Model Multiprofil de Maturitate a Securității Informației (M^3SI)

Valentin BRICEAG

Universitatea de Stat din Moldova
valentinbriceag@gmail.com

Rezumat: În lucrare este examinat un Model Multiprofil de Maturitate a Securității Informației (M^3SI), *simplu și transparent*, orientat spre generarea Profilurilor particulare (Individuale) de Securitate a Informației (PISI). M^3SI are la bază cele mai bune practici de securitate a informației/cadre normative de reglementare cunoscute în acest moment, *e.g. OISM3:2017, NIST SP 800-53 rev.5 (2020), NIST 800-207 Zero Trust Architecture (2020), ISO/IEC 27001:2013, PCI-DSS 3.2.1 (2018), COBIT 5:2012, COBIT:2019, ISO/IEC 20000-1:2018, ITIL v4:2019 etc.* M^3SI este flexibil, astfel încât permite adăugarea, eliminarea, modificarea de noi cunoștințe structurate privind amenințările și riscurile existente, controalele și metricile preconizate pentru evaluarea nivelului de maturitate a SecInf. M^3SI este însoțit de o aplicație instrumentală software care -ermite generarea profilurilor individuale de securitate a informației tipice *unor industrii (PMSITI)*, e.g. educație, bănci, medicină; *la nivel de entitate concretă*, e.g. Universitatea de Stat din Moldova, bancă comercială, clinică privată; *la nivel de subdiviziuni sau zone/sfere* ale SecInf *a unei entități,* e.g. Departamentul 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. În continuare, PISI poate fi utilizat pentru măsurarea și evaluarea maturității SecInf în cadrul misiunilor interne de autoevaluare, a misiunilor externe de evaluare a conformității și/sau a misiunilor de consultanță și/sau pentru compararea maturității unor organizații tipice, care aparțin unei anumite industrii. Raportul evaluării conform PISI reflectă sfera și starea curentă a SecInf, riscurile și amenințările specifice și sugerează țintele recomandate de îmbunătățire.

Cuvinte cheie: Sistem de Management al Securității Informației (SMSI), Declarația de aplicabilitate a SMSI (SoA), Model Multiprofil de Maturitate al Securității Informației (M^3SI), Profil particular (Individual) de Securitate a Informației (PISI), Securitatea Informației (SecInf), valori țintă ale criteriilor de evaluare, măsurarea criteriilor.

Information Security Multiprofile Maturity Model (ISM^3)

Abstract: The paper examines a Multiple Profile Model of Information Security Maturity (ISM3), uncomplicated and clear, aimed at generating particular (Individual) Information Security Profiles (PISI). ISM3 is based on currently known best practices for information security / regulatory frameworks, *e.g. OISM3: 2017, NIST SP 800-53 rev.5 (2020), NIST 800-207 Zero Trust Architecture (2020), ISO / IEC 27001: 2013, PCI-DSS 3.2.1 (2018), COBIT 5: 2012, COBIT: 2019, ISO / IEC 20000-1: 2018, ITIL v4: 2019 etc.* The ISM3 flexibility allows the addition, deletion, modification of new structured knowledge concerning the existing threats and risks, controls and metrics expected for the assessment of InfoSec maturity level. ISM3 is accompanied by a software tool application, which allows the generation of individual security profiles for specific information of *certain industries (PMSITI)*, e.g. education, banking, medicine; at a concrete entity level, e.g. State University of Moldova, commercial bank, private hospital; *at some InfoSec subdivision or area levels/spheres, of an entity*, e.g. the commercial payments department of the Commercial Bank or the information systems security area with specific requirements for the internal/external context, with target values of the evaluation criteria and specific metrics for criteria measurement. Furthermore, PISI can be used for measurement and assessment of InfoSec maturity either in internal self-assessment missions or in external conformity assessment missions and / or advisory missions and / or to compare the maturity of some typical organizations belonging to a certain industry. The PISI assessment report reflects the scope and current status of the InfoSec, the specific risks and threats, and suggests recommended targets for improvement.

Keywords: Information Security Management System (ISMS), Statement of Aplicability (SoA), Multipurpose Information Security Maturity Model (ISM3), Individual Information Security Profile (ISP), Information Security (InfoSec), target criteria evaluation, measurement criteria.

https://doi.org/10.33436/v32i1y202208

1. Introducere

Actualitatea. Astăzi, majoritatea absolută a persoanelor fizice și juridice, a organizațiilor private, publice, guvernamentale etc. sunt prezente în spațiul virtual global, fără a avea frontiere bine delimitate. Acest lucru constituie o sursă majoră a riscurilor de securitate pentru datele personale și informațiile sensibile manipulate în spațiul cibernetic și care sunt valoroase pentru o persoană fizică, organizație, regiune sau un stat. Ca urmare, asigurarea securității informației în spațiul cibernetic devine o preocupare majoră a tuturor actorilor implicați la diferite niveluri, pornind de la persoane fizice *(protecția datelor personale),* organizații particulare și publice *(universități, școli, spitale, primării, bănci etc.);* și terminând cu nivelul organelor guvernamentale de reglementare și supraveghere *(ministerul educației, ministerul sănătății, ministerul finanțelor, banca națională, inspectoratul fiscal de stat etc.),* unde se concentrează responsabilitatea elaborării și aplicării de politici de securitate coerente în domeniul respectiv la nivel de stat sau la nivel global pe anumite industrii. Importanța securității informației a crescut esențial în ultimii doi ani, o dată cu izolarea impusă de pandemia COVID-19 și cu migrarea *„peste noapte"* a majorității organizațiilor spre telemuncă, cu accesarea online a datelor sensibile.

Marea problemă este că, în prezent, atât la nivel național cât și la nivel internațional se vehiculează mai mulți termeni apropiați, cum ar fi: *securitatea informațională, securitatea informației, securitatea cibernetică, securitatea informatică, securitatea IT etc.* și că se atestă o multitudine de standarde/cadre de abordare cât și de reglementare a securității cibernetice, tehnologia informației și sistemelor informaționale în spațiul virtual, cu un număr foarte mare de controale: 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"* (Bragaru et al., 2019). Marea diversitate a termenilor apropiați, a cadrelor de reglementare și a controalelor de SecInf, aplicate la diferite niveluri, pentru diferite industrii, complică și îngreunează determinarea/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.

Scop urmărit. Sarcina de implementare a SMSI și de îmbunătățire continuă a proceselor de gestionare a SecInf într-o entitate concretă trebuie să corespundă obiectivelor afacerii, cerințelor contextului intern și mediului extern de reglementare și de supraveghere; să țină cont de specificul industriei și de starea curentă a SecInf, de riscurile informaționale, de cultura informațională corporativă și cea a personalului implicat în SecInf etc. Ca urmare, pentru a construi, organiza și asigura cu succes securitatea informației într-o entitate, pornind de la analiza necesității, identificării cerințelor, riscurilor etc., este nevoie de un model individual simplu, transparent și ușor de personificat și 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 unui asemenea PISI necesită cheltuieli importante de bani și de timp, precum și un personal înalt calificat. Automatizarea și intelectualizarea procesului de realizare PISI și a evaluării nivelului de maturitate al SMSI conform acestui model ar putea soluționa problema. În acest sens, rezultatele preconizate presupun adoptarea unui cadru generic unic și anume, un model multiprofil de maturitate a SecInf M^3SI cu o bază de date unică privind cunoștințele de SecInf, din care pot fi generate în mod inteligent profiluri particulare ale SecInf, potrivite necesităților concrete de analiză, măsurare și îmbunătățire continuă a SecInf. Modelul M^3SI și profilurile particulare 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 scopului au fost realizate următoarele **obiective majore**:

- studiul diverselor cadre de abordare și de reglementare a securității informației, analiza și cartografierea relațiilor dintre ele cu crearea unei baze generice de date M^3SI privind

cunoștințele despre cadre, zone, cerințe, amenințări, riscuri și controale de SecInf, inclusiv specifice pentru diferite industrii;

- elaborarea aplicației instrumentale de administrare a modelului multiprofil M[3]SI și a profilurilor personificate PISI;
- generarea, aprobarea și validarea unor profiluri PISI tipice pentru activitatea bancară, respectiv pentru o bancă comercială concretă;
- evaluarea nivelului de maturitate a unei entități conform profilului PISI.

Metodologia utilizată. Pentru a determina starea actuală a SMSI și direcțiile prioritare de dezvoltare a acestuia, este utilizat așa numitul „model de maturitate" (MM), general acceptat la nivel global, de exemplu a se vedea (O-ISM3, 2017), (Rabii et al., 2020), (Bilge et al., 2021). 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 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 sale continue.

Importanța/valoarea aplicativă a rezultatelor obținute constă în funcționarea cât mai sigură a organizațiilor. Profilurile tipice PMSITI 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 cât mai sigură a obiectivelor de afaceri.

Aplicația instrumentală de suport M[3]SI simplifică și ușurează esențial munca în teren, automatizând operațiile rutinare de administrare a bazei de date cu cunoștințele despre amenințări *(care exploatează vulnerabilitățile și duc la pierderi de active),* riscuri, cerințe și controale specifice, de generare a profilurilor particulare și de evaluare a nivelului de maturitate. Aplicația M[3]SI este de tip web cu acces controlat. Toate acestea luate împreună permit diferitelor entități *organizarea, abordarea și gestionarea eficientă a securității informației,* prevenirea și combaterea cât mai eficientă a riscurilor și amenințărilor la adresa securității informației.

2. Cadrul conceptual general și definitoriu de securitate a informației

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 lucrare numite generic **entități**.

2.1. Similitudinea conceptelor de securitate cibernetică și securitate a informației

Fără a intra în prea multe detalii, termenii de *Securitate a informației și Securitate cibernetică* pot fi considerați sinonimici, ținând cont de faptul că actualmente, informațiile sunt preponderent în format digital, și că ambele concepte se referă la „*conservarea confidențialității, integrității și disponibilității informației"* (The ISO27k Standards), inclusiv *„în spațiul cibernetic"* (ISO/IEC 27032:2012). Cele trei caracteristici primare fundamentale ale informației, care constituie obiectul SecInf, sunt referite în literatura de specialitate ca triada CIA *(Confidentiality, Integrity and Availability).*

Astfel, prin securitatea informației vom înțelege setul de orice fel de controale (preventive, detective, corective) și proceduri ce asigură caracteristicile primare și secundare ale informației și ale tuturor activelor informaționale din cadrul entității, inclusiv personal, tehnologii informaționale și comunicaționale (TIC), servicii de suport etc. pentru a ține sub control incidentele de securitate 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. În marea majoritate a cazurilor, securitatea cibernetică acoperă cca 95% din securitatea informației (Bragaru et al., 2019), având în vedere că doar o mică parte a activelor informaționale continuă să circule în format tradițional pe hârtie.

2.2. Focusarea cercetării

Problemele, amenințările, riscurile, soluțiile, costurile SecInf sunt diferite pentru anumite organizații, industrii și domenii de activitate *(e.g. educație, medicină, servicii bancare, e-afaceri, e-guvernare),* deoarece sunt altele cerințele și contextele interne/externe, infrastructurile, produsele utilizate și personalul implicat. SecInf poate fi extrem de diferită, îndeosebi pentru diferitele industrii și întreprinderi de diverse mărimi, în special mici-medii, care nu dispun de personalul și instrumentele necesare. În general, SecInf include: securitatea infrastructurilor critice *(tehnologiile informaționale (IT), sistemele informaționale (IS), rețele private/intranet, internet și extranet etc.)*, securitatea web și securitatea bazelor de date și 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 este modelul/profilul individual al SecInf pentru o oarecare organizație sau o parte a acesteia, independent 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 experimentate de generare a profilurilor particulare de SecInf în baza unui model generic, precum și a activităților de apreciere a riscurilor, inclusiv de colectare a măsurărilor și de evaluare a nivelului de maturitate.

2.3. Paradigme, principii și cadre de abordare a SecInf

Paradigma actuală a SecInf este în proces de trecere de la modelul concentrat pe probleme tehnice, gestionate la nivel de IT 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 de afaceri *(Briceag & Bragaru, 2020).* Numeroasele cadre/standarde de securitate examinate servesc pentru crearea bazei de date a aplicației M^3SI și identificarea domeniilor de interes pentru profilurile individuale.

2.3.1. Principii de abordare a SecInf

Oricare ar fi paradigma și cadrul de abordare, conceptul modern al securității informației unei organizații are la bază domeniile, obiectivele și controalele standardelor formatoare ISO/IEC 27001:2013, seria NIST SP 800-53 rev.5 (2020) sau COBIT 2019. În toate cazurile este aplicată abordarea procesuală PDCA (Plan-DO-Check-Act) și îmbunătățirea continuă ca cerință-cheie. Alte cadre standard, e.g. PCI DSS, ISO/IEC 27032, ISO/IEC 27033 etc. au rolul preponderent de *suport tehnic specific domeniului, contextului, controlului* etc. ținând cont de misiunile și țintele urmărite.

Totodată, în realizarea SMSI și gestionarea SecInf sunt utilizate o serie de alte principii și paradigme. De exemplu, zece principii sunt examinate în *(O-ISM3, 2017),* printre care sunt demne de menționat: *Abordarea bazată pe risc, Arhitectura zero trust (ZTA), Privilegii minimale, Securitate prin design, Apărarea în profunzime, Paradoxul lui Mayfield* și altele, unele dintre ele sunt expuse succint în continuare.

Abordarea bazată pe risc. Crearea unui profil particular al controalelor de securitate pentru o organizație presupune o analiză minimă a riscurilor de securitate 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. Pentru mai multe detalii a se vedea *(Briceag & Bragaru, 2021).*

Arhitectura zero trust sau zero încredere *(NIST SP 800-207:2020)* 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 telemuncii 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 (W210, 2021).*

2.3.2. Cele mai răspândite cadre/bune practici/modele de abordare a SecInf

Astăzi ne aflăm într-o societate informațională globală în care organizațiile de la mici și mari, publice și private au sarcina de a respecta multiplele politici, cadrele legale de reglementare în domeniul securității cibernetice la nivel global, național și local. La nivel global, cel mai universal și recunoscut cadru de abordare al SecInf este *ISO/IEC 27001:2013*, reconfirmat de ISO și IEC în 2019. Familia *ISO/IEC 27000 (ISO 27k)* 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 este o normă internațională formatoare cu peste șaizeci de standarde 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 27001:2013, 14 domenii, 114 controale),* securitatea în Cloud (ISO/IEC 27017), securitatea cibernetică (ISO/IEC 27032) și securitatea în rețea *(ISO/IEC 27033, 6 părți).* Conform ISO/IEC 27001:2013, SMSI realizează gestionarea SecInf la trei niveluri:

- strategic, care se ocupă de obiective pe termen lung și furnizarea de resurse;
- tactic, care se ocupă de obiective specifice pe termen scurt și gestionarea resurselor;
- operațional, care 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 IT)* 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 IT/IS, ci și în construirea unui sistem eficient de management al informației și tehnologiei informației, adecvat obiectivelor stabilite de conducere a organizației. COBIT 2019 include 5 domenii de management *(Evaluare, direcționare și monitorizare (EDM); Aliniere, planificare și organizare (APO); Construire, achiziționare și implementare (BAI); Livrare, service și asistență (DSS); Monitorizare, evaluare și apreciere (MEA))* cu sumarul de patruzeci de procese. Pentru detalii a se vedea *(COBIT®, 2019).*

Un alt cadru elaborat de National Institute of Standards and Technology (NIST) SUA, utilizat pe larg în toată lumea pentru gestionarea securității cibernetice, este seria de publicații speciale **NIST SP 800.** 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 *(Health Insurance Portability and Accountability Act*). Însă cea mai importantă este seria NIST SP 800-53 rev.5, în 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)** 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 necesită 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) 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 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.

3. Cadrul conceptual al modelului de maturitate multiprofil

Maturitatea este o măsurare a capacității unei organizații de îmbunătățire continuă a unor domenii de management (O-ISM3, 2017). De exemplu, Modelul de Maturitate a Capacității (CMM) (Diogo & José, 2018) este orientat pe procese și abordarea procesuală PDCA (Plan-Do-Check-Act). La fel și modelul de maturitate a calității, care este promovat de ISO 9000:2015, și modelul de maturitate a securității informației, promovat de ISO/IEC 27001, se bazează pe abordarea procesuală și metrici specifice. 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. Aceasta este ideea de bază, susținută în cadrul lucrării sub conceptul de PISI, dezvoltat conform necesităților specifice ale entității, așa cum îl vede entitatea, cu metricile de care are nevoie. Iar modelele de maturitate generice sunt întrunite în cadrul unui model multiprofil, ca bază generică comună de cunoștințe.

În linii mari, PISI, ca modele de maturitate ale SMSI, sunt menite 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 se poate 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.

3.1. Securitatea informației bazată pe modelul de maturitate

În esență, modelele de maturitate reprezintă seturi de bune practici globale dovedite, 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, COBIT, ITIL, ISO 9001:2015 etc. în general sunt compatibile cu cerințele ISO 27001, nu există o înțelegere clară a relaționării domeniilor și proceselor de bază folosite de acestea. Spre deosebire de diferitele cadre ale SecInf oferite de bunele practici/standarde internaționale și

modelele de maturitate izolate, modelul multiprofil al maturității securității informației M^{3}SI oferă o imagine universală și unică 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 PMSITI și terminând cu nivelul de aplicare local/profiluri particulare PISI, specifice cerințelor și contextelor concrete al unei organizații, misiuni etc.

Un **Model de maturitate personificat** permite 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 nivele 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. Obiectele evaluării maturității conform profilurilor particulare pot fi: 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/îmbunătăți și altele. De exemplu, ca obiecte ale 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/acreditare etc.

Indiferent de modul de utilizare, zonele SMSI și profilul PISI sunt 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.

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 PMSITI și a profilurilor derivate PISI.

3.2. Modelul mutiprofil de maturitate al Securității Informației (M^{3}SI)

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^{3}SI asupra SecInf din partea părților-cheie este primordială pentru o entitate. Viziunea M^{3}SI acoperă întreaga organizație, de la consiliul de administrație spre executiv, ofițer de securitate a informației, specialiști în securitate IT/IS, manageri de risc, până la toți angajații care utilizează IT/IS în activitățile lor. Provocarea realizării acesteia devine din ce în ce mai mare pe măsură ce organizațiile migrează spre munca online, la distanță, mediată de Internet și TIC moderne (telemunca). 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.

M^{3}SI este conceput pentru a face față provocărilor de SecInf. M^{3}SI presupune metode eficiente de analiză, măsurare, evaluare și apreciere a SecInf nu doar pentru un anumit obiect izolat în schimbare, ci și pentru un grup 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 PMSITI, având la bază domenii de SecInf *(e.g. oameni, procese, infrastructură IT, IS utilizate)*, obiective, măsuri/controale de securitate și metrici sau ținte ale criteriilor de evaluare din M^{3}SI *(Figura 1)*.

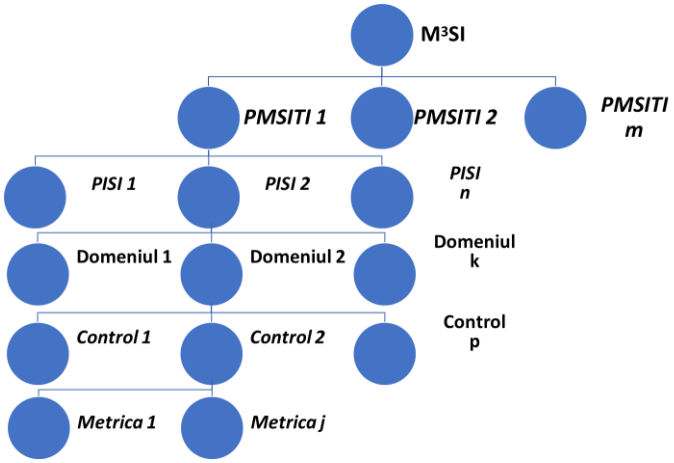


Figura 1. O viziune ierarhică simplificată a M³SI

La cel mai de sus nivel, M³SI include zone/domenii de SecInf conform cadrelor generale de abordare corelate (prin cartografiere), e.g. ISO/IEC 27001:2013, NISP SP 800, COBIT 2019. A se vedea și *(CMMC 1.2, 2020), (Bilge et al., 2021), (Rabii et al., 2020).* Modelul multiprofil acoperă mai multe 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.).* Evident, pentru fiecare dintre ramurile și entitățile tipice există diferite reglementări la nivel național și local, cu cerințe specifice cazului concret, 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 *„Hotărârea Comitetului Executiv al Băncii Naționale nr. 237 din 26 septembrie 2018 Cu privire la modificarea Regulamentului cu privire la sistemul automatizat de plăți interbancare”;* la nivel local *„Regulament intern al Băncii Comerciale”*. Domeniile de securitate și controalele specifice sunt conform cerințelor de securitate specificate fie în ISO 27001:2013, fie în publicația specială NIST SP 800-53 rev.5, (2020) sau în alte cadre de abordare, cartografiate în cadrul aplicației. Detalii privind scările nivelului de maturitate pot fi găsite în (Briceag & Bragaru, 2020).

Criteriile de evaluare sunt autoritare și oferă o bază de cunoștințe (controale pe domenii), pentru ca mai mulți evaluatori să poată ajunge la aceleași rezultate în evaluarea repetată a unor practici/controale/procese prezente în PISI. Caracteristicile modelului multiprofil M³SI și a profilurilor rezultante PMSITI și PISI, expuse mai jos, permit nu doar generarea intelectuală a unui PISI în baza PMSITI și M³SI, foarte utilă și necesară pentru marea majoritate a utilizatorilor, ci și modificarea acestora de către experți cu adăugarea în baza de date a noilor cunoștințe:

- Flexibilitate – procesele pot fi definite în concordanță cu obiectivele propuse în diverse cadre, inclusiv combinate din două sau mai mute cadre;
- Modularitate – modelul este împărțit pe zone de procese și pe niveluri ierarhice distincte;
- Scalabilitate – modelul se poate folosi 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 pot fi implementate incremental, pe etape/niveluri de maturitate, în funcție de dimensiunea organizației, țintele și aspectele pe care aceasta se focusează la momentul respectiv.

3.2.1. Particularitățile modelelor tipice unor industrii PMSITI

De regulă, cerințele specifice de SecInf pentru diversele industrii sunt formulate în standarde și reglementări specifice *(e.g. PCI DSS, GDPR)*, acte global aplicabile *(e.g. HIPAA)*, și

reglementări locale ale organelor de supraveghere. Profilul de maturitate PMSITI ar putea specifica aceste cerințe pentru satisfacerea necesităților managementului *(Figura 2)*.

ID	Nume Control	Descriere	Risk	Niveluri de Maturitate	Actiuni
1	+ Cadrul de organizare a securităţii informaţiei				
2	+ Managementul resurselor informaţionale				
3	+ Securitatea Resurse Umane				
4	- Securitatea fizică şi a mediului de lucru				
4.1	Zone de securitate	să prevină accesul fizic neautorizat, distrugerile şi pătrunderile în interiorul băncii, precum şi accesul la resursele informaţionale.		1. Controalele sunt doar partial definite si/sau executate intr-un mod inconsecvent 2. Controalele sunt in vigoare si executate doar intr-un mod structurat si consecvent, dar informal 3. Controalele sunt documentate si executate intr-un mod structurat, formal si dovedit 4. Eficacitatea controalelor este evaluata si verificata periodic pentru calitate 5. A fost creat un sistem ecologic care sa asigure un control continuu si eficient si sa rezolve riscurile	Editeaza Sterge
4.2	Securitatea echipamentelor	să prevină pierderea, distrugerea, furtul sau compromiterea echipamentelor TI şi întreruperea proceselor de activitate ale băncii.		1. Controalele sunt doar partial definite si/sau executate intr-un mod inconsecvent 2. Controalele sunt in vigoare si executate doar intr-un mod structurat si consecvent, dar informal 3. Controalele sunt documentate si executate intr-un mod structurat, formal si dovedit 4. Eficacitatea controalelor este evaluata si verificata periodic pentru calitate 5. A fost creat un sistem ecologic care sa asigure un control continuu si eficient si sa rezolve riscurile	Editeaza Sterge
5	+ Managementul comunicaţiilor şi operaţiunilor				
6	+ Controlul accesului la resursele informaţionale				
7	+ Achiziţionarea, dezvoltarea şi mentenanţă sistemelor de aplicaţii				
8	+ Managementul incidentelor de securitate a informaţiei				
9	+ Managementul continuitatii activitatii				
10	+ Conformitatea				
11	+ Auditul intern al securităţii informaţiei				

Figura 2. Un fragment de PMSITI pentru activitatea bancară din Republica Moldova

Modelul PMSITI 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 particular sau pentru compararea maturității diferitelor entități tipice.

3.2.2. Generarea profilurilor individuale de maturitate (PISI)

Deoarece măsurile și controalele securității sunt derivate din situațiile statice și/sau dinamice concrete de funcționare ale organizației și misiunii evaluării, PISI ar trebuie particularizate/ interpretate de la caz la caz în baza unui PMSITI sau a unui PISI similar. Orice entitate concretă își va crea propriul profil PISI conform contextului său specific, care va ține cont de aria SMSI/SoA și țintele stabilite. Un fragment de PISI a se vedea în *Figura 3*.

ID	Nume Control	Descriere	Nivel curent	Evidente
1	- Cadrul de organizare a securităţii informaţiei		3.25	
1.1	Politica de securitate a informaţiei	să asigure orientarea generală de management şi sprijinul pentru securitatea informaţiei în conformitate cu cerinţele de afacere, legislaţia şi actele normative aplicabile.	3	lista
1.2	Organizarea SMSI	să asigure cadrul intern adecvat pentru managementul securităţii informaţiei.	4	lista
1.3	Relaţia cu terţele părţi	să asigure securitatea informaţiei în relaţia cu terţele părţi care prestează sau beneficiază de servicii ce implică informaţia băncii	3	lista
1.4	Externalizarea serviciilor TI	să asigure securitatea şi continuitatea serviciilor TI externalizate către furnizori externi de servicii.	3	lista
2	- Managementul resurselor informaţionale		2.67	
2.1	Responsabilitatea pentru resurse	să asigure stabilirea şi asumarea responsabilităţii pentru protecţia corespunzătoare a resurselor informaţionale ale băncii.	3	lista
2.2	Clasificarea informaţiei	să asigure faptul că informaţia beneficiază de un nivel de protecţie adecvat, proporţional importanţei ei, reglementărilor aplicabile şi ameninţărilor aferente	2	lista
2.3	Managementul riscurilor	să asigure faptul că banca isi gestioneaza riscurile intr-o maniera eficace si eficienta	3	lista
3	- Securitatea Resurse Umane		3.00	
3.1	Înainte de angajare	să asigure faptul că noii angajaţi, terţele părţi, precum şi reprezentanţii acestora sunt corespunzător verificaţi înainte de acordarea accesului la sisteme, iar responsabilităţile pentru securitatea informaţiei sunt adecvat stabilite, comunicate şi asumate.	4	lista
3.2	Instruirea	să asigure faptul că cerinţele de securitate sunt cunoscute în măsură suficientă de către angajaţii băncii, terţele părţi, precum şi reprezentanţii acestora.	3	lista
3.3	Pe perioada angajării	să asigure faptul că cerinţele de securitate sunt respectate necondiţionat de către angajaţii băncii, terţele părţi, precum şi de reprezentanţii acestora, iar responsabilităţile şi răspunderea juridică ale acestora sunt stabilite şi conştientizate corespunzător.	3	lista
3.4	Încetarea contractului sau schimbul locului de muncă	să asigure faptul că angajaţii, terţele părţi, precum şi reprezentanţii acestora încetează relaţia cu banca într-o manieră controlată din punct de vedere al riscurilor de securitate.	2	lista
4	- Securitatea fizică şi a mediului de lucru		3.50	
4.1	Zone de securitate	să prevină accesul fizic neautorizat, distrugerile şi pătrunderile în interiorul băncii, precum şi accesul la resursele informaţionale.	4	lista
4.2	Securitatea echipamentelor	să prevină pierderea, distrugerea, furtul sau compromiterea echipamentelor TI şi întreruperea proceselor de activitate ale băncii.	3	lista

Figura 3. Un fragment de PISI pentru o bancă ipotetică

PISI mai conține și Nivelul de maturitate așteptat, Nivelul de maturitate identificat, Lista de probe și argumente de rigoare atașate care documentează nivelul de maturitate identificat. În ultimă instanță, rezultatul evaluării conform PISI permite identificarea etapelor/pașilor de îmbunătățire continuă a securității informației, succint expuse în continuare. Totodată, este posibilă și acumularea istoricului privind domeniile și îmbunătățirile incrementale, care pot apărea în entitatea analizată de la o lună la alta, de la un trimestru la altul sau de la un an la altul, în funcție de frecvența impusă de cerințele afacerii.

3.3. Evaluarea nivelului de maturitate pentru o entitate concretă/un profil PISI

PISI permite entității să se pronunțe asupra modului în care funcționează SMSI, precum și identificarea punctelor slabe ale SMSI și planificarea remedierii eventualelor deficiențe. Totodată, PISI furnizează o evaluare unică, în urma căreia este permisă nu doar compararea internă și dinamică în timp a nivelurilor de maturitate pe domeniile/procesele SMSI, 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.

De regulă, fiecare PISI are propriile sale metrici, orientate spre atingerea obiectivelor specifice. Iar determinarea maturității se bazează pe revizuirea documentației SMSI, intervievarea personalului, efectuarea unor măsurători, a unor analize a discrepanței pentru fiecare dintre domeniile de securitate incluse în PISI și valorile măsurate. Evaluarea nivelurilor pentru fiecare dintre domeniile PISI se realizează conform criteriilor elaborate/metricilor modelului. De exemplu, scorul de măsurare a îndeplinirii criteriului poate fi „Conform”, „Conform parțial”, „Neconform”. 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. Rezultatul evaluării se afișează inclusiv în diagrame de tip radar (Figura 4).

Figura 4. Un fragment al raportului de evaluare pentru o bancă ipotetică Alfa

4. 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 și versiuni profesionale cu plată. De exemplu, Instrumentul de autoevaluare a controalelor *Controls Self-Assessment Tool de la Center of Internet Security, (CIS CSAT)* versiunea 8 din 2020 promovat și de către Institutul SANS cu o listă dinamică a măsurilor de securitate, permite organizațiilor să evalueze și să urmărească implementarea controalelor CIS în vederea conformării.

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 alte instrumente răspândite prin: a) actualizarea și sistematizarea cunoștințelor despre cadrele de abordare în vigoare și bune practice privind SecInf în Baza de Date (BD) cumulativă;

b) acumularea istoricului evaluării nivelurilor de maturitate conform PISI și urmărirea dinamicii; c) asigurarea comparabilității evaluării din contul formalizării criteriilor de evaluare și a metricelor de SecInf; d) aplicabilitatea universală, nu doar pentru cazuri concrete e.g. „Top 20 CIS Controls", care sunt orientate preponderent spre Internet.

Pentru a utiliza aplicația care integrează modelul generic PMSITI și PISI, evaluatorul trebuie:

1. Să definească aria de aplicabilitate a SMSI sau a misiunii de evaluare, pornind de la modelul tipic industriei, prin eliminarea/adăugarea/modificarea, la nevoie a unor controale specifice în M^{3}SI și PMSITI, dictate de necesitățile și constrângerile organizației;
2. Să genereze profilul individualizat de maturitate al securității informației PISI (Eventual prin identificarea unui PISI similar/apropiat și adaptarea lui sau prin construirea inițială a PISI prin combinarea domeniilor de control și controalelor aferente în conformitate cu riscurile și amenințările caracteristice pentru industria și entitatea dată);
3. Să selecteze/completeze chestionarele/listele de întrebări și/sau metricile criteriilor respective (din meniurile derulante de pe paginile fiecărui control, inclus în PISI). În baza răspunsurilor la fiecare întrebare (alegerii unor opțiuni din listele derulante sau a introducerii rezultatelor măsurărilor criteriilor de evaluare) aplicația determină în mod automat scorurile nivelului de maturitate conform metricilor furnizate pe domenii/controale, după care afișează „Raportul" rezultant al evaluării cu diagrame de tip radar și/sau diagrame detaliate sub forma unor bare color pe domeniile de control conform scării/culorilor matricei de analiză a riscurilor (Briceag & Bragaru 2021).
4. Să efectueze recomandările 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 (cel mai înalt nivel de maturitate).

4.1. Interfața aplicației M3SI și scenariul de utilizare

Interfața aplicației M^{3}SI este intuitivă *(Figura 5)*, iar pașii scenariului de utilizare includ actualizarea PISI (eventual și a bazei de cunoștințe) conform misiunii, realizarea evaluării, documentarea și afișarea rezultatelor evaluării.

Figura 5. Fragment al interfeței aplicației M^{3}SI

4.1.1. Baza de date a aplicației

Baza de date (BD) a modelului M^{3}SI 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^{3}SI, care să corespundă nevoilor generale și specifice de îmbunătățire a performanței. Nucleul BD îl constituie harta/tabelul comun al referințelor încrucișate a ariilor, controalelor,

criteriilor de evaluare a celor mai răspândite cadre de SecInf, e.g OISM3:2018, NIST SP:2018, . familia ISO 27k, inclusiv ISO/IEC 27001:2013, ISO/IEC 27004, ISO/IEC 27032:2012,. ISO/IEC 27033 (2012-2016), PCI DSS 3.2.1 (2018, COBIT 5:2012, COBIT:2019, ISO/IEC 20000-1:2018 ITIL v4:2019; harta structurată a amenințărilor conform (ENISA, 2020), nomenclatoare de vulnerabilități și cataloage de risc recunoscute la nivel global (e.g. ISO/IEC 27005:2018, CVE:2021, CIS Controls v8 (2020)) etc.

Aplicația conține și cartografierea relațiilor dintre controalele cu referire la clauzele respective ale cadrelor mapate. Aceasta este necesară/ajută atât la o mai bună înțelegere a controalelor, cât și la buna organizare și monitorizare a SecInf pe domenii/zone prin precizări specifice ale criteriilor și măsurărilor nivelului de maturitate, specificărilor tehnice și altor atribute necesare pentru dezvoltarea unei bune strategii de guvernanță a SecInf.

5. Concluzii finale

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. Pe de altă parte, este dificil să se aplice modele de maturitate personificate fără a înțelege modelul de bază/enunțul general al problemei 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 PMSITI, 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. Toate acestea 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.

În esența sa, M^{3}SI reprezintă o bază de date generică, cumulativă, adaptabilă și extensibilă privind cunoștințele despre cadrele de abordare, zonele, controalele, criteriile și țintele de SecInf, din care pot fi generate profiluri tipice unor industrii PMSITI (*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. Numărul nivelurilor de evaluare a maturității este de 5. PISI face referință la capacitățile-cheie ale SMSI, controale, teste/chestionare și șabloane tipice de evaluare și măsurare a nivelului de maturitate, care sunt destinate pentru aprecierea *(măsurarea-evaluarea)* și/sau pentru îmbunătățirea continuă a SMSI, care să răspundă atât propriilor nevoi și politici particulare de securitate a informației specifice organizației, cât și celor globale. Aplicația aferentă oferă suport inteligent de generare a profilurilor de evaluare consistentă pentru maturizarea SecInf prin îmbunătățirea sa continuă.

Abordarea *„model multiprofil – profil tipic – profil particular”* și aplicația respectivă M^{3}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, și să asigure raportarea/informarea, cât și pentru toți cei care au nevoie de acces la informațiile de securitate. M^{3}SI posedă următoarele caracteristici:

a. Este o platformă integrată de concepere, dezvoltare, evaluare și îmbunătățire continuă a securității cibernetice a entității, o metodă practică de determinare a riscului de securitate a informației și măsurare obiectivă a capacității de a le atenua pe cele mai importante riscuri prin identificarea decalajelor dintre capacitățile actuale ale organizației și nivelul de maturitate necesar stabilit de cadrul legal;

b. Oferă o sursă de informații obiective și consistente, pe care auditorii și organele de supraveghere le pot folosi pentru a înțelege, evalua și gestiona eficient riscurile.

c. Consiliul de conducere poate obține informații calitative și rapide asupra stării SecInf. Aplicația poate crea rapid rapoarte și diagrame vizuale privind starea, obiectivele și necesitățile de îmbunătățire a SecInf, bazate pe dovezi documentate;

d. Ofițerii de SecInf și echipele de profesioniști de Securitate IT/IS/Cibernetică etc. pot elimina o mare parte a rutinei privind planificarea sarcinilor de viitor, colectarea, documentarea și aprecierea nivelului de maturitate al SecInf; pot determina cu ușurință cât de bine capacitățile organizației se aliniază cadrelor/reglementărilor de securitate comune și propriilor politici de securitate și pot genera o foaie de parcurs pentru îmbunătățirea securității informației entității.

În practică, multor organizații le este greu să obțină o viziune unică, obiectivă, comprehensibilă a riscurilor și capacităților de securitate cibernetică, aceasta necesitând timp îndelungat. Complexitatea este un factor foarte important în realizarea unei viziuni unice și obiective a riscurilor și capacităților de securitate cibernetică. Riscurile sunt în creștere continuă, cauzată de integrarea noilor aplicații TIC, apariția noilor vulnerabilități, amenințări, atacuri etc. Planificarea-evaluarea conform modelelor multiprofil și criteriilor de evaluare, devin mai transparente, mai simplu și mai ușor de înțeles și de aplicat.

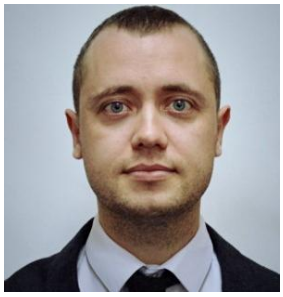
O altă problemă, uneori și mai mare, este felul în care informațiile privind securitatea cibernetică sunt colectate, gestionate, raportate/difuzate către rolurile respective, ceea ce face extrem de dificilă monitorizarea și suportul în timp real.

Momentan, evaluarea și urmărirea securității informatice prin colectarea și înregistrarea „manuală" a informațiilor pe foi de calcul sau alte instrumente pentru a urmări numeroasele amenințări, inițiative/proiecte, programe și procese de securitate și alinierea acestora la diferite reglementări și cadre, nu mai este eficientă. Devine extrem de dificilă nu doar colectarea de date și evaluarea, ci și actualizarea și păstrarea consistenței numeroaselor documente pentru obținerea unei imagini coerente asupra tuturor aspectelor securității cibernetice. În mod ideal, pe termen lung, organizațiile ar putea implementa/extinde aplicația pentru a automatiza colectarea celor mai multe dintre datele inițiale/măsurări ale criteriilor, metricilor etc. Iar în viitor, M^{3}SI ar putea colabora cu alte instrumente simulare inclusiv la nivel de import/export de date.

BIBLIOGRAFIE

1. Amenințări generice la adresa securității cibernetice, ENISA (2020). https://dnsc.ro/vezi/document/amenintari-generice-securitate-cibernetica/.
2. Bilge, Y. O., Sonny van Lingen & Marco, S. (2021). The Cybersecurity Focus Area Maturity (CYSFAM), 2021. www.mdpi.com/journal/jcp.
3. 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.
4. Briceag, V., Bragaru, T. (2020). *Evaluarea securității informației organizației în baza unui model de maturitate*. În Materialele Conferinței științifico-practice internaționale „Teoria și practica administrării publice", Chișinău, AAP, 2020, pp. 248-252.
5. Briceag, V., Bragaru, T. (2021). *Evaluarea riscului securității cibernetice.* Revista Economica, 2(122), SEP ASEM, 2021, pp. 138-147.
6. CIS Controls v8 (2020). *Cybersecurity Maturity Model Certification Mapping*. https://www.cisecurity.org/white-papers/cis-controls-v8-cybersecurity-maturity-model-certification-mapping/.
7. *Cybersecurity Maturity Model Certification v.1.02* (2020). CMMC 1.2, 2020. https://www.acq.osd.mil/cmmc/draft.html.
8. *COBIT® 2019*. Framework: Governance and Management Objectives. ISACA, 2019.
9. *Common Vulnerabilities and Exposures* (CVE, 2021). https://cve.mitre.org/cve/.

10. 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.
11. *General Data Protection Regulation*. GDPR, (2016). https://gdpr-info.eu/.
12. ISO/IEC 27001:2013. Information Technology. Security Techniques. Information security management systems. Requirements.
13. The ISO27k *Standards*. https://www.iso27001security.com/ISO27k_Standards_listing.pdf.
14. ISO/IEC 27032:2012 IT. *Security Techniques*. Guidelines for cybersecurity (first edition).
15. ISO/IEC 27033:2012-2016 IT. *Security Techniques*. Network security (part 1-6).
16. Mayfield, R., Cvitanic, J. (2001). *Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information Security*. Information Systems Control Journal, 2, ISACA, pp. 32-35.
17. NIST 800-207 Zero Trust Architecture (2020): https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-207.pdf.
18. *Open Information Security Management Maturity Model* (O-ISM3, 2017), Version 2.0, 130 p.
19. *Payment Card Industry Data Security Standard (PCI-DSS 3.2.1, 2018)*. History and Overview. https://www.truvantis.com/pci-dss-history-and-overview/.
20. Rabii, A., Assoul, S., Ouazzani Touhami, K., Roudies, O. (2020). *Information and Cyber Security Maturity Models: A Systematic Literature Review*. Inf. Comput. Secur. 2020, 28, pp. 627–644.



Valentin BRICEAG este doctorand la Universitatea de Stat din Moldova, specialitatea Tehnologii, Produse și Sisteme Informaționale, deține o diplomă de licență în tehnologii informaționale și un master în tehnologii de rețea. Este specializat în managementul riscurilor de securitate a informației.

Valentin BRICEAG is a PhD student at the Moldova State University, specializing in Information Technology, Products and Systems, has a bachelor's degree in information technology and a master's degree in network technology. He is specialised in information security risk management.