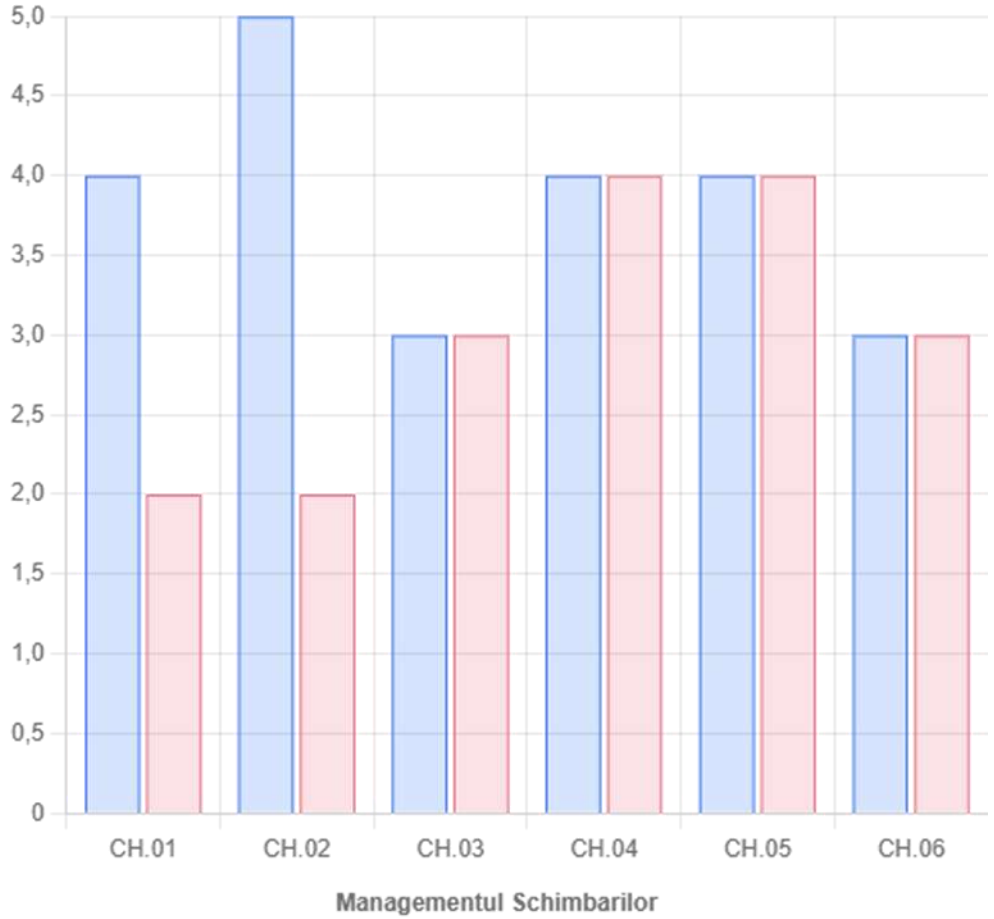

5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
DM.01
DM.02
DM.03
DM.04
DM.05
Gestionarea Informatiei


5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
HR.01
HR.02
HR.03
HR.04
HR.05
Managementul Resurselor Umane


5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
IM.01
IM.02
IM.03
Managementul Incidentelor


5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
SC.01
SC.02
SC.03
Managementul lanțului de aprovizionare


5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
OR.01
OR.02
Organizare


5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0
CH.01
CH.02
CH.03
CH.04
CH.05
CH.06
Managementul Schimbarilor

Riscuri de securitate identificate

#	ID	Aria	Nume control	Descriere risc	Risc inerent
1	GU.02	Guvernanta	Politici	Incapacitatea de a respecta cerințele legislative, regulatorii și/sau interne de IT (securitate) din cauza unui cadru de politici ineficient care susține strategia IT și securitatea informațiilor.	Mic
2	GU.03	Guvernanta	Plan / Foaie de parcurs	Organizația nu oferă îndrumare și suport pentru securitatea informațiilor în conformitate cu obiectivele de afaceri, riscurile și cerințele de conformitate.	Mic
3	GU.04	Guvernanta	Arhitectura	O viziune incompletă asupra arhitecturii actuale și țintă poate duce la creșterea costurilor, complexității și incapacității de a răspunde în timp util la provocările determinate de schimbările din afaceri.	Mediu
4	OR.02	Organizare	Segregarea responsabilitatilor	Acțiuni unilaterale (de exemplu, accesul neautorizat la date) ar putea avea loc în procesele cheie de IT, ceea ce ar putea duce la un impact negativ asupra proceselor de afaceri, de exemplu, riscul de utilizare neglijentă sau deliberată a sistemului.	Mic
5	RM.01	Managementul Riscurilor	Cadrul de management al riscului informațional	Cadrul de management al riscului și controlului informațional nu este în conformitate cu modelul de management al riscului la nivel de organizație, ceea ce duce la interpretări greșite ale riscurilor și/sau nerespectarea obiectivelor IT și de afaceri.	Mic
6	RM.03	Managementul Riscurilor	Plan de acțiune și atenuare a riscurilor (inclusiv acceptarea riscului)	Răspunsurile la risc nu sunt identificate și implementate. Acțiunile solicitate nu sunt comunicate și executate, conducând la o posibilă manifestare a riscurilor. Costuri mari/beneficii scăzute legate de riscuri moderate sau scăzute. Eșecul de a prioritiz	Mic
7	HR.03	Managementul Resurselor Umane	Dependența de indivizi	Dependența critică de indivizi cheie va cauza riscuri în caz de plecare sau indisponibilitate extinsă a personalului IT cheie; dacă echipa cheie de dezvoltare părăsește organizația sau dacă nu este posibilă recrutarea personalului IT.	Mic
8	HR.04	Managementul Resurselor Umane	Schimbarea locului de muncă și/sau încetarea locului de muncă	Accesul utilizatorilor nu este dezactivat în timp util după ce angajații au părăsit echipa sau nu ar mai trebui să aibă acces din niciun motiv. Continuitatea funcției este pusă în pericol din cauza lipsei de transfer de cunoștințe.	Mic
9	IM.01	Managementul Incidentelor	Gestionarea incidentelor	Incidentele nu sunt clasificate corespunzător și sunt tratate incorect în procesul de gestionare a incidentelor și problemelor, scăzând în cele din urmă performanța (de exemplu, integritatea și disponibilitatea) IT.	Mic
10	IM.04	Managementul Incidentelor	Managementul problemelor	Incidentele nu sunt clasificate corespunzător și tratate incorect de către procesul de gestionare a incidentelor și problemelor, reducând în cele din urmă performanța IT.	Mic
11	CH.01	Managementul Schimbarilor	Schimbați standardele și procedurile	Lipsa unui proces formal de management al schimbărilor IT, care să asigure că modificările propuse sunt revizuite, autorizate, testate, implementate, documentate și publicate într-o manieră controlată, ar putea duce la întreruperi în afaceri și/sau la pie	Mic
12	CH.02	Managementul Schimbarilor	Evaluarea impactului, prioritizarea și autorizarea	Evaluarea inadecvată a impactului, prioritizarea sau autorizarea ar putea duce la întreruperi în afaceri, corupție și/sau pierderea datelor confidențiale.	Mediu
13	SD.01	Dezvoltarea Sistemelor si aplicatiilor	Metodologie pentru dezvoltarea și implementarea în siguranță a software-ului	Dezvoltari de software și/sau sisteme care nu sunt proiectate și implementate în conformitate cu cerințele funcționale, tehnice și de securitate convenite, standardele de aprobare și arhitectura informațională, ceea ce duce la neîndeplinirea cerințelor de	Mic
14	DM.02	Gestionarea Informatiei	Clasificare	Deciziile privind clasificarea informațiilor și sistemelor, precum și nivelul de protecție aferent, nu sunt în conformitate cu cerințele de afaceri. Datele pot fi compromise în diferite moduri dacă datele sensibile nu sunt clasificate la nivelul corespunz	Mic
15	DM.05	Gestionarea Informatiei	Schimb de date (sensibile).	Acces neautorizat la resurse (date) conectate la o rețea sau dezvăluirea informațiilor sensibile transmise într-o rețea. Acest lucru ar putea duce în cele din urmă la furt, corupție, utilizarea necorespunzătoare sau neautorizată a activelor informaționale	Mic
16	ID.02	Managementul Accesului	Administrarea drepturilor de acces	Acces neautorizat la date, aplicații, sisteme de operare și resurse aferente (de exemplu tabele de baze de date, tabele de parole, memorie), cauzate de un proces inadecvat de atribuire, monitorizare, revizuire și încetare a drepturilor de acces ale utiliz	Mic

#	ID	Aria	Nume control	Descriere risc	Risc inerent
17	ID.03	Managementul Accesului	Super utilizatori	Gestionarea inadecvată a super-utilizatorilor ar putea duce la acces neautorizat la programe și date sau la întreruperea serviciilor IT.	Mic
18	SM.06	Gestionarea Securității	Gestionarea patch-urilor	Absența patch-urilor sau a corecțiilor de securitate ar putea determina utilizarea abuzivă a vulnerabilităților cunoscute pentru a obține acces neautorizat la infrastructura IT.	Mic
19	SM.09	Gestionarea Securității	Întreținerea infrastructurii	Întreruperea afacerii din cauza predării nesigure a modificărilor în infrastructura de producție, sistem și întreținere de rutină.	Mic
20	PH.02	Securitatea Fizica	Gestionarea drepturilor de acces fizic	Nu sunt definite și implementate proceduri pentru a acorda, limita și revoca accesul la spații, clădiri și zone în funcție de nevoile afacerii, inclusiv de urgențe. Accesul în spații, clădiri și zone nu poate fi justificat, autorizat, înregistrat sau moni	Mic
21	OP.03	Operatiuni cu hosturile	Managementul capacității și performanței	Performanța și capacitatea nu sunt gestionate în mod corespunzător și în timp util, ceea ce duce la întreruperi în afaceri atunci când se atinge capacitatea maximă sau performanța minimă.	Mic
22	BC.01	Managementul Continuitatii Activitatii	Planificarea continuității afacerii	Absența înțelegerii legate de risc cu privire la impactul potențial al afacerii și cerințele de rezistență, procesare alternativă și recuperare a tuturor serviciilor IT critice. Acest lucru ar putea duce în cele din urmă la o întrerupere majoră a funcțiil	Mic
23	BC.03	Managementul Continuitatii Activitatii	Spațiu de stocare de rezervă în afara locației	Suporturile critice nu sunt stocate în afara locației, ceea ce duce la indisponibilitatea datelor de rezervă în cazul unui dezastru la centrul de date. Backup-urile critice ale suporturilor nu sunt testate periodic, ceea ce înseamnă posibil că datele nu p	Mic
24	BC.05	Managementul Continuitatii Activitatii	Management de criza	Gestionarea inadecvată a crizelor ar putea duce la răspunsuri inadecvate la calamități, ducând în cele din urmă la pierderea afacerilor.	Mic
25	SC.02	Managementul lanțului de aprovizionare	Managementul nivelului de servicii	Lipsa managementului și monitorizării furnizării serviciilor, ceea ce înseamnă că abaterile în performanța furnizorilor de servicii nu sunt detectate la timp. Tendințele în statisticile de performanță pentru serviciile individuale și globale nu sunt ident	Mic

Anexa 3. Declarația privind asumarea răspunderii

Subsemnatul, Briceag Valentin, declar pe răspundere personală că materialele prezentate în teza de doctorat sunt rezultatul propriilor cercetări și realizări științifice.

Conștientizez că, în caz contrar, urmează să suport consecințele în conformitate cu legislația în vigoare.

Briceag Valentin

Semnătura 

Data 29.02.2024 www.m3-si.eu

Anexa 4. CV EUROPASS

INFORMAȚII PERSONALE

Valentin Briceag

Consultant Certificat Splunk, Arhitect,
10 ani de experiență în Securitatea Cibernetică

(+40) 790 733406
valentinbriceag@gmail.com

EXPERIENȚA DE MUNCĂ

---

ianuarie 2020 – prezent

Persoana Fizica Autorizată, Subcontractor la Comisia Europeană, Consultant Superior Splunk, Inginer de Platformă SIEM

- Proiectarea și implementarea Splunk Enterprise și Splunk Enterprise Security în medii de întreprinderi mari
- Dezvoltarea regulilor de identificare a atacurilor cibernetice pentru Enterprise Security
- Evaluarea maturității implementărilor soluție Splunk Enterprise
- Operarea, întreținerea, ajustarea și depanarea mediului Splunk Enterprise
- Integrarea diferitelor surse de date în Splunk
- Crearea regulilor de analiză pentru sursele noi integrate în Splunk
- Crearea și implementarea politicilor de păstrare a datelor în Splunk
- Dezvoltarea de diagrame, vizualizări, rapoarte și alerte
- Scalarea arhitecturii Splunk
- Implementarea, configurarea și ajustarea aplicațiilor în Splunk

mai 2014 – ianuarie 2020

Expert în securitatea informațiilor, Banca Națională a Moldovei, www.bnm.md

- Responsabil pentru deciziile privind politica de securitate cibernetică, planificare, cooperare și abordare a protecției infrastructurii Băncii Naționale a Moldovei
- Participare la elaborarea și revizuirea cadrului de reglementare bancar privind securitatea informațiilor, probleme de securitate cibernetică
- Responsabil în cadrul Băncii Naționale a Moldovei pentru obiectivele strategice, tehnicile, politicile și cele mai bune practici care asigură disponibilitatea, integritatea, autentificarea, confidențialitatea și nerepudierea informațiilor și sistemelor informaționale ale BNM
- Participare în elaborarea legislației, politicilor și practicilor de securitate cibernetică legate de sectorul bancar al Republicii Moldova
- Participare în elaborarea standardelor interne la nivel de entitate bancară și încurajarea utilizării celor mai bune practici pentru securitatea cibernetică în băncile comerciale și în sectorul nebancar.

Proiecte implementate:

- Soluție SIEM (Splunk / Qradar)
- Prevenirea scurgerii de date
- Web Gateway
- Managementul dispozitivelor mobile
- Clasificarea informației TITUS
- Managementul vulnerabilităților
- Managementul riscurilor

august 2011 – mai 2014

Administrator de rețea și securitate a informațiilor, Institutul de Dezvoltare a Societății Informaționale, www.idsi.md

- Identificarea și remedierea amenințărilor și vulnerabilităților

- Administrarea rețelei MAN „ACADEMICA” (firewall, dispozitive de rețea, VMware, servere de găzduire web, servere de email, DNS, server de dezvoltare, Active Directory)
- Auditor intern pentru implementarea ISO/IEC 27001
- Investigarea și cooperarea cu agențiile de profil în cazul infracțiunilor cibernetice

august 2008 – august 2011

Administrator de sistem TIC, Serviciul Grăniceri al Republicii Moldova, www.border.gov.md

- Administrarea rețelei (firewall, dispozitive de rețea, comunicații VPN, Active Directory, server DNS, server de sistem de fișiere)
- Mentenanță servere și calculatoare

EDUCATIE

septembrie 2012 – iunie 2014 — Master în Tehnologii de Rețea, Universitatea de Stat din Moldova, Facultatea de Matematică și Informatică

septembrie 2004 – iunie 2008 — Inginer în Tehnologii Informaționale, Universitatea Tehnică din Moldova, Facultatea de Calculatoare, Informatică și Microelectronică

COMPETENTE PERSONALE

Limba maternă: Română

Alte limbi străine	ÎNȚELEGERE		VORBIRE		SCRIERE
	Ascultare	Citind	Participarea la conversație	Vorbitor	
Engleză	C2	C2	C2	C2	C2
Rusă	C2	C2	C2	C2	C2

INFORMAȚII SUPLIMENTARE

Certificări

Credly - https://www.credly.com/users/valentin-briceag/badges

- Splunk Core Certified Consultant (License Cert-352263)
- Splunk Accredited Enterprise Security Implementation (License Cert-356378)
- Splunk Enterprise Certified Architect (License Cert-343944)
- Splunk Enterprise Security Certified Admin (License Cert-301618)
- Splunk Enterprise Certified Admin (License Cert-295293)
- Splunk Core Certified Power User (License Cert-293412)
- Certified Ethical Hacker (Dec 2016 / EC-Council / License ECC93354947119)
- VMware Certified Professional 6 Network Virtualization
- VMware Certified Professional 6.5 DC Virtualization
- CCNA Security (Nov 2015 / Cisco / License 423924621920AODF)
- CCNA Routing and Switching (Nov 2015/ Cisco / License 423164171361DTVH)

29-02-2024  **V. Briceag**