Universitatea Politehnica Timișoara
Şcoala Doctorală de Studii Inginereşti
Domeniul de doctorat: Inginerie şi Management

REZUMATUL TEZEI DE DOCTORAT

CONTRIBUTIONS TO CYBERSECURITY RISK MANAGEMENT: IoT SECURITY RISK MANAGEMENT STRATEGY REFERENCE MODEL (IoTSRM2)

CONTRIBUŢII ÎN MANAGEMENTUL RISCULUI DE SECURITATE CIBERNETICĂ: MODEL DE REFERINŢĂ PENTRU STRATEGIA DE MANAGEMENT AL RISCULUI SECURITĂŢII CIBERNETICE PENTRU INTERNETUL OBIECTELOR (IoTSRM2)

Doctorand: **Ing. Traian Mihai POPESCU**

Conducător ştiinţific: **Prof. dr. ing. Gabriela PROȘTEAN**

Timișoara 2021

Cuprins

Cuprins Teză

Capitolul 1. Introducere

Capitolul 1 oferă fundalul, motivaţia, obiectivele, şi structurarea acestei teze de doctorat.

În primul rând, **Capitolul 1.1** este structurat în două părţi: prima parte oferă fundalul („background") managementului riscului de securitate cibernetică şi a doua parte oferă fundalul privind internetul obiectelor („Internet of Things" – IoT). Astfel, cu privire la fundalul managementului riscului de securitate cibernetică, subcapitolul schiţează unele dintre posibilele implicaţii pentru organizaţiile care operează în era actuală a transformărilor digitale din perspectiva securităţii cibernetice, introduce câteva concepte-cheie de management al riscului de securitate cibernetică, şi oferă prezentări generale ale mai multor standarde şi metodologii de management al riscului de securitate cibernetică. În ceea ce priveşte posibilele implicaţii pentru organizaţiile care adoptă progresele tehnologice, acestea includ lărgirea suprafeţei de atac („attack surface"), evoluţia continuă a peisajului ameninţărilor cibernetice, cadrul din ce în ce mai mare de reglementare privind securitatea cibernetică, şi, în consecinţă, necesitatea îmbunătăţirii continue a practicilor de management al riscului de securitate cibernetică în organizaţii. În plus, subcapitolul defineşte şi prezintă unele dintre principalele concepte de management al riscului de securitate cibernetică relevante pentru această teză, şi anume unii dintre termenii-cheie legaţi de securitatea cibernetică, procesul de management al riscului de securitate cibernetică, şi şase domenii de securitate cibernetică importante pentru strategia de management al riscului de securitate cibernetică. Mai mult, subcapitolul oferă o imagine de ansamblu asupra standardelor de management al riscului privind securitatea cibernetică, care s-a axat pe două categorii de standarde, şi anume standarde de tip „cybersecurity risk management" (standarde de management al riscului de securitate cibernetică) şi „generic risk management" (standarde de management al riscului generic), care pot fi valorificate de orice organizaţie indiferent de tipul acesteia, dimensiunea acesteia, sau sectorul de activitate al acesteia. Astfel, cu privire la standardele de tip „cybersecurity risk management", opt standarde au fost descrise care oferă cerinţe privind sistemul de management al securității informațiilor (ISMS), orientări pentru ISMS, orientări pentru managementul riscului de securitate informatică, orientări pentru securitate cibernetică, sau cerinţe pentru managementul riscului de securitate cibernetică. În privinţa standardelor de tip „generic risk management", trei standarde au fost prezentate care oferă fie principii şi orientări pentru managementul riscurilor, fie orientări pentru evaluarea riscurilor. În plus, Figura 1.1 arată standardele selectate pentru cele două categorii de standarde.

Figura 1.1. Standardele selectate privind managementul riscului de securitate cibernetică

În continuare, subcapitolul oferă o imagine de ansamblu asupra metodologiilor de management al riscului privind securitatea cibernetică, care include câteva metodologii notabile care prezintă caracteristici ce corespund uneia din următoarele trei categorii de metodologii pentru managementul riscului de securitate cibernetică: metodologii de tip „cybersecurity risk assessment" (metodologii de evaluare a riscului de securitate cibernetică), „cybersecurity risk management" (metodologii de management al riscului de securitate cibernetică), sau „cybersecurity maturity assessment" (metodologii de evaluare a maturităţii securităţii cibernetice). Prin urmare, au fost descrise patru metodologii pentru categoria „cybersecurity risk assessment", o metodologie pentru categoria „cybersecurity risk management", şi o metodologie pentru categoria „cybersecurity maturity assessment". În plus, Figura 1.2 arată metodologiile selectate pentru cele trei categorii de metodologii.

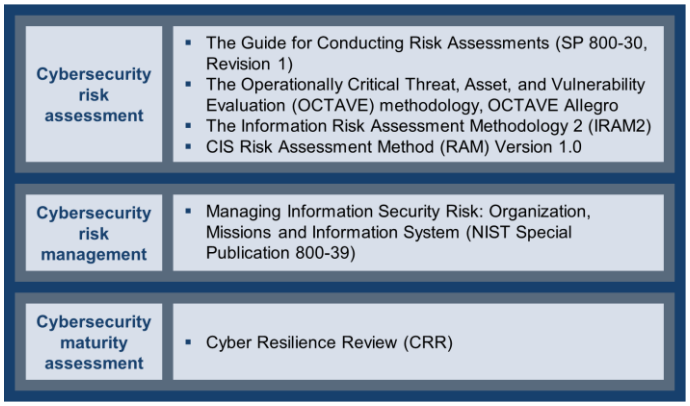

Figura 1.2. Metodologiile selectate privind managementul riscului de securitate cibernetică

Pe urmă, referitor la fundalul privind internetul obiectelor, subcapitolul schiţează diversele domenii de aplicare ale internetului obiectelor (de exemplu, pentru asistenţă medicală, pentru protecţia mediului, pentru aplicaţii comerciale, în scopuri industriale, pentru aplicaţii în oraşele inteligente, şi pentru aplicaţii în domeniul infrastructurii), diferite proiecţii pentru adoptarea de sisteme IoT evidenţiind consensul asupra creşterii internetului obiectelor, şi introduce unele dintre conceptele-cheie pentru IoT incluzând componentele modelului de referinţă pentru IoT de la ITU-T [ITU12].

În continuare, **Capitolul 1.2** oferă motivaţia pentru această teză de doctorat, făcându-se trimitere la primele trei provocări cu care se confruntă organizaţiile, şi anume riscurile în creştere de securitate cibernetică, dificultatea adoptării de noi tehnologii, şi practicile deficitare de management al riscului [ATK18]. Subcapitolul indică faptul că aceste provocări sunt legate de prevalenţa strategiilor reactive de securitate cibernetică [Nat17], de dificultatea adoptării de IoT în mod securizat, şi de absenţa răspândită de strategii robuste de management al riscului securităţii cibernetice pentru internetul obiectelor în organizaţii. În acest context, Figura 1.3 exemplifică modul în care se integrează temele privind securitatea cibernetică, managementul riscului de securitate cibernetică, securitatea cibernetică pentru internetul obiectelor, şi managementul riscului securităţii cibernetice pentru internetul obiectelor, şi evidenţiază temele de interes ale acestei teze de doctorat, şi anume managementul riscului de securitate cibernetică şi managementul riscului securităţii cibernetice pentru internetul obiectelor.

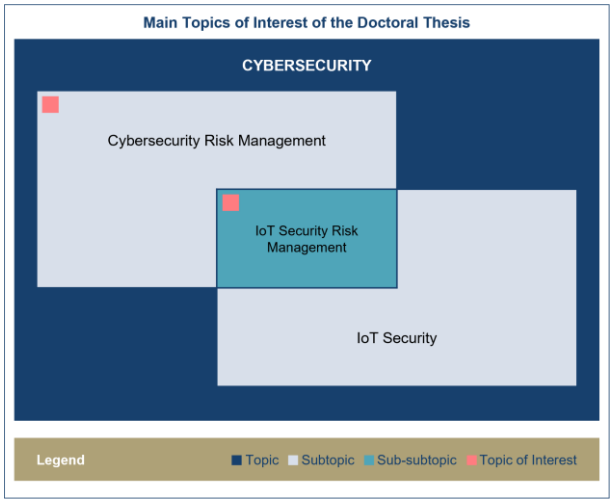

Fig. 1.3. Temele de interes ale tezei de doctorat

În continuare, subcapitolul oferă raţiunea care a stat la baza axării asupra forţelor motrice şi asupra facilitatorilor cheie pentru managementul riscului de securitate cibernetică, evidenţiind legătura dintre forţele motrice cheie şi importanţa analizei strategice pentru formularea unei strategii eficace, şi legătura dintre facilitatorii cheie şi importanţa utilizării de instrumente de planificare în vederea obţinerii unor strategii care se pot pune în aplicare. Ulterior, subcapitolul oferă raţiunea care a stat la baza axării tezei de doctorat asupra celor patru zone de interes (şi anume peisajul ameninţărilor cibernetice, cadrul de reglementare privind securitatea cibernetică, cadrele privind

managementul riscului de securitate cibernetică, şi bunele practici de securitate cibernetică pentru internetul obiectelor), împreună cu obiectivele tezei.

În continuare, **Capitolul 1.3** oferă obiectivele urmărite în cadrul tezei mele, care sunt enumerate mai jos:

- **Obiectivul 1:** Oferirea unei imagini de ansamblu a peisajului actual de ameninţări cibernetice al organizaţiilor;
- **Obiectivul 2:** Oferirea unei prezentări generale a cadrului de reglementare privind securitatea cibernetică, care să se axeze asupra legilor şi reglementărilor cheie privind securitatea cibernetică din jurisdicţiile cheie pentru securitatea cibernetică;
- **Obiectivul 3:** Oferirea unei prezentări generale a mai multor cadre renumite de management al riscului de securitate cibernetică;
- **Obiectivul 4:** Oferirea unei prezentări generale a bunelor practici de securitate cibernetică pentru internetul obiectelor şi clasificarea acestora cu ajutorul unei taxonomii ierarhice propuse;
- **Obiectivul 5:** Propunerea unei metode de „rating" (clasificare) a ameninţărilor cibernetice care urmăreşte atenuarea complexităţii şi incertitudinii asociate cu metodele existente de „rating" a ameninţărilor cibernetice şi prioritizarea ameninţărilor cibernetice actuale cu ajutorul metodei propuse;
- **Obiectivul 6:** Propunerea unei metode de evaluare a legilor şi reglementărilor cheie privind securitatea cibernetică în vederea stabilirii punctelor comune între acestea din perspectiva înţelegerii organizaţionale în ceea ce priveşte gestionarea riscului de securitate cibernetică, şi oferirea unei evaluări critice a legilor şi reglementărilor din sfera de aplicare a evaluării pe baza metodei propuse;
- **Obiectivul 7:** Propunerea unei metodologii pentru evaluarea cadrelor de management al riscului de securitate cibernetică, şi oferirea unei evaluări critice a cadrelor de management al riscului de securitate cibernetică din sfera de aplicare a evaluării pe baza metodologiei propuse;
- **Obiectivul 8:** Propunerea unei metodologii pentru dezvoltarea unui model de referinţă pentru strategia de management al riscului securităţii cibernetice pentru internetul obiectelor, elaborarea modelului de referinţă pentru strategia de management al riscului securităţii cibernetice pentru internetul obiectelor (IoTSRM2), şi evaluarea modelului IoTSRM2 faţă de bunele practici de securitate cibernetică pentru internetul obiectelor care sunt cele mai relevante pentru modelul propus;
- **Obiectivul 9:** Propunerea unei metodologii pentru realizarea unui studiu bazat pe un sondaj în vederea determinării stadiului actual al strategiilor de management al riscului de securitate cibernetică în organizaţiile incluse în sondaj faţă de modelul IoTSRM2 propus, realizarea studiului pe baza metodologiei, şi raportarea concluziilor sondajului pe baza metodologiei propuse.

În final, **Capitolul 1.4** oferă structura acestei teze conform reprezentării din Figura 1.4, care, de asemenea, corelează obiectivele tezei cu capitolele şi/sau subcapitolele tezei acolo unde acestea sunt îndeplinite, şi oferă o „mapă de citire" („reading map") care să ghideze navigarea prin teză către diferite obiective ale tezei. În ceea ce priveşte „mapa de citire", aceasta trebuie să fie coroborată cu cele nouă obiective ale tezei de către cititorii interesaţi de anumite obiective ale tezei, unde:

- **„Mapping 1" (cartografierea 1)** corespunde rezultatelor cercetării mele legate de peisajul ameninţărilor cibernetice, care s-au concretizat în realizarea Obiectivului 1 şi Obiectivului 5;
- **„Mapping 2" (cartografierea 2)** corespunde rezultatelor cercetării mele legate de cadrul de reglementare privind securitate cibernetică, care s-au concretizat în realizarea Obiectivului 2 şi Obiectivului 6;
- **„Mapping 3" (cartografierea 3)** corespunde rezultatelor cercetării mele legate de cadrele de management al riscului de securitate cibernetică, care s-au concretizat în realizarea Obiectivului 3 şi Obiectivului 7;
- **„Mapping 4" (cartografierea 4)** corespunde rezultatelor cercetării mele legate de bunele practici privind securitatea cibernetică pentru internetul obiectelor, care s-au concretizat în realizarea Obiectivului 4, Obiectivului 8 şi Obiectivului 9.

De exemplu, presupunând că un cititor este interesat de Obiectivul 9, Figura 1.4 ghidează cititorul prin „Mapping 4" în vederea citirii Capitolelor 1, 2.4, 5, 6, şi 7.

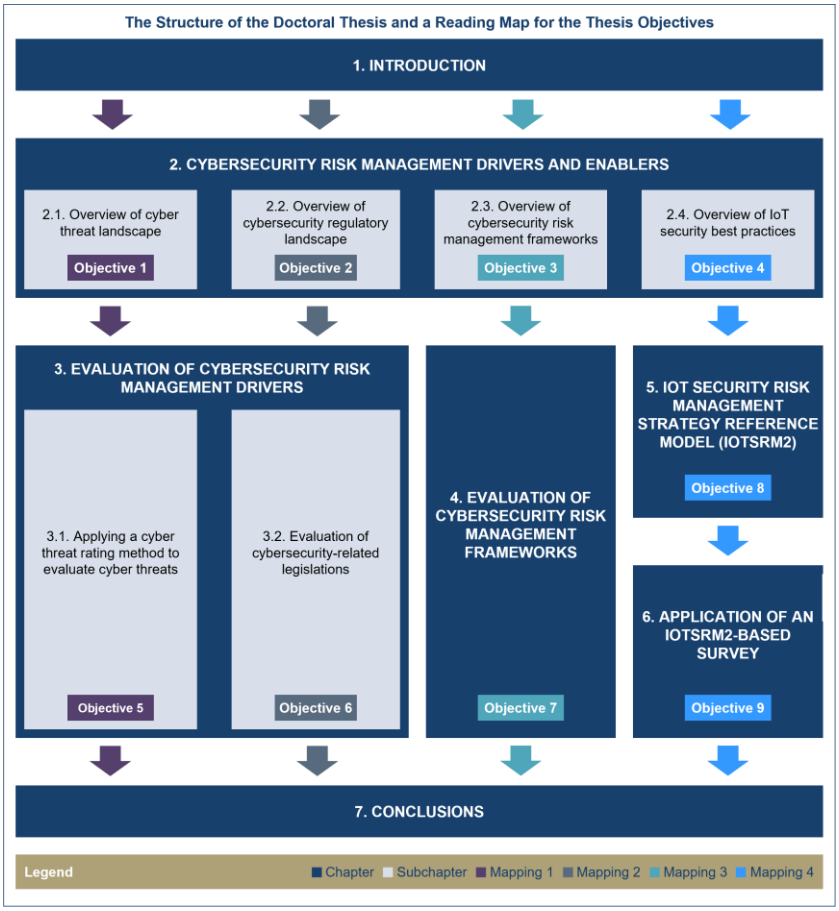

Figure 1.4. Structura tezei şi o „mapă de citire” pentru obiectivele tezei

Capitolul 2. Forţe Motrice şi Facilitatori pentru Managementul Riscului Securităţii Cibernetice

Capitolul 2 prezintă o imagine de ansamblu a forţelor motrice şi a facilitatorilor esenţiali pentru managementul riscului de securitate cibernetică în organizaţii. Cu privire la forţele motrice cheie, capitolul se axează pe creionarea stadiului actual al peisajului ameninţărilor cibernetice şi al cadrului de reglementare al securităţii cibernetice, iar cu privire la facilitatorii cheie, capitolul se axează pe creionarea stadiului actual al cadrelor de management al riscului de securitate cibernetică şi al bunelor practici de securitate cibernetică pentru internetul obiectelor (denumit în continuare „IoT”).

Astfel, **Capitolul 2.1** oferă o prezentare generală a peisajului ameninţărilor cibernetice cu scopul de a facilita evaluarea riscului de securitate cibernetică pentru organizaţii şi de a le permite acestora să ţină pasul cu evoluţia continuă a peisajului ameninţărilor cibernetice. Această vedere de ansamblu a fost obţinută prin consolidarea şi categorisirea celor mai des întâlnite ameninţări cibernetice din 17 surse pertinente şi renumite, incluzând nouă rapoarte privind peisajul ameninţărilor cibernetice, două sondaje privind incidente de securitate cibernetică şi încălcări ale securităţii datelor, un raport al unei autorităţi europene de aplicare a legii privind criminalitatea informatică, un sondaj asupra stadiului securităţii cibernetice la nivel global, două rapoarte care furnizau opinii privind investigaţii legate de incidente de securitate cibernetică, şi un raport privind tendinţele securităţii cibernetice. Ca atare, pe baza examinării acestor 17 surse, 13 categorii de ameninţări cibernetice curente au fost determinate şi descrise, şi anume atacuri prin intermediul unor programe „malware” (programe ostile cu scop distructiv), atacuri de tip „social engineering” (atacuri bazate pe inginerie socială), ameninţări de tip „denial of service” (blocare a accesului), ameninţări de tip „spam” (mesaj electronic nesolicitat), ameninţări de tip „insider” (ameninţări din interior), atacuri de tip „hacking” (piratăj informatic), atacuri asupra vieții private și asupra datelor cu caracter personal, atacuri de tip „cryptojacking” (minarea ilicită de criptomonede), spionaj cibernetic, atacuri ţintite asupra

infrastructurii critice, atacuri în lanțul de aprovizionare, propaganda cibernetică, şi sancțiuni legale şi de reglementare.

De asemenea, studierea literaturii de specialitate a arătat că este nevoie de o metodă de „rating" (clasificare) a ameninţărilor cibernetice în funcţie de gradul de ameninţare al acestora pentru organizaţii, care să fie disociată de elementele (de exemplu, nivelul de competenţă al agentului, motivaţia actorului, oportunitatea ameninţării) care cauzează incertitudine, şi acest lucru a justificat metoda propusă pentru clasificarea categoriilor de ameninţări cibernetice din **Capitolul 3**.

Mai departe, **Capitolul 2.2** oferă o prezentare generală a cadrului legislativ în domeniul securităţii cibernetice care vizează legislaţiile şi normele cele mai esenţiale de securitate cibernetică din jurisdicţiile cele mai relevante pentru securitatea cibernetică, şi urmăreşte să pregătească terenul pentru stabilirea punctelor comune între aceste legi din perspectiva înţelegerii organizaţionale în ceea ce priveşte gestionarea riscului de securitate cibernetică. Aşadar, această prezentare a legislaţiilor de securitate cibernetică s-a concentrat exclusiv asupra jurisdicţiilor (şi anume Uniunea Europeană – UE, Singapore, şi Statele Unite ale Americii – SUA) care au dat dovadă de cele mai ridicate niveluri de angajament în direcţia securităţii cibernetice conform raportului privind indicele global de securitate cibernetică [ITU17], s-a axat pe cele mai relevante domenii (şi anume domeniul privind protecția datelor și a vieții private și domeniul privind protecţia infrastructurilor critice) ale legilor şi reglementărilor de securitate cibernetică în vigoare pentru declanşarea îmbunătăţirii practicilor de management al riscului de securitate cibernetică din organizaţii, şi s-a centrat pe legile şi reglementările de securitate cibernetică care erau general aplicabile şi care se aflau în vigoare la momentul realizării studiului [Giu+21]. De asemenea, această prezentare generală a legilor şi reglementărilor de securitate cibernetică a exclus legile şi reglementările referitoare la servicii sau produse specifice de securitate cibernetică, legile şi reglementările de securitate cibernetică specifice unui anumit sector de activitate, legile şi reglementările privind securitatea cibernetică care nu erau promulgate la momentul realizării studiului, legile şi reglementările de securitate cibernetică legate de alte domenii (de exemplu, de controlul exporturilor, de criminalitatea informatică), legile şi reglementările de securitate cibernetică aplicabile numai anumitor state membre ale UE sau SUA, şi acordurile de cooperare internațională în materie de securitate cibernetică.

Astfel, cu privire la UE, în ceea ce priveşte protecția datelor și a vieții private s-a identificat Regulamentul (UE) 2016/679 privind prelucrarea datelor cu caracter personal și libera circulație a acestor date, iar în ceea ce priveşte protecţia infrastructurilor critice s-a identificat Directiva (UE) 2016/1148 (NIS) privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune. Legat de Singapore, în ceea ce priveşte protecția datelor și a vieții private s-a identificat Legea privind protecția datelor cu caracter personal din 2012 (PDPA), iar în ceea ce priveşte protecţia infrastructurilor critice s-a identificat Legea privind securitatea cibernetică (CA). Legat de SUA, în ceea ce priveşte protecția datelor și a vieții private nu a existat nici o lege sau reglementare general aplicabilă la nivel federal, iar în ceea ce priveşte protecţia infrastructurilor critice s-au identificat Legea privind protecția infrastructurilor critice din 2001, Ordinul executiv 13636 privind îmbunătățirea securității cibernetice a infrastructurilor critice, Directiva privind politica prezidențială în ceea ce priveşte securitatea și reziliența infrastructurilor critice, şi Ordinul executiv 13800 privind consolidarea securității cibernetice a rețelelor federale și a infrastructurii critice. Mai mult, este important de reținut că în ceea ce priveşte domeniul protecţiei infrastructurilor critice, cadrul pentru îmbunătățirea securității cibernetice a infrastructurilor critice (CSF) elaborat de Institutul Național pentru Standarde și Tehnologie („National Institute of Standards and Technology" – NIST) [NIS18a] a fost identificat ca fiind un produs secundar al legislaţiei SUA în materie de protecţie a infrastructurilor critice.

De asemenea, acest studiu a arătat că este nevoie de evaluari critice ale legislaţiilor şi reglementărilor de securitate cibernetică în vederea stabilirii punctelor comune între acestea, iar acest aspect a motivat evaluarea critică a legilor de securitate cibernetică expusă în **Capitolul 3**.

Capitolul 2.3 oferă o prezentare generală a mai multor cadre renumite de management al riscului de securitate cibernetică, prin definirea termenului „cybersecurity risk management framework" (cadrul privind managementul riscului de securitate cibernetică) şi prin descrierea câtorva dintre cadrele pentru managementul riscului de securitate cibernetică adoptate cel mai des. În acest context, aceste cadre au fost selectate pentru a putea fi valorificate de orice organizaţie indiferent de tipul acesteia, dimensiunea acesteia, sectorul de activitate al acesteia, sau domeniul de interes al acesteia privind securitatea cibernetică, şi grupate în trei categorii relevante pentru managementul riscului de securitate cibernetică, si anume cadre de tip „cybersecurity-related" (cadre legate de securitatea cibernetică), „generic risk management" (cadre pentru managementul riscului generic), şi „IT-related" (cadre legate de tehnologia informaţiei). În privinţa cadrelor de tip „cybersecurity-related", au fost descrise zece cadre care sunt aplicabile fie activităţilor de evaluare al riscului, fie activităţilor de management al riscului, şi sunt sprijinite de o abordare bazată pe riscuri sau pe reguli. În ceea ce priveşte cadrele de tip „generic risk management", au fost descrise trei cadre care oferă obiective de controale generice, controale interne, principii, sau orientări privind

managementul riscului. Legat de cadrele de tip „IT-related”, au fost descrise patru cadre care corespund următoarelor domenii de interes: gestionarea serviciului informatic, guvernanța și gestionarea sistemelor informatice pentru întreprinderi, managementul riscurilor tehnologiei informației pentru întreprinderi, sau managementul capacităţii informatice. În plus, Figura 2.1 ilustrează cadrele selectate pentru cele trei categorii de cadre relevante pentru managementul riscului de securitate cibernetică.

Figura 2.1. Cadrele selectate privind managementul riscului de securitate cibernetică

De asemenea, acest studiu a indicat că este nevoie de evaluări critice ale cadrelor de management al riscului de securitate cibernetică în relaţie cu fiecare dintre cele considerate, în vederea sprijinirii procesului decizional atunci când vine vorba de selectarea unui cadru, iar acest aspect a motivat evaluarea critică a cadrelor de management al riscului de securitate cibernetică furnizată în **Capitolul 4**.

Ulterior, **Capitolul 2.4** propune o nouă taxonomie ierarhică pentru clasificarea bunelor practici de securitate pentru IoT în funcţie de grupul publicului vizat, şi anume public-ţintă de tip „adopter specific” (care vizează în principal organizaţiile care adoptă IoT), „general” (care vizează utilizatorii, producătorii, şi/sau furnizorii de IoT), „manufacturer specific” (care vizează în principal producătorii de IoT), şi „supplier specific” (care vizează în principal furnizorii de IoT), şi în funcţie de tipul de bune practici, şi anume bune practici de tip „codes of practice” (coduri de bune practici), „standards” (standarde), „guidelines” (orientări), şi „frameworks” (cadre). În plus, acest subcapitol oferă o imagine cuprinzătoare a 25 de bune practici selectate privind securitatea pentru IoT care sunt clasificate cu ajutorul taxonomiei ierarhice propuse. În plus, Figura 2.4 prezintă taxonomia ierarhică propusă pentru clasificarea bunelor practici privind securitatea cibernetică pentru IoT.

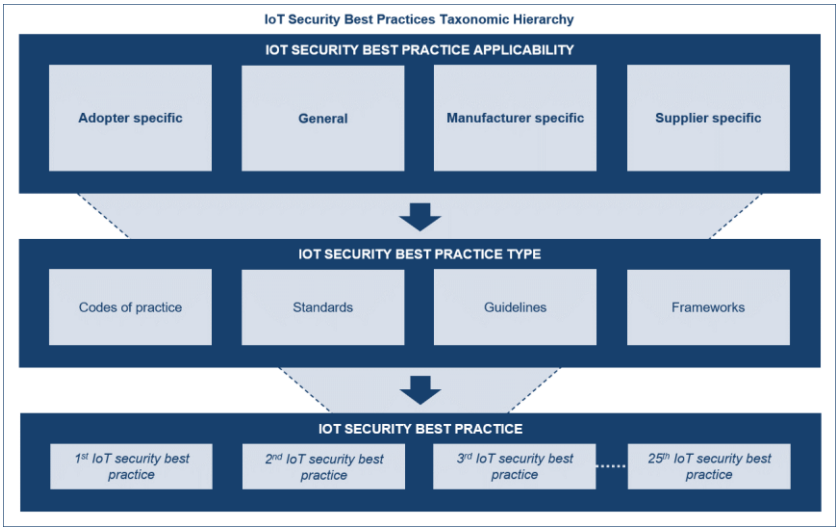

Figura 2.2. Taxonomia ierarhică propusă pentru bunele practici de securitate privind IoT [Pop+21a]

Astfel, identificarea bunelor practici de securitate pentru IoT din sfera de aplicare a prezentului studiu a fost bazată pe studierea literaturii de specialitate şi nu a luat în considerare bunele practici de securitate pentru IoT care se concentrează exclusiv pe aspecte tehnice, bunele practici de securitate pentru IoT care sunt destinate certificării, versiuni provizorii sau expirate ale bunelor practici de securitate pentru IoT, bunele practici de securitate cibernetică care nu sunt specifice pentru IoT, şi rapoarte ale furnizorilor care abordează bunele practici de securitate pentru IoT.

În consecinţă, cu privire la bunele practici de securitate pentru IoT de tip „adopter specific”, acest subcapitol a expus o bună practică de tip „frameworks” şi trei bune practici de tip „guidelines”, fiecare dintre aceste trei orientări concentrându-se pe controale generice de securitate pentru IoT, recomandări pentru IoT privind managementul identității și accesului, sau bune practici de securitate pentru IoT specifice asistenței medicale. În plus, Figura 2.5 arată bunele practici selectate de securitate pentru IoT de tip „adopter specific”.

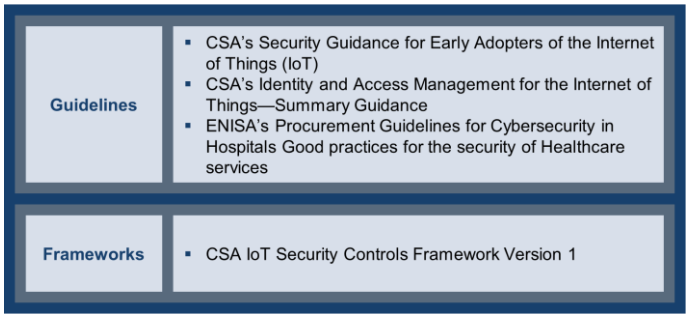

Figura 2.3. Bunele practici selectate de securitate pentru IoT de tip „adopter specific”. Adaptare după [Pop+21a]

În privinţa bunelor practici de securitate pentru IoT de tip „general”, subcapitolul a prezentat două bune practici de tip „codes of practice”, care se axează pe ciclul de viaţă pentru dezvoltarea robustă a sistemelor IoT, două bune practici de tip „guidelines” care ţintesc organizaţii din anumite sectoare de activitate, o bună practică de tip „guidelines” privind ciclul de viaţă pentru dezvoltarea robustă a sistemelor IoT, o bună practică de tip „guidelines” pentru securizarea lanţului de aprovizionare cu IoT, şi trei bune practici de tip „frameworks”, care abordează principii strategice sau cerinţe de fiabilitate. În plus, Figura 2.6 arată bunele practici selectate de securitate pentru IoT de tip „general”.

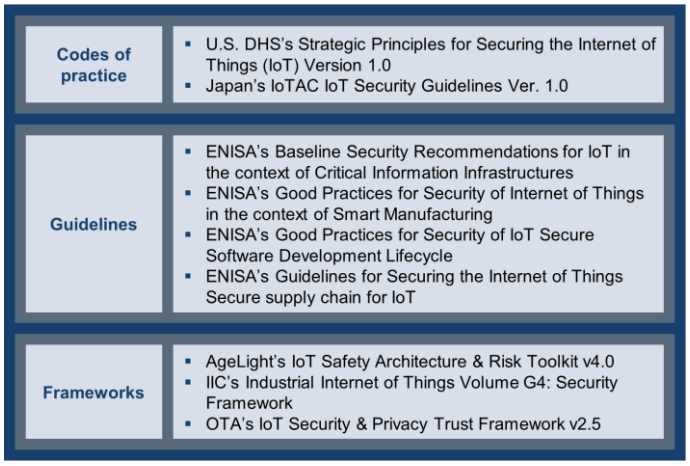

Figura 2.4. Bunele practici selectate de securitate pentru IoT de tip „general". Adaptare după [Pop+21a]

În ceea ce privește bunele practici de securitate pentru IoT de tip „manufacturer specific", subcapitolul a descris două bune practici de securitate pentru IoT de tip „standards" şi patru bune practici de securitate pentru IoT de tip „guidelines", fiecare dintre aceste patru orientări oferind recomandări de securitate, cerințe de bază privind capacităţile, sau principii pentru dispozitivele IoT. În plus, Figura 2.7 arată bunele practici selectate de securitate pentru IoT de tip „manufacturer specific".

Figura 2.5. Bunele practici selectate de securitate pentru IoT de tip „manufacturer specific". Adaptare după [Pop+21a]

Legat de bunele practici de securitate pentru IoT de tip „supplier specific", subcapitolul a descris două bune practici de tip „codes of practice", care furnizează măsuri de securitate pentru IoT, două bune practici de securitate pentru IoT de tip „guidelines", şi două bune practici de securitate pentru IoT de tip „frameworks". În plus, Figura 2.8 arată bunele practici selectate de securitate pentru IoT de tip „supplier specific"

Figura 2.6. Bunele practici selectate de securitate pentru IoT de tip „supplier specific". Adaptare după [Pop+21a]

De asemenea, studiul a revelat necesitatea unui model de referinţă pentru strategia de management al riscului securităţii cibernetice pentru IoT, iar acest aspect a motivat dezvoltarea modelului de referinţă propus pentru strategia de management al riscului de securitate privind IoT, care este furnizat în **Capitolul 5**.

Capitolul 3. Evaluarea Forţelor Motrice pentru Managementul Riscului Securităţii Cibernetice

Capitolul 3 extinde munca de cercetare redată în **Capitolul 2** privind forţele motrice pentru managementul riscului de securitate cibernetică, şi anume peisajul ameninţărilor cibernetice şi cadrul de reglementare al securităţii cibernetice. Astfel, cu privire la munca de cercetare privind peisajul ameninţărilor cibernetice, prin abordarea nevoii pentru o metodă de „rating" (clasificare) a ameninţărilor de securitate cibernetică bazată pe elemente măsurabile, acest capitol vizează sprijinirea prioritizării ameninţărilor cibernetice în funcţie de potenţialul lor de a cauza „cyber harm" (prejudiciu cibernetic) organizaţiilor şi părţilor interesate ale acestora, şi să faciliteze formarea unei reprezentări mai holistice a unora dintre cele mai curente ameninţări cibernetice. În privinţa muncii de cercetare legate de cadrul de reglementare al securităţii cibernetice, prin abordarea necesităţii realizării de evaluări ale legislaţiilor şi reglementărilor privind securitatea cibernetică în vederea stabilirii punctelor comune între acestea, acest capitol urmăreşte atenuarea gradului de complexitate asociat atingerii conformităţii la nivel organizaţional cu legislaţiile şi reglementările în materie de securitate cibernetică.

În acest context, **Capitolul 3.1** oferă o nouă metodă de „rating" a categoriilor de ameninţări cibernetice care permite analiza categoriilor de ameninţări cibernetice din sfera de aplicare a acestei metode de „rating", estimarea gradelor de aplicabilitate ale acestora la „cyber harm" pe baza taxonomiei dezvoltate de Agrafiotis et al. (2018) [Agr+18] pentru „cyber harm" la nivel organizaţional, şi prioritizarea categoriilor de ameninţări cibernetice din sfera de aplicare a acestei metode. Taxonomia pentru „cyber harm" este alcatuită din „cyber harm" de tip „Physical/Digital" (fizic sau digital) având 15 subtipuri de „cyber harm", „cyber harm" de tip „Economic" (economic) având 16 subtipuri de „cyber harm", „cyber harm" de tip „Psychological" (psihologic) având 12 subtipuri de „cyber harm", „cyber harm" de tip „Reputational" (reputaţional) având zece subtipuri de „cyber harm", şi „cyber harm" de tip „Social/Societal" (social şi societal) având patru subtipuri de „cyber harm".

În plus, această taxonomie este reprezentată cu ajutorul a şase ecuaţii, o ecuaţie reprezentând tipurile de „cyber harm", iar celelalte cinci ecuaţii reprezentând subtipurile fiecarui tip de „cyber harm". De exemplu, Ecuaţia (3.1) este utilizată pentru reprezentarea subtipurilor (i.e., y_{1j}) de „cyber harm" de tip „Physical/Digital" (i.e., y_1):

$$y_{1j} = \left\{ \begin{array}{c} \text{Damaged or unavailable, Destroyed, Theft,} \\ \text{Compromised, Infected, Exposed / leaked,} \\ \text{Corrupted, Reduced performance,} \\ \text{Bodily injury, Pain, Loss of life,} \\ \text{Prosecution, Abuse, Mistreatment,} \\ \text{Identity theft} \end{array} \right\}, \text{ where } j = [1..15] \quad (3.1)$$

Mai mult, această metodă de „rating" a ameninţărilor cibernetice a introdus o serie de ecuaţii care permit calculul asociat cu deteminarea măsurii în care o anumită categorie de ameninţări cibernetice poate fi aplicabilă la un anumit tip de „cyber harm" şi la nivelul tuturor tipurilor de „cyber harm". Aşadar, metoda de „rating" propusă pentru clasificarea categoriilor de ameninţări cibernetice implică evaluarea fiecărei categorii de ameninţări cibernetice din mulţimea de categorii de ameninţări cibernetice din sfera de aplicare a acestei metode de „rating" (şi anume x_k) faţă de toate subtipurile (şi anume y_{ij}) ale fiecărui tip de „cyber harm" (şi anume y_i) utilizând Ecuaţia (3.2), în care $\text{Rating}_{x_k}\left(y_{ij}\right)$ reprezintă clasificarea în cauză, C reprezintă cardinalitatea mulţimii de categorii de ameninţări cibernetice din sfera de aplicare a acestei metode de „rating" (şi anume x_k), şi n_i reprezintă numărul de subtipuri al fiecărui tip de „cyber harm":

$$\text{Rating}_{x_k}\left(y_{ij}\right) = \left\{ \begin{array}{c} 1, \text{ if the sub-type is applicable for } x_k \\ 0, \text{ otherwise} \end{array} \right., \quad (3.2)$$

where k=[1..C], C=$|x_k|$, i = [1..5], j = [1..n_i]

Mai departe, pentru fiecare categorie de ameninţări cibernetice din mulţimea de categorii de ameninţări cibernetice din sfera de aplicare a metodei de „rating”, folosind Ecuaţia (3.3), clasificările corespunzătoare subtipurilor fiecărui tip de „cyber harm” sunt însumate pentru determinarea gradului la care categoria de ameninţări cibernetice în cauză poate fi aplicabilă pentru un anumit tip de „cyber harm”:

$$\text{Threat rating } (x_k) = \sum_{j=1}^{n_i} \text{Rating}_{x_k}\left(y_{ij}\right), \text{ where } k=[1..C],\ C=|x_k|,\ i = [1..5] \qquad (3.3)$$

Ulterior, rezultatele obţinute sunt ponderate cu $1/n_i$, unde n_i este numărul de subtipuri al fiecărui tip de „cyber harm”. Aceste rezultate ponderate permit comparaţiile între gradele posibile la care o anumită categorie de ameninţări cibernetice din mulţimea de categorii de ameninţări cibernetice din sfera de aplicare a metodei de „rating” este aplicabilă la diferite tipuri de „cyber harm” şi între toate categoriile de ameninţări cibernetice din sfera de aplicare a metodei de „rating” în relaţie cu gradele posibile la care acestea sunt aplicabile la un anumit tip de „cyber harm”. În sfârşit, pentru fiecare categorie de ameninţări cibernetice din mulţimea de categorii de ameninţări cibernetice din sfera de aplicare a metodei de „rating”, rezultatele obţinute pentru tipurile de „cyber harm” sunt însumate pentru a indica măsura în care categoria de ameninţări cibernetice în cauză este aplicabilă la nivelul tuturor tipurilor de „cyber harm”. Pentru fiecare categorie de ameninţări cibernetice din mulţimea de categorii de ameninţări cibernetice din sfera de aplicare a metodei de „rating”, rezultatele obţinute sunt ponderate cu 1/5, unde 5 este numărul de tipuri de „cyber harm”. Aceste scoruri generale oferă un mijloc de comparare a categoriilor de ameninţări cibernetice din sfera de aplicare a metodei de „rating” în funcţie de gradele posibile de aplicabilitate la un anumit tip de „cyber harm” luând în considerare taxonomia selectată pentru „cyber harm”. În plus, toate scorurile ponderate sunt exprimate în procente şi convertite în clasificări calitative utilizând o scară de intensitate cu cinci puncte, şi anume „Very Low” (foarte scăzut) pentru scoruri cuprinse între 0% şi 20%, „Low” (scăzut) pentru scoruri cuprinse între 21% şi 40%, „Medium” (moderat) pentru scoruri cuprinse între 41% şi 60%, „High” (ridicat) pentru scoruri cuprinse între 61% şi 80%, şi „Very High” (foarte ridicat) pentru scoruri cuprinse între 81% şi 100%.

În continuare, această metodă de „rating” a ameninţărilor cibernetice a fost aplicată pe cele 13 categorii de ameninţări cibernetice curente din **Capitolul 2** cu ajutorul unui instrument de „rating” al ameninţărilor bazat pe Excel, care fost creat pentru a facilita determinarea clasificărilor ameninţărilor şi evaluarea ulterioară a categoriilor de ameninţări cibernetice din sfera de aplicare a metodei de „rating”.

În plus, capitolul oferă o evaluare critică a celor 13 categorii de ameninţări cibernetice în funcţie de clasificările acestora care au rezultat din aplicarea metodei de „rating” a ameninţărilor cibernetice care a permis prioritizarea acestor categorii de ameninţări cibernetice. Astfel, Figura 3.1 prezintă rezultatele instrumentului de „rating” al ameninţărilor pentru fiecare categorie de ameninţări cibernetice din sfera de aplicare a metodei de „rating” în ceea ce priveşte tipurile de „cyber harm”.

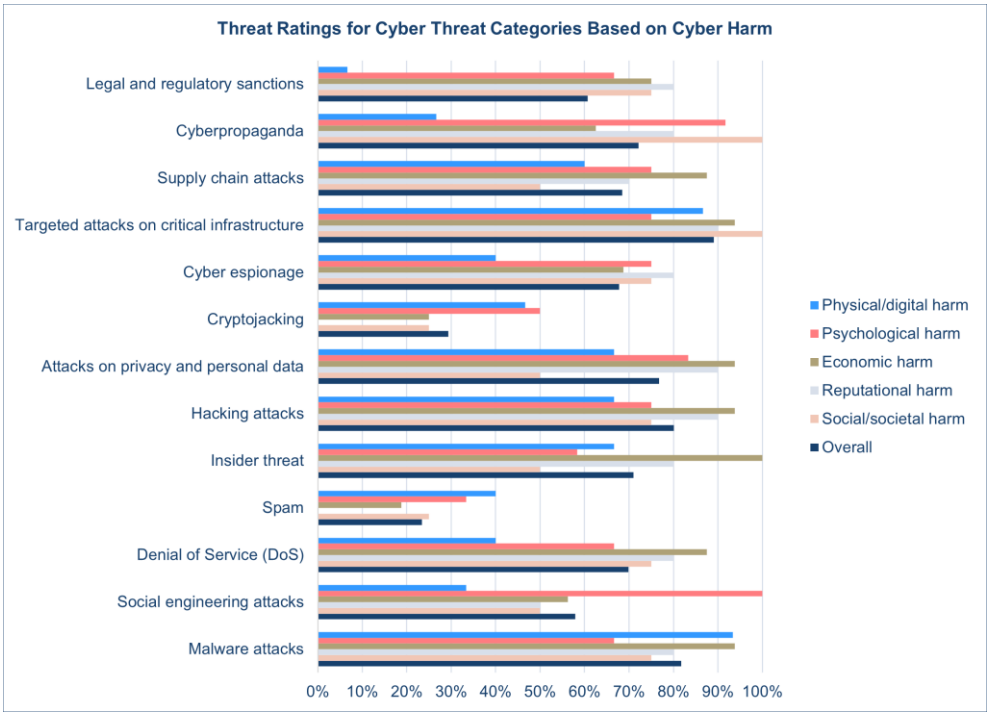

Figura 3.1. Clasificările ameninţărilor în funcţie de „cyber harm" pentru categoriile de ameninţări cibernetice din sfera de aplicare a metodei de „rating" [Pop+19b]

Această evaluare a arătat că trei categorii de ameninţări cibernetice prezintă un grad „Very High" de aplicabilitate la „cyber harm", şapte categorii de ameninţări cibernetice prezintă un grad „High" de aplicabilitate la „cyber harm", o categorie de ameninţări cibernetice prezintă un grad „Medium" de aplicabilitate la „cyber harm", şi două categorii de ameninţări cibernetice prezintă un grad „Low" de aplicabilitate la „cyber harm". Cu privire la gradul „Very High" de aplicabilitate la „cyber harm", categoriile de ameninţări „Targeted attacks on critical infrastructure" (atacuri ţintite asupra infrastructurii critice), „Malware attacks" (atacuri prin intermediul unor programe ostile), şi „Hacking attacks" (atacuri de tip piratăj informatic) au avut drept rezultat scoruri care corespund gradului de clasificare „Very High". Astfel, aceste categorii de ameninţări cibernetice ar trebui să fie în capul listei când vine vorba despre ameninţări cibernetice. În ceea ce priveşte gradul „High" de aplicabilitate la „cyber harm", categoriile de ameninţări „Attacks on privacy and personal data" (atacuri asupra vieţii private şi asupra datelor cu caracter personal), „Cyberpropaganda" (propaganda cibernetică), „Insider threat" (ameninţări din interior), „Denial of Service (DoS)" (ameninţări de tip blocare a accesului), „Supply chain attacks" (atacuri în lanţul de aprovizionare), „Cyber espionage" (spionaj cibernetic), şi „Legal and regulatory sanctions" (sancţiuni legale şi de reglementare) au avut drept rezultat scoruri care corespund gradului de clasificare „High". Astfel, deşi aceste categorii de ameninţări cibernetice nu sunt în capul listei când vine vorba despre ameninţări cibernetice, ele ar trebui să fie de interes focal pentru organizaţiile care vizează să trateze ameninţările cibernetice. Legat de gradul „Medium" de aplicabilitate la „cyber harm", categoria de ameninţări "Social engineering attacks" (atacuri bazate pe inginerie socială) a avut drept rezultat un scor care corespunde gradului de clasificare „Medium". Aşadar, deşi această categorie de ameninţări cibernetice pare mai puţin periculoasă decât cele care prezintă grade de aplicabilitate la „cyber harm" mai ridicate, aceasta ar trebui tratată cu seriozitate în continuare de organizaţii având în vedere faptul că aceasta ar putea fi un vector de atac pentru alte ameninţări cibernetice. În ceea ce priveşte gradul „Low" de aplicabilitate la „cyber harm", categoriile de ameninţări „Cryptojacking" (minarea ilicită de criptomonede) şi „Spam" (ameninţări de tip mesaj electronic nesolicitat) au avut drept rezultat scoruri care corespund gradului de clasificare „Low". Astfel, deşi aceste categorii de ameninţări cibernetice sunt cele mai puţin aplicabile la „cyber harm" între cele 13 categorii de ameninţări cibernetice, acestea nu trebuie trecute cu vederea de organizaţii când vine vorba despre ameninţări cibernetice întrucât aceste două categorii de ameninţări cibernetice nu sunt neglijabile.

În plus, Figura 3.2 arată o altă imagine consolidată a clasificărilor globale pentru cele 13 categorii de ameninţări cibernetice.

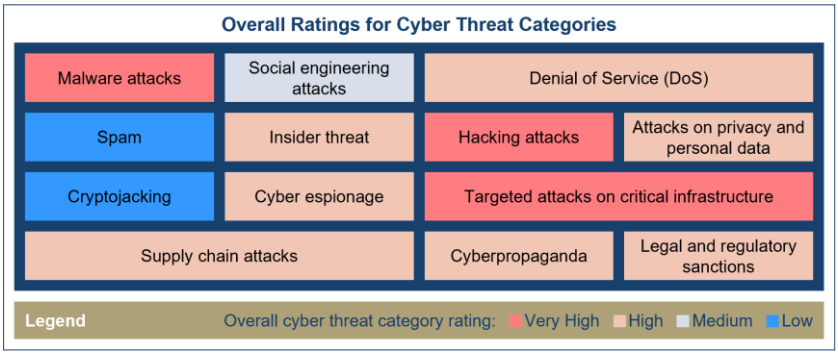

Figura 3.2. Clasificările globale pentru cele 13 categorii de ameninţări cibernetice în funcţie de potenţialul „cyber harm”

În continuare, capitolul oferă concluziile rezultate din revizuirea lucrărilor conexe. Astfel, una dintre principalele concluzii a fost aceea că metoda propusă pentru clasificarea categoriilor de ameninţări cibernetice valorifică cea mai recentă taxonomie pentru „cyber harm” în moduri noi care nu au fost anterior explorate.

În continuare, **Capitolul 3.2** prezintă o metodă propusă pentru evaluarea unor legislaţii şi reglementări selectate privind securitatea cibernetică din perspectiva înţelegerii organizaţionale în ceea ce priveşte gestionarea riscului de securitate cibernetică, care este bazată pe prezentarea generală a legislaţiilor şi reglementărilor cheie privind securitatea cibernetică din jurisdicţiile cheie pentru securitate cibernetică de la **Capitolul 2.2** şi pe „Identify Function” (funcţia de identificare) a cadrului pentru îmbunătățirea securității cibernetice a infrastructurilor critice (denumit în continuare „NIST CSF”) elaborat de Institutul Național pentru Standarde și Tehnologie („National Institute of Standards and Technology” – NIST) [NIS18a]. Astfel, această metodă de evaluare s-a axat pe domeniile (şi anume domeniul privind protecția datelor și a vieții private şi domeniul privind protecţia infrastructurilor critice) legilor şi reglementărilor de securitate cibernetică în vigoare relevante pentru declanşarea îmbunătăţirii practicilor de management al riscului de securitate cibernetică din organizaţii, şi s-a concentrat asupra jurisdicţiilor care au demonstrat la scară mondială cele mai ridicate niveluri de angajament în direcţia securităţii cibernetice, şi anume Uniunea Europeană – UE, Singapore, şi Statele Unite ale Americii – SUA.

În primul rând, metoda de evaluare propusă a dat motivaţia pentru bazarea evaluării critice pe „Identify Function” a cadrului NIST CSF [NIS18a]. În al doilea rând, metoda propusă a introdus categoriile subiacente funcţiei de indentificare a cadrului NIST CSF, şi anume „Asset Management” (gestionarea activelor), „Business Environment” (mediul de afaceri), „Governance” (guvernanţa), „Risk Assessment” (evaluarea riscurilor), „Risk Management Strategy” (strategia de gestionare a riscurilor), şi „Supply Chain Risk Management” (gestionarea riscurilor aferente lanţului de aprovizionare), care au fost utilizate pentru compararea legilor din sfera de aplicare a metodei de evaluare a legislaţiilor. În al treilea rând, legile şi reglementările de securitate cibernetică prezentate în **Capitolul 2.2** şi absenţa unei legi general aplicabile în SUA la nivel federal privind protecția datelor și a vieții private au fost reiterate. Ulterior, metoda de evaluare propusă a oferit motivaţia pentru axarea exclusivă pe cadrul NIST CSF decât pe legislaţia americană specifică privind protecţia infrastructurilor critice, şi anume cu scopul de a reduce redundanţa având în vedere că acest cadru este un produs secundar al legislaţiei americane privind protecţia infrastructurilor critice.

În continuare, metoda de evaluare propusă a oferit legile şi reglementările privind securitatea cibernetică din sfera de aplicare a acestei metode de evaluare în vederea evaluării critice a acestora (şi anume „General Data Protection Regulation” – GDPR, „Personal Data Protection Act 2012” – PDPA, „Directive on Security of Network and Information Systems” – NISD, şi „Cybersecurity Act” – CA). De asemenea, metoda de evaluare propusă a oferit definiţiile valorilor lingvistice de „rating” utilizate pentru reprezentarea rezultatelor evaluării, şi anume „True” (adevărat), „Fairly True” (aproape adevărat), „Partly True” (parţial adevărat), „Nearly False” (aproape fals), „False” (fals). În primul rând, valoarea „True” a fost utilizată pentru a indica faptul că statutul cuprinde cerinţe care corespund pe deplin categoriei NIST CSF fără discrepanţe evidente. În al doilea rând, valoarea „Fairly True” a fost utilizată pentru a indica faptul că statutul cuprinde cerinţe care aproape corespund categoriei NIST CSF cu discrepanţe minore. În al treilea rând, valoarea „Partly True” a fost utilizată pentru a indica faptul că statutul cuprinde cerinţe care corespund parţial categoriei NIST CSF cu anumite discrepanţe. În al patrulea rând, valoarea „Nearly False” a fost utilizată pentru a indica faptul că statutul cuprinde cerinţe care aproape se abat de la categoria NIST CSF cu anumite similitudini. În final, valoarea „False” a fost utilizată pentru a indica faptul că statutul cuprinde cerinţe care se abat de la categoria NIST CSF cu discrepanţe majore.

Mai departe, capitolul oferă evaluarea critică a legilor şi reglementărilor privind securitatea cibernetică din sfera de aplicare a metodei de evaluare în vederea identificării punctelor comune între acestea şi sprijinirii unei abordări pragmatice în scopul atingerii conformităţii pentru organizaţiile care se străduiesc să evite sancţiunile şi procesele costisitoare ca urmare a încălcării legii. Aşadar, Tabelul 3.1 rezumă concluziile evaluării fiecărei legi sau reglementări selectate privind securitatea cibernetică în relaţie cu categoriile funcţiei de identificare a cadrului NIST CSF (coloana din tabel denumită „NIST CSF Category").

Tabelul 3.1. Rezultatele evaluării legilor şi reglementărilor din sfera de aplicare a metodei de evaluare a legislaţiilor [Pop+19a]

Unique ID.	NIST CSF Category	GDPR	PDPA	NISD	CA
ID.AM	Asset Management	Fairly True	Nearly False	True	True
ID.BE	Business Environment	Partly True	Nearly False	Fairly True	Partly True
ID.GV	Governance	Fairly True	Partly True	True	Partly True
ID.RA	Risk Assessment	Partly True	Nearly False	Fairly True	Fairly True
ID.RM	Risk Management Strategy	Partly True	Nearly False	Fairly True	Nearly False
ID.SC	Supply Chain Risk Management	Fairly True	Nearly False	Fairly True	Nearly False

În consecinţă, cu privire la categoria „Asset Management" a funcţiei de identificare a cadrului NIST CSF, cerinţele din CA şi NISD corespund pe deplin acestei categorii fără discrepanţe evidente şi cerinţele din GDPR aproape corespund acestei categorii cu discrepanţe minore. În ceea ce priveşte categoria „Business Environment" a funcţiei de identificare a cadrului NIST CSF, cerinţele din NISD aproape corespund acestei categorii cu discrepanţe minore. În privinţa categoriei „Governance" a funcţiei de identificare a cadrului NIST CSF, cerinţele din NISD corespund pe deplin acestei categorii fără discrepanţe evidente şi cerinţele din GDPR aproape corespund acestei categorii cu discrepanţe minore. Cu privire la categoria „Risk Assessment" a funcţiei de identificare a cadrului NIST CSF, cerinţele din CA şi NISD aproape corespund acestei categorii cu discrepanţe minore. Legat de categoria „Risk Management Strategy" a funcţiei de identificare a cadrului NIST CSF, cerinţele din NISD aproape corespund acestei categorii cu discrepanţe minore. Cu privire la categoria „Supply Chain Risk Management" a funcţiei de identificare a cadrului NIST CSF, cerinţele din GDPR şi NISD aproape corespund acestei categorii cu discrepanţe minore.

În continuare, capitolul oferă lucrările conexe care au arătat că în momentul realizării studiului nu a fost găsit nici un studiu anterior care să evalueze toate cele patru norme de securitate cibernetică (şi anume GDPR, NISD, PDPA, CA) faţă de funcţia de identificare a cadrului NIST CSF.

Capitolul 4. Evaluarea Cadrelor de Management al Riscului Securităţii Cibernetice

Capitolul 4 extinde munca de cercetare redată în **Capitolul 2** privind cadrele pentru managementul riscului de securitate cibernetică, prin propunerea unei metodologii pentru evaluarea cadrelor de management al riscului de securitate cibernetică, evaluarea critică a cadrelor de management al riscului de securitate cibernetică din sfera de aplicare a metodologiei propuse, şi oferirea unei analize cuprinzătoare a lucrărilor conexe. Astfel, capitolul vizează sprijinirea luării deciziei cu privire la selectarea cadrelor de management al riscului de securitate cibernetică, şi facilitarea implementării pragmatice de programe de securitate cibernetică prin abordarea necesităţii de realizare a mai multor evaluări critice ale cadrelor de management al riscului de securitate cibernetică în raport cu acestea.

Capitolul 4.1 oferă modul în care a fost concepută o metodologie în trei etape, care a fost propusă în vederea evaluării cadrelor de management al riscului de securitate cibernetică din sfera de aplicare a acestei metodologii (a se vedea Figura 4.1).

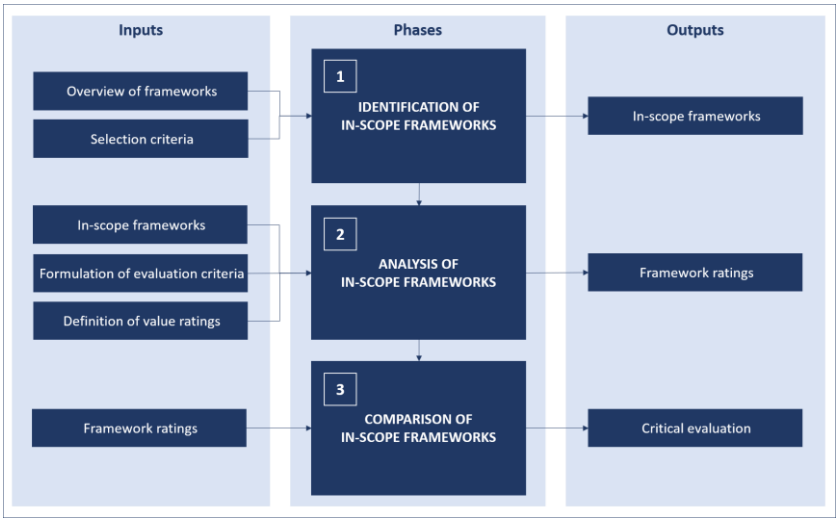

Figura 4.1. Metodologia propusă pentru evaluarea cadrelor [Pop20]

Cu privire la prima etapă a metodologiei, şi anume etapa „identification of in-scope frameworks" (identificarea cadrelor din sfera de aplicare a acestei metodologii), aceasta se foloseşte de prezentarea generală a cadrelor de management al riscului de securitate cibernetică de la **Capitolul 2.3.1** şi de criteriile de selecţie de a alege doar cadrele acordate cu titlu gratuit care au documentaţia uşor accesibilă, în vederea determinării cadrelor din sfera de aplicare a acestei metodologii. Astfel, pentru identificarea cadrelor din sfera de aplicare a acestei metodologii, criteriile de selecţie sunt aplicate la cadrele de management al riscului de securitate cibernetică descrise în cadrul prezentării generale de la **Capitolul 2.3.1**.

Cu privire la a doua etapă a metodologiei, şi anume etapa „analysis of in-scope frameworks" (analiza cadrelor din sfera de aplicare a acestei metodologii), aceasta se foloseşte de o structură ierarhică propusă pentru evaluarea cadrelor şi este bazată pe abordarea de tip „Multiple Attribute Decision Making (MADM)" şi de definirea valorilor de „rating" (clasificare) pentru a analiza cadrele de management al riscului de securitate cibernetică din sfera de aplicare a metodologiei şi pentru determinarea valorilor de „rating" ale cadrelor. În ceea ce priveşte structura ierarhică propusă (a se vedea Figura 4.2), aceasta constă din şapte dimensiuni şi 13 criterii de evaluare, iar aceste criterii au fost formulate pentru a permite o mai amplă caracterizare a cadrelor pe baza dimensiunilor următoare: definiţia, scopul, şi tipul cadrului de management al riscului de securitate cibernetică, compatibilitatea cu alte cadre şi standarde sau cerinţe de reglementare, elemente esenţiale aparţinând procesului de management al riscului, documentaţia aferentă disponibilă, şi îmbunătăţirea continuă a cadrelor.

În ceea ce priveşte definirea valorilor de „rating", şase valori lingvistice au fost definite incluzând „True", „Partly", „Partly*", „Partly**", „False", şi „Unclear". În primul rând, valoarea „True" a fost utilizată pentru a indica faptul că acel criteriu de evaluare este îndeplinit pe deplin. În al doilea rând, valoarea „Partly" a fost utilizată pentru a indica faptul că acel criteriu de evaluare se aplică într-o anumită masură, dar nu este îndeplinit pe deplin. În al treilea rând, valoarea „Partly*" a fost utilizată pentru a indica, după caz, faptul că acel criteriu de evaluare se aplică în ambele sensuri. În al patrulea rând, valoarea „Partly**" a fost utilizată pentru a indica faptul că acel criteriu de evaluare se aplică în limita unor anumite constrângeri de accesibilitate. În al cincilea rând, valoarea „False" a fost utilizată pentru a indica faptul că acel criteriu de evaluare, aşa cum acesta este exprimat, nu este îndeplinit. În al şaselea şi ultimul rând, valoarea „Unclear" a fost utilizată pentru a indica faptul că valoarea corespunzătoare acelui criteriu de evaluare nu poate fi atribuită cu precizie la nici una dintre cele cinci volori descrise anterior deoarece informaţiile necesare nu sunt clar specificate. În consecinţă, pentru determinarea valorilor de „rating" ale cadrelor, analiza cadrelor din sfera de aplicare a acestei metodologii implică alocarea valorilor lingvistice de „rating" fiecărui criteriu de evaluare pentru fiecare cadru din sfera de aplicare a metodologiei în cauză cu scopul de a indica în ce masură aceste cadre îndeplinesc anumite criterii de evaluare.

Cu privire la a treia etapă a metodologiei, şi anume etapa „comparison of in-scope frameworks" (compararea cadrelor din sfera de aplicare a acestei metodologii), aceasta se foloseşte de valorile de „rating" ale cadrelor care rezultă din etapa a doua a metodologiei propuse în vederea stabilirii diferenţelor şi asemănărilor între cadrele de management al riscului de securitate cibernetică din sfera de aplicare a metodologiei în cauză.

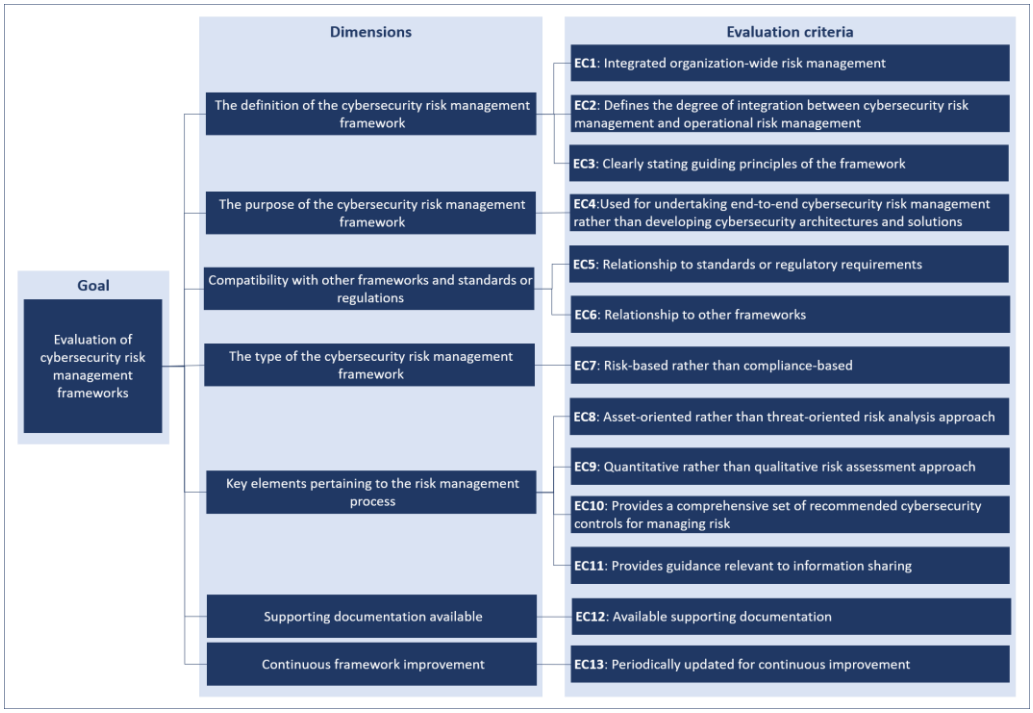

Figura 4.2. Structura ierarhică propusă pentru evaluarea cadrelor din sfera de aplicare a metodologiei de evaluare a cadrelor [Pop20]

În continuare, **Capitolul 4.2** oferă o evaluare critică a cadrelor de management al riscului de securitate cibernetică din sfera de aplicare a metodologiei propuse pentru evaluarea cadrelor. Astfel, au fost identificate opt cadre de management al riscului de securitate cibernetică ca fiind în sfera de aplicare a metodologiei în cauză, şi anume „NIST's Framework for Improving Critical Infrastructure Cybersecurity" (denumit în continuare NIST CSF), „NIST's Unified Information Security Framework" (denumit în continuare NIST UISF), „Operationally Critical Threat, Asset, and Vulnerability Evaluation" (denumit în continuare OCTAVE), „Factor Analysis of Information Risk framework" (denumit în continuare FAIR), „Sherwood Applied Business Security Architecture" (denumit în continuare SABSA), „MITRE's Cyber Resiliency Engineering Framework" (denumit în continuare MITRE CREF), „AICPA's Cybersecurity Risk Management Reporting Framework" (denumit în continuare AICPA), şi „CIS Controls version 7 framework" (denumit în continuare CIS).

Mai mult, evaluarea critică a acestor cadre este prezentată împreună cu concluziile care oferă o caracterizare consolidată a cadrelor de management al riscului de securitate cibernetică din sfera de aplicare a metodologiei în cauză şi evidenţiază asemănările şi deosebirile între acestea prin intermediul celor 13 criterii de evaluare ale metodologiei de evaluare propuse. Prin urmare, referitor la criteriul de evaluare EC1, şi anume „Integrated organization-wide risk management" (managementul integrat al riscului la nivel de organizaţie), acesta este îndeplinit pe deplin de cadrele NIST CSF, NIST UISF, şi SABSA şi nu este îndeplinit de cadrele OCTAVE, FAIR, AICPA, şi CIS. Referitor la criteriul de evaluare EC2, şi anume „Defines the degree of integration between cybersecurity risk management and operational risk management" (defineşte gradul de integrare între managementul riscului de securitate cibernetică şi managementul riscului operaţional), acesta este îndeplinit pe deplin de cadrele NIST CSF, SABSA, şi CIS şi nu este îndeplinit de celelalte cadre. Referitor la criteriul de evaluare EC3, şi anume „Clearly stating guiding principles of the framework" (principiile directoare ale cadrului sunt stitpulate în mod clar), acesta este îndeplinit pe deplin de cadrele OCTAVE, SABSA, MITRE CREF, AICPA, şi CIS şi nu este îndeplinit de cadrul FAIR. Referitor la criteriul de evaluare EC4, şi anume „Used for undertaking end-to-end cybersecurity risk management rather than developing cybersecurity architectures and solutions" (utilizat mai degrabă pentru întreprinderea de management al riscului de securitate cibernetică cap la cap decât pentru arhitecturi şi soluţii de securitate cibernetică), acesta este îndeplinit pe deplin de cadrele NIST CSF şi NIST UISF şi se aplică în ambele sensuri la cadrul SABSA. Referitor la criteriul de evaluare EC5, şi anume „Relationship to standards or regulatory requirements" (relaţia cu standarde sau cerinţe de reglementare), şi EC6, şi anume „Relationship to other frameworks" (relaţia cu alte cadre), acesta este îndeplinit pe deplin de toate cadrele de management al riscului de securitate cibernetică din sfera de aplicare a metodologiei în cauză. Referitor la criteriul de evaluare EC7, şi anume „Risk-based rather than compliance-based" (bazat mai degrabă pe riscuri decât pe reguli), acesta este îndeplinit pe deplin de cadrele NIST CSF,

NIST UISF, OCTAVE, FAIR, SABSA, şi MITRE CREF, se aplică în ambele sensuri la cadrul CIS, şi nu este îndeplinit de cadrul AICPA. Referitor la criteriul de evaluare EC8, şi anume „Asset-oriented rather than threat-oriented risk analysis approach" (abordare de analiză a riscului orientată mai degrabă către active decât către ameninţări), acesta este îndeplinit pe deplin de cadrele OCTAVE, FAIR, SABSA, şi AICPA, se aplică în ambele sensuri la cadrul CIS, şi nu este îndeplinit de cadrul NIST UISF. Referitor la criteriul de evaluare EC9, şi anume „Quantitative rather than qualitative risk assessment approach" (abordare de evaluare a riscului mai degrabă cantitativă decât calitativă), acesta este îndeplinit pe deplin de cadrul FAIR, se aplică în ambele sensuri la cadrul SABSA, şi nu este îndeplinit de cadrele NIST UISF, OCTAVE, şi CIS. Referitor la criteriul de evaluare EC10, şi anume „Provides a comprehensive set of recommended cybersecurity controls for managing risk" (oferă un set complet de controale de securitate cibernetică recomandate pentru managementul riscului), acesta este îndeplinit pe deplin de cadrele NIST UISF, OCTAVE, SABSA, AICPA, şi CIS, şi nu este îndeplinit de cadrul FAIR. Referitor la criteriul de evaluare EC11, şi anume „Provides guidance relevant to information sharing" (oferă orientări privind schimbul de informaţii), acesta este îndeplinit pe deplin de cadrele NIST CSF, NIST UISF, SABSA, MITRE CREF, şi AICPA, şi nu este îndeplinit de cadrele OCTAVE şi FAIR. Referitor la criteriul de evaluare EC12, şi anume „Available supporting documentation – procedures, templates, methods, case studies, etc." (Documnetaţie aferentă disponibilă – proceduri, şabloane, metode, studii de caz, etc.), acesta este îndeplinit pe deplin de cadrele NIST CSF, NIST UISF, OCTAVE, şi CIS. Referitor la criteriul de evaluare EC13, şi anume „Periodically updated for continuous improvement" (actualizate periodic în vederea îmbunătăţirii continue), acesta este îndeplinit pe deplin de toate cadrele de management al riscului de securitate cibernetică din sfera de aplicare a metodologiei în cauză (cu excepţia cadrului OCTAVE).

În continuare, **Capitolul 4.3** oferă lucrările conexe privind evaluarea cadrelor de management al riscului de securitate cibernetică şi acestea sunt discutate prin analizarea sferei de aplicare a lucrărilor de cercetare anterioare şi prin analizarea abordărilor adoptate de aceste lucrări în vederea tratării problemelor legate de domeniul de aplicare al acestor lucrări. Cu privire la domeniul de aplicare al lucrărilor de cercetare anterioare, lucrările conexe s-au axat în principal pe evaluări cu un domeniu de aplicare mai restrâns (şi anume care aboredează mai puţine cadre, care sunt limitate la un anumit domeniu de interes) sau pe evaluări cu un domeniu de aplicare parţial diferit (şi anume care abordează bunele practici indiferent de tipul acestora, care se axează doar pe evaluarea riscului sau pe metodologii pentru managementul riscului sau pe metode). Cu privire la abordările adoptate de lucrările conexe în vederea tratării problemelor legate de domeniul de aplicare al acestor lucrări, au fost identificate patru tipuri de abordări. Aceste tipuri includ prezentarea punctelor forte şi punctelor slabe, comparaţia fondată pe structura procesului de evaluare al riscului sau de management al riscului, comparaţia fondată pe criterii de evaluare definite, comparaţia de tip caracteristică cu caracteristică. Aşadar, analiza a scos la iveală faptul că studiile conexe anterioare nu au avut un domeniu de aplicare mai larg şi nici nu s-au exat exclusiv pe evaluarea cadrelor.

Capitolul 5. Model de Referinţă pentru Strategia de Management al Riscului Securităţii Cibernetice pentru Internetul Obiectelor (IoTSRM2)

Capitolul 5 extinde munca de cercetare redată în **Capitolul 2** privind bunele practici de securitate cibernetică pentru internetul obiectelor (IoT), prin propunerea unei metodologii pentru dezvoltarea modelului de referinţă pentru strategia de management al riscului securităţii cibernetice pentru internetul obiectelor, elaborarea modelului de referinţă propus pentru strategia de management al riscului securităţii cibernetice pentru IoT (IoTSRM2), evaluarea critică a unor referinţe informative selectate a modelului IoTSRM2, şi oferirea unei analize cuprinzătoare a lucrărilor conexe pentru IoTSRM2 bazată pe opt criterii de evaluare. Astfel, prin abordarea necesităţii pentru un model de referinţă pentru strategia de management al riscului securităţii cibernetice pentru internetul obiectelor, capitolul vizează să sprijine practicienii din organizaţiile care adoptă tehnologii de tip IoT în vederea formulării sau redefinirii strategiilor lor de management al riscului de securitate cibernetică pentru IoT şi în vederea obţinerii unei adoptări adecvate de IoT, şi să sprijine alţi cercetători din mediul academic care urmăresc să studieze tema strategiei de management al risuclui de securitate cibernetică pentru IoT în cadrul demersurilor lor de cercetare.

Capitolul 5.1 descrie metodologia în trei etape pentru dezvoltarea modelului IoTSRM2 prin descrierea celor nouă paşi a metodologiei şi a rezultatelor asociate (a se vedea Figura 5.1).

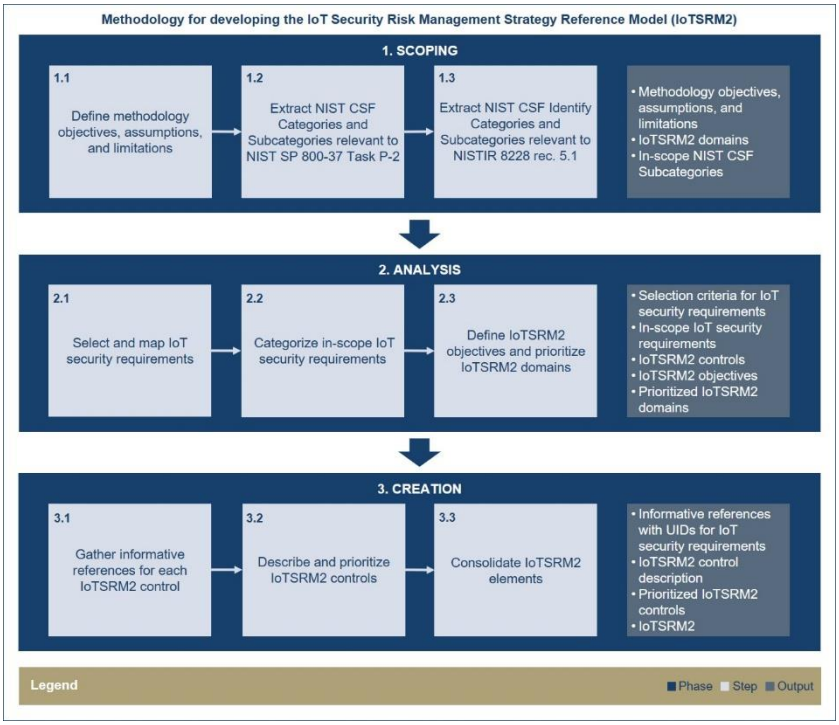

Figura 5.1. Methodologia în trei etapte propusă pentru dezvoltarea modelului IoTSRM2 [Pop+21a]

Cu privire la prima etapă („Phase") a metodologiei, şi anume etapa de „Scoping" (definirea domeniului de aplicare al metodologiei), care include trei paşi, Pasul 1.1 („Step") a implicat definirea obiectivelor, ipotezelor, şi limitărilor metodologiei pentru dezvoltarea modelului IoTSRM2. În continuare, Pasul 1.2 a implicat identificarea celor şase domenii a modelului IoTSRM2. Pe urmă, Pasul 1.3 a implicat determinarea subcategoriilor cadrului privind securitatea cibernetică de la NIST (denumite în continuare „NIST CSF Subcategories") din sfera de aplicare a acestei metodologii. Cu privire la a doua etapă a metodologiei, şi anume etapa de „Analysis" (analiză), care include trei paşi, Pasul 2.1 a implicat definirea criteriilor de selecţie a cerinţelor de securitate cibernetică pentru IoT din cadrul celor 25 bune practici de securitate cibernetică pentru IoT selectate (a se vedea **Capitolul 2.4**), şi corelarea cerinţelor de securitate cibernetică pentru IoT selectate cu „NIST CSF Subcategories" din sfera de aplicare a acestei metodologii în vederea determinării cerinţelor de securitate cibernetică pentru IoT din sfera de aplicare a metodologiei în cauză. În continuare, Pasul 2.2 a implicat categorisirea cerinţelor rezultate de securitate cibernetică pentru IoT din sfera de aplicare a acestei metodologii pentru a permite determinarea controalelor modelului IoTSRM2. Pe urmă, Pasul 2.3 a implicat definirea fiecarui obiectiv al modelului IoTSRM2 pe baza subcategoriei asociate „NIST CSF Subcategory" din sfera de aplicare a metodologiei în cauză şi pe baza controalelor associate din cadrul modelului IoTSRM2. În plus, Pasul 2.3 a implicat prioritizarea domeniilor modelului IoTSRM2 pe baza numărului de obiective al modelului IoTSRM2 corespunzător acestor domenii. În sfârşit, cu privire la a treia etapă a metodologiei, şi anume etapa de „Creation" (creare), care include trei paşi, Pasul 3.1 a implicat pentru fiecare control al modelului IoTSRM2, colectarea şi documentarea referinţelor informative asociate şi identificatorilor unici ai cerinţelor de securitate cibernetică pentru IoT din sfera de aplicare a acestei metodologii. Ulterior, Pasul 3.2 a implicat decrierea într-o manieră consistentă a controalelor modelului IoTSRM2 conform cu nivelele de detaliere pentru controale bazate pe granularitatea ţintă privind informaţia, şi anume descrierea controlului trebuia să includă activităţile/acţiunile privind securitatea cibernetică pentru IoT aşteptate din partea celor care adoptă IoT („IoT adopters"), puncte de integrare între activităţile/acţiunile privind securitatea cibernetică pentru IoT aşteptate din partea celor care adoptă IoT şi programele de securitate cibernetică a acestora, şi activităţile/acţiunile privind securitatea cibernetică pentru IoT ale furnizorilor de IoT („IoT suppliers") care guvernează acţiunile acestora după introducerea produselor IoT pe piaţă (etapa de „postmarket") şi care ar trebui sa fie aşteptate din partea acestora de către organizaţia care adoptă IoT. De asemenea, acest pas a implicat prioritizarea controalelor modelului IoTSRM2 în cadrul fiecarui obiectiv pe baza ponderilor ajustate corespunzătoare acestora, care au fost determinate cu ajutorul Ecuaţiilor (5.1) şi (5.2). Aşadar, Ecuaţia (5.1) permite determinarea ponderilor corespunzătoare fiecărui control al modelului IoTSRM2 ţinând seama pentru fiecare control de numarul mediu de cerinţe de securitate cibernetică pentru IoT din sfera de aplicare a metodologiei în cauză pe o referinţă informativă aplicabilă şi de numarul de cerinţe de securitate cibernetică pentru

IoT din sfera de aplicare a metodologiei în cauză raportat la cele 25 de bune practici de securitate cibernetică pentru IoT selectate. În această ecuaţie, x_{ijk} reprezintă controalele obiectivelor x_{ij} corespunzător domeniilor x_i ale modelului IoTSRM2, $R(x_{ijk})$ reprezintă numarul de cerinţe de securitate cibernetică pentru IoT din sfera de aplicare a metodologiei în cauză aplicabile pentru fiecare din controalele x_{ijk} al fiecăruia din obiectivele x_{ij} al fiecăruia din domeniile x_i ale modelului IoTSRM2, $I(x_{ijk})$ reprezintă numărul de cerinţe informative aplicabile pentru fiecare din controalele x_{ijk} al fiecăruia din obiectivele x_{ij} al fiecăruia din domeniile x_i al modelului IoTSRM2, p reprezintă numarul de bune practici de securitate cibernetică pentru IoT selectate (a se vedea **Capitolul 2.4**), C reprezintă cardinalitatea mulţimii x_i de domenii ale modelului IoTSRM2, C_i reprezintă cardinalităţile mulţimilor x_{ij} de obiective ale fiecarui domeniu din mulţimea x_i de domenii ale modelului IoTSRM2, şi n_{ij} reprezintă numarul de controale corespunzător fiecarui obiectiv al multimii x_{ij} de obiective.

$$\text{Weight}\,(x_{ijk}) = \frac{R(x_{ijk})}{I(x_{ijk})} + \frac{R(x_{ijk})}{p}\,, \qquad \text{where } C=|x_i|,\ i=[1..C],\ C_i=|x_{ij}|,\ j=[1..C_i],\ k=[1..n_{ij}] \tag{5.1}$$

În continuare, ponderile controalelor au fost ajustate cu ajutorul Ecuaţiei (5.2) în vederea normalizării valorilor:

$$\text{Adjusted weight}\,(x_{ijk}) = \frac{1}{\sum_1^C C_q} * \frac{\text{Weight}\,(x_{ijk})}{\sum_{s=1}^{n_{ij}} \text{Weight}\,(x_{ijs})} * 100\%\,, \qquad \text{where } i=[1..C],\ j=[1..C_i],\ k=[1..n_{ij}],\ \sum_{i=1}^{C}\sum_{j=1}^{C_i}\sum_{k=1}^{n_{ij}} \text{Adjusted weight}\,(x_{ijk}) = 100\% \tag{5.2}$$

În final, Pasul 3.3 a implicat consolidarea elementelor modelului IoTSRM2 pentru a pune în valoare modelul IoTSRM2 propus.

Ulterior, **Capitolul 5.2** prezintă modelul IoTSRM2 propus care conţine şase domenii, 16 obiective, şi 30 controale pentru organizaţiile din orice sector care adoptă IoT, care ar trebui abordate atât de cele care adoptă IoT, cât şi de cele care furnizează IoT. În primul rând, capitolul oferă o prezentare genrală ilustrativă a modelului IoTSRM2 propus (a se vedea Figura 5.2).

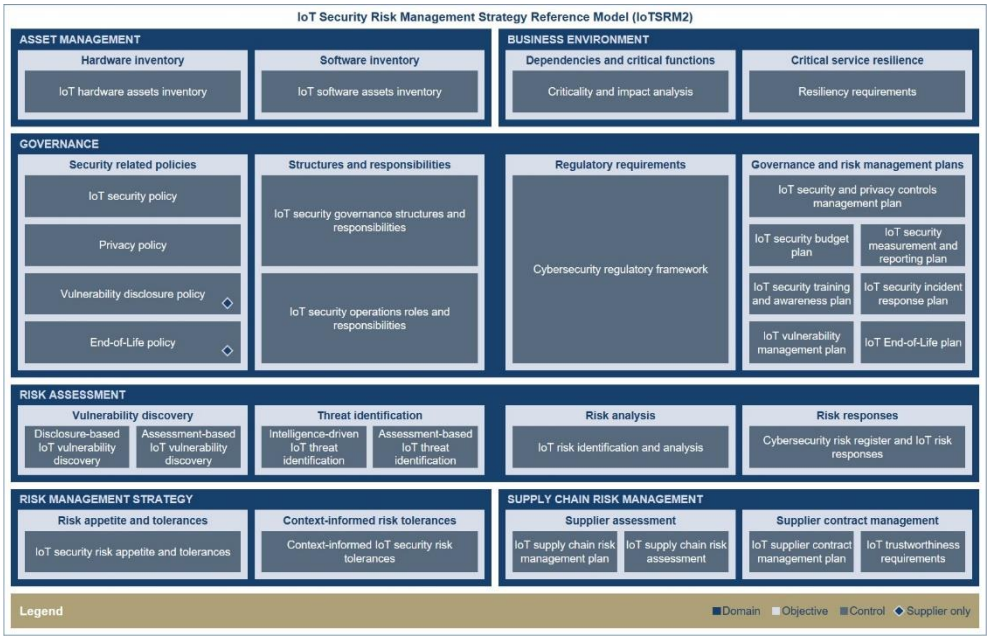

Figura 5.2. Modelul IoTSRM2 propus [Pop+21a]

În continuare, pentru fiecare referinţă informativă a modelului IoTSRM2 propus, capitolul oferă numarul total de cerinţe unice de securitate cibernetică pentru IoT din sfera de aplicare a metodologiei de elaborare a modelului în cauză corelate cu controalele modelului IoTSRM2, şi indică dacă referinţa informativă a rezultat ca fiind una dintre cele mai relevante referinţe dintre referinţele informative ale modelului IoTSRM2 pentru strategia de management al riscului de securitate cibernetică pentru IoT. În continuare, pentru fiecare domeniu al modelului IoTSRM2, capitolul oferă obiectivele domeniului respectiv al modelului IoTSRM2, şi pentru fiecare obiectiv al domeniului respectiv capitolul descrie controalele obiectivului respectiv în conformitate cu granularitatea ţintă privind informaţia. În plus, pentru fiecare domeniu al modelului IoTSRM2, capitolul oferă, printre altele, prioritizarea controalelor obiectivului în cauză pe baza ponderilor ajustate ale acestora care au fost calculate folosind Ecuaţiile (5.1) şi (5.2).

În continuare, **Capitolul 5.3** oferă o evaluare critică a unor referinţe informative selectate a modelului IoTSRM2 pe baza legăturii lor cu modelul IoTSRM2 din punct de vedere procentual, care este structurată în şapte părţi, şi anume în evaluarea globală a referinţelor informative selectate şi evaluările individuale ale referinţelor informative selectate pentru fiecare domeniu al modelului IoTSRM2. În acest context, din cele 25 de referinţe informative ale modelului IoTSRM2, şapte referinţe informative (şi anume ref. [Age20a], ref. [CSA19a], ref. [ENI18b], ref. [ENI20a], ref. [IoT16], ref. [IoT20a], şi ref. [NIS20a]) au fost selectate pentru evaluare luând în considerare că acestea au rezultat ca fiind cele mai relevante pentru strategia de management al riscului de securitate cibernetică pentru IoT pe baza îndeplinirii a două criterii de includere şi a două condiţii, şi anume să includă referinţele informative care sunt cele mai axate pe strategia de management al riscului de securitate cibernetică pentru IoT şi acele referinţe informative care sunt cele mai aplicabile la modelul IoTSRM2 astfel încât numarul total de cerinţe de securitate cibernetică pentru IoT aplicabile la modelul IoTSRM2 al referinţelor informative unice selectate să se ridice la cel puţin jumătate din numarul total de cerinţe de securitate cibernetică pentru IoT aplicabile la modelul IoTSRM2 al tutror celor 25 referinţe informative. Astfel, cu privire la evaluarea globală a referinţelor informative selectate, de exemplu, concluziile au arătat că ref. [ENI18b] prezintă cele mai puternice legături cu modelul IoTSRM2 dintre cele 25 de referinţe informative şi că ref. [IoT16] este cea mai puţin legată de modelul IoTSRM2 dintre referinţele informative selectate (a se vedea Figura 5.3).

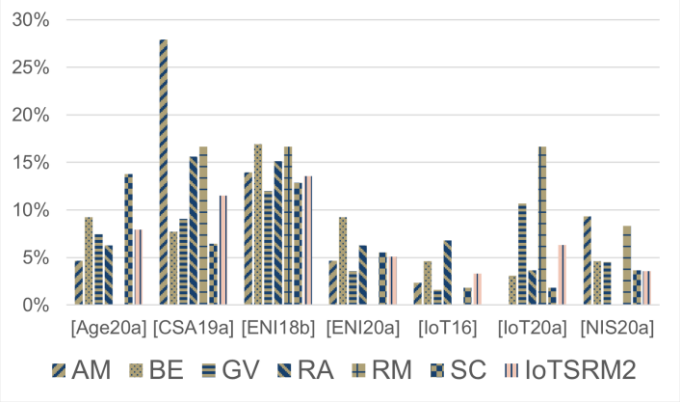

Figura 5.3. Evaluarea referinţelor informative ale modelului IoTSRM2 din punct de vedere procentual [Pop+21a]

Mai mult, printre altele, concluzile au arătat că majoritatea referinţelor informative selectate sunt cel mai axate pe domeniul „Governance" (guvernanţa) al modelului IoTSRM2, şi acestea sunt cel mai puţin axate pe domeniul „Risk Management Strategy" (strategia de gestionare a riscurilor) al modelului IoTSRM2 (a se vedea Figura 5.4).

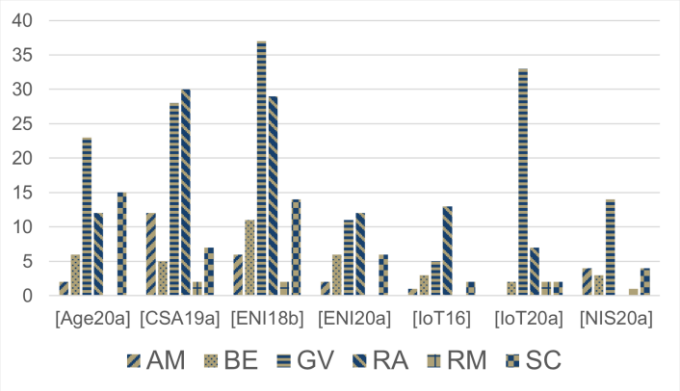

Figura 5.4. Evaluarea referinţelor informative selectate ale modelului IoTSRM2 [Pop+21a]

În continuare, cu privire la evaluările individuale ale referinţelor informative selectate pentru fiecare domeniu al modelului IoTSRM2, în primul rând, referitor la domeniul „Asset Management" (gestionarea activelor) al modelului IoTSRM2, concluziile au arătat printre altele că ref. [CSA19a] este cea mai legată de domeniul în cauză şi că ref. [IoT20a] este cea mai puţin legată de domeniul în cauză dintre referinţele informative selectate. În al doilea rând, referitor la domeniul „Business Environment" (mediul de afaceri) al modelului IoTSRM2, concluziile au arătat printre altele că ref. [ENI18b] este cea mai legată de domeniul în cauză şi că ref. [IoT20a] este cea mai puţin legată de domeniul în cauză dintre referinţele informative selectate. În al treilea rând, referitor la domeniul „Governance" (guvernanţa) al modelului IoTSRM2, concluziile au arătat printre altele că ref. [ENI18b] este cea mai legată de domeniul în cauză şi că ref. [IoT16] este cea mai puţin legată de domeniul în cauză dintre referinţele informative selectate. În al patrulea rând, referitor la domeniul „Risk Assessment" (evaluarea riscurilor) al modelului IoTSRM2, concluziile au arătat printre altele că ref. [CSA19a] este cea mai legată de domeniul în cauză şi că ref. [NIS20a] este cea mai puţin legată de domeniul în cauză dintre referinţele informative selectate. În al cincilea rând, referitor la domeniul „Risk Management Strategy" (strategia de gestionare a riscurilor) al modelului IoTSRM2, concluziile au arătat printre altele că ref. [CSA19a], ref. [ENI18b], şi ref. [IoT20a] sunt cele mai legate de domeniul în cauză şi că ref. [IoT16], ref. [ENI20a], şi ref. [Age20a] sunt cele mai puţin legate de domeniul în cauză dintre referinţele informative selectate. În al şaselea şi ultimul rând, referitor la domeniul „Supply Chain Risk Management" (gestionarea riscurilor aferente lanțului de aprovizionare) al modelului IoTSRM2, concluziile au arătat printre altele că ref. [Age20a] este cea mai legată de domeniul în cauză şi că ref. [IoT20a] şi ref. [IoT16] sunt cele mai puţin legate de domeniul în cauză dintre referinţele informative selectate [Pop21].

Mai departe, **Capitolul 5.4** descrie lucrările conexe. În primul rând, capitolul evidenţiază lipsa lucrărilor de cercetare care să se concentreze doar pe strategia de management al riscului de securitate cibernetică pentru IoT. În continuare, capitolul discută studiile anterioare care se axează pe stadiul actual al cercetării sau pe prezentări generale privind bunele practici de securitate cibernetică pentru IoT faţă de IoTSRM2. În plus, pentru a compara modelul IoTSRM2 propus cu bunele practici aferente privind securitatea cibernetică pentru IoT, capitolul discută modelul IoTSRM2 şi cele 25 de bune practici selectate privind securitatea cibernetică pentru IoT pe baza a opt criterii de evaluare şi trei tipuri de aplicabilitate pentru fiecare criteriu de evaluare (şi anume criteriul de evaluare se aplică pe deplin, criteriul de evaluare se aplică într-o anumită masură dar nu pe deplin, şi criteriul de evaluare nu se aplică). Aşadar, legat de criteriul de evaluare E1, şi anume „Focus on strategic IoT security practices over technical IoT security practices" (prevalează practicile strategice asupra celor tehnice de securitate cibernetică pentru IoT), acesta se aplică pe deplin la şapte referinţe informative şi la IoTSRM2, şi se aplică într-o anumită masură dar nu pe deplin la zece referinţe informative. Legat de criteriul de evaluare E2, şi anume „Methodology for developing the recommended IoT security requirements / controls is clearly described" (metodologia pentru elaborarea cerinţelor / controalelor recomandate pentru securitatea cibernetică privind IoT este descrisă în mod clar), acesta se aplică pe deplin la şapte referinţe informative şi la IoTSRM2, şi se aplică într-o anumită masură dar nu pe deplin la patru referinţe informative. Legat de criteriul de evaluare E3, şi anume „Mapping of IoT security requirements / controls to NIST CSF's Categories and Subcategories" (corelează cerinţele / controalele recomandate pentru securitatea cibernetică privind IoT cu categoriile şi subcategoriile ale cadrului de securitate cibernetică de la NIST), acesta se aplică pe deplin la IoTSRM2, şi se aplică într-o anumită masură dar nu pe deplin la două referinţe informative. Legat de criteriul de evaluare E4, şi anume „Clearly indicate for each IoT security requirement / control expected IoT security actions / activities from IoT suppliers of the target audience" (precizează pentru fiecare cerinţă / control de securitate cibernetică pentru IoT care sunt acţiunile / activităţile aşteptate din partea furnizorilor de

IoT ai publicului ţintă), acesta se aplică pe deplin la IoTSRM2, şi se aplică într-o anumită masură dar nu pe deplin la zece referinţe informative. Legat de criteriul de evaluare E5, şi anume „Provides integration points with the cybersecurity program as part of each IoT security requirement / control" (oferă puncte de integrare cu programul de securitate cibernetică în cadrul fiecărei cerinţe / fiecarui control de securitatea cibernetică pentru IoT), acesta se aplică pe deplin la IoTSRM2, şi se aplică într-o anumită masură dar nu pe deplin la patru referinţe informative. Legat de criteriul de evaluare E6, şi anume „Mapping of relevant IoT security best practices with unique identifiers to each recommended IoT security requirement / control" (corelează bunele practici relevante de securitate cibernetică şi identificatorii unici asociaţi cu fiecare control recomandat / cerinţă recomandată pentru securitatea cibernetică privind IoT), acesta se aplică pe deplin la două referinţe informative şi la IoTSRM2, şi se aplică într-o anumită masură dar nu pe deplin la 11 referinţe informative. Legat de criteriul de evaluare E7, şi anume „Prioritization of the recommended IoT security requirements / controls" (prioritizarea cerinţelor / controalelor recomandate pentru securitatea cibernetică privind IoT), acesta se aplică pe deplin la trei referinţe informative şi la IoTSRM2, şi se aplică într-o anumită masură dar nu pe deplin la patru referinţe informative. În sfârşit, legat de criteriul de evaluare E8, şi anume „Provides statistics for the mapping of informative references" (oferă statistici cu privire la corelarea de referinţe informative), acesta se aplică pe deplin la o referinţă informativă şi la IoTSRM2, şi nu se aplică la celelalte referinţe informative.

Capitolul 6. Aplicarea unui Sondaj bazat pe Modelul IoTSRM2

Capitolul 6 extinde munca de cercetare redată în **Capitolul 5** privind modelul de referinţă pentru strategia de management al riscului securităţii cibernetice pentru internetul obiectelor (IoTSRM2), prin prezentarea celor 14 „research questions" (întrebări de cercetare) pentru sondajul bazat pe IoTSRM2, propunerea unei metodologii de sondaj pentru a răspunde la „research questions", prezentarea rezultatelor sondajului în urma analizei răspunsurilor primite în cadrul sondajului de la lideri din industrii şi guverne din întreaga lume, şi oferirea unei analize cuprinzătoare a lucrărilor conexe corespunzătoare studiului de sondaj bazat pe modelul IoTSRM2 utilizând şapte criterii de evaluare. Astfel, prin abordarea necesitaţii de studii de cercetare axate pe determinarea stadiului actual al strategiilor de management al riscului securităţii cibernetice pentru IoT din organizaţii, capitolul vizează să sprijine practicienii din domeniul securităţii cibernetice pentru IoT din industrii şi guverne în vederea stabilirii stadiului actual al strategiilor lor de management al riscului securităţii cibernetice pentru IoT în comparaţie cu cele ale omologilor lor şi, prin urmare, să le permită acestora să-şi consolideze aceste strategii pentru a atinge sau întrece strategiile omologilor lor.

În primul rând, **Capitolul 6.1** enumeră cele 14 „research questions" pentru studiul de sondaj bazat pe IoTSRM2 şi oferă o „mapă de citire" („reading map") pentru „research questions" (a se vedea Figura 6.1). Cele 14 „research questions" sunt următoarele:

- **RQ1:** Care este tendinţa globală a strategiilor de management al riscului securităţii cibernetice pentru IoT ale organizaţiilor din cadrul sondajului, să respecte sau să devieze de la controalele modelului IoTSRM2?
- **RQ2:** Care este scorul de conformitate cu modelul IoTSRM2 al fiecăreia din organizaţiile incluse în sondaj?
- **RQ3:** Care este cel mai frecvent tip de organizaţie din organizaţiile incluse în sondaj pe baza răspunsurilor respondenţilor la sondaj?
- **RQ4.a:** Care este cel mai frecvent sector industrial al organizaţiilor din cadrul sondajului pe baza răspunsurilor respondenţilor la sondaj?
- **RQ4.b:** Care este cel mai frecvent sector industrial al celui mai frecvent tip de organizaţie din organizaţiile incluse în sondaj pe baza răspunsurilor respondenţilor la sondaj?
- **RQ5.a:** Pentru fiecare control al modelului IoTSRM2, care este media totală a scorului de conformitate cu modelul IoTSRM2 al organizaţiilor din cadrul sondajului?
- **RQ5.b:** Pentru fiecare control al modelului IoTSRM2, care este media totală a scorului de conformitate cu modelul IoTSRM2 al celui mai frecvent tip de organizaţie din organizaţiile incluse în sondaj pe baza răspunsurilor respondenţilor la sondaj?
- **RQ5.c:** Pentru fiecare control al modelului IoTSRM2, care este media totală a scorului de conformitate cu modelul IoTSRM2 al organizaţiilor din cel mai frecvent sector industrial al celui mai frecvent tip de organizaţie din organizaţiile incluse în sondaj pe baza răspunsurilor respondenţilor la sondaj?
- **RQ6.a:** Care este cea mai frecventă poziţie a respondenţilor la sondaj pe baza răspunsurilor acestora?

- **RQ6.b:** Care este cea mai frecventă poziţie a respondenţilor la sondaj privind cel mai frecvent tip de organizaţie din organizaţiile incluse în sondaj pe baza răspunsurilor acestora?
- **RQ6.c:** Care este cea mai frecventă poziţie a respondenţilor la sondaj privind organizaţiilor din cel mai frecvent sector industrial al celui mai frecvent tip de organizaţie din organizaţiile incluse în sondaj pe baza răspunsurilor acestora?
- **RQ7.a:** Care este cea mai frecventă regiune în care îşi au sediul organizaţiile din cadrul sondajului pe baza răspunsurilor respondenţilor la sondaj?
- **RQ7.b:** Care este cea mai frecventă regiune în care îşi au sediul organizaţiile celui mai frecvent tip de organizaţie din organizaţiile incluse în sondaj pe baza răspunsurilor respondenţilor la sondaj?
- **RQ7.c:** Care este cea mai frecventă regiune în care îşi au sediul organizaţiile din cel mai frecvent sector industrial al celui mai frecvent tip de organizaţie din organizaţiile incluse în sondaj pe baza răspunsurilor respondenţilor la sondaj?

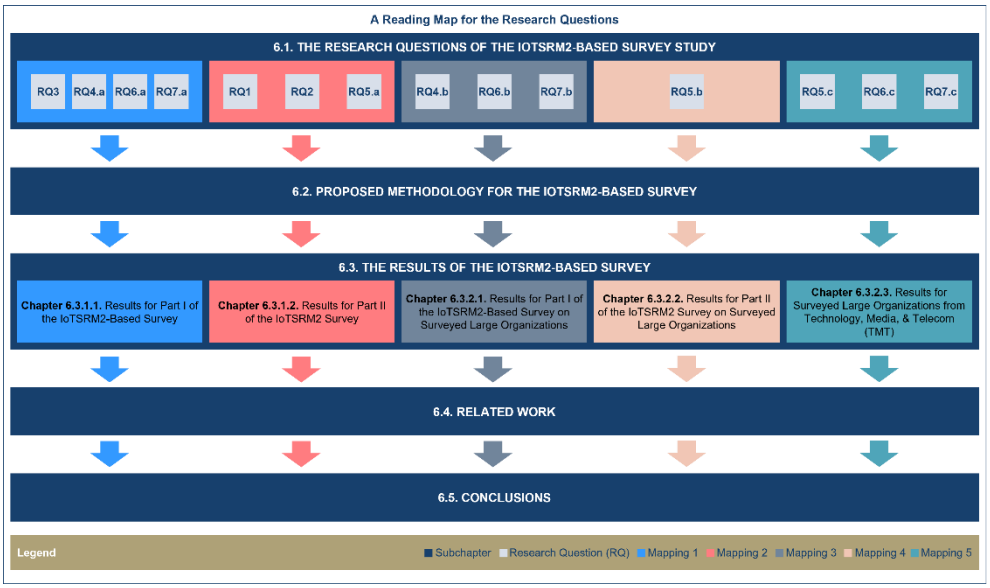

Figura 6.1. O „mapă de citire” pentru „research questions” [Pop+21b]

În continuare, **Capitolul 6.2** descrie metodologia de sondaj în trei etape propusă pentru a răspunde la „research questions” prin descrierea celor nouă paşi ai metodologiei şi a rezultatelor asociate (a se vedea Figura 6.2). Cu privire la prima etapă („Phase”) a metodologiei de sondaj, şi anume etapa de „Plan and Create” (planificare şi creare), care include trei paşi, Pasul I.1 („Step”) a implicat definirea obiectivelor metodologiei de sondaj, ipotezelor, şi limitărilor metodologiei de sondaj şi sondajului aferent. În continuare, Pasul I.2 a implicat crearea chestionarului pentru sondajul bazat pe modelul IoTSRM2, care este structurat în două părţi: partea I a chestionarului incluzând cinci întrebări de fond şi de „screening” (selecţie) cu răspunsurile posibile aferente, şi partea II a chestionarului incluzând 30 de întrebări legate de modelul IoTSRM2 cu răspunsurile posibile aferente (şi anume „No, to a great extent” – nu, într-o mare măsură; „No, to a certain extent” – nu, într-o oarecare măsură, „Yes, to a certain extent” – da, într-o oarecare măsură; „Yes, to a great extent” – da, într-o mare măsură). Pe urmă, Pasul I.3 a implicat conceperea şi elaborarea sondajului pe baza principiilor pentru proiectarea chestionarelor web create de Dillman et al. (1999) [Dil+99], împreună cu elaborarea planului de analiză a sondajului. Cu privire la a doua etapă a metodologiei de sondaj, şi anume etapa de „Launch and Run” (lansare şi derulare), care include trei paşi, Pasul II.1 a implicat identificarea respondenţilor ţintă pentru baza de sondaj („sampling frame”), şi crearea şi trimiterea solicitărilor de participare la sondajul bazat pe modelul IoTSRM2 către respondenţii vizaţi. În continuare, Pasul II.2 a implicat trimiterea unei combinaţii de note de reamintire incluzând mesaje private şi postări pe platformele de comunicare socială despre sondajul bazat pe modelul IoTSRM2. Pe urmă, Pasul II.3 a implicat exportarea din SurveyMonkey în Excel a tuturor răspunsurilor primite în cadrul sondajului de îndată ce sondajul s-a încheiat.

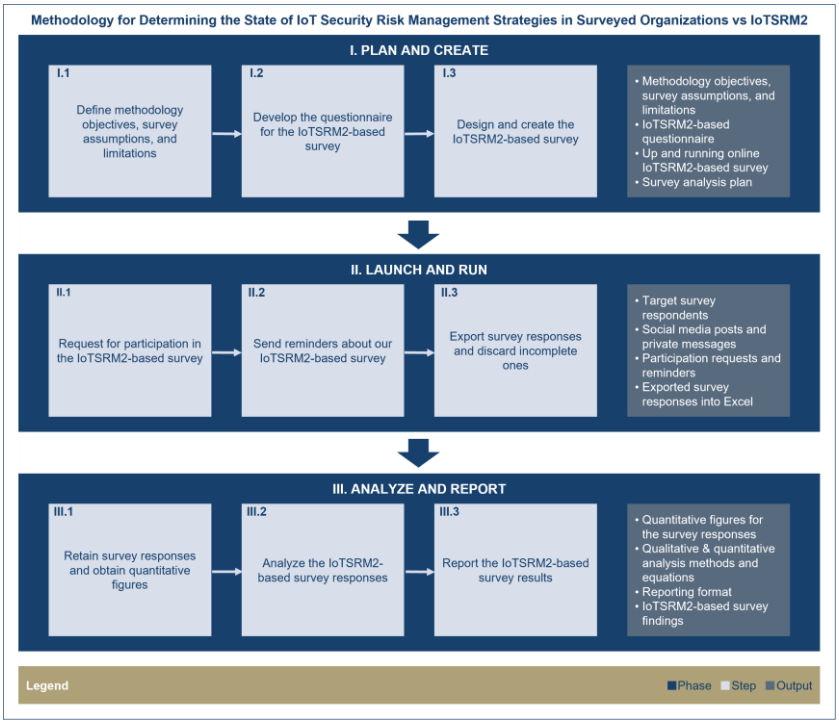

Figura 6.2. Metodologia în trei etape propusă pentru sondajul bazat pe modelul IoTSRM2 [Pop+21b]

În sfârşit, cu privire la a treia etapă a metodologiei de sondaj, şi anume etapa de „Analyze and Report" (analiză şi raportare), care include trei paşi, Pasul III.1 a implicat păstrarea răspunsurilor primite în cadrul sondajului în forma lor originală şi conversia răspunsurilor calitative legate de modelul IoTSRM2 în valori cantitative cu ajutorul Ecuaţiei (6.1), în care Q_j reprezintă cele 30 de întrebări legate de modelul IoTSRM2, $Response_i(Q_j)$ reprezintă răspunsurile respondenţilor din cadrul sondajului la întrebările legate de modelul IoTSRM2, R_{ij} reprezintă procentele corespunzătoare raspunsurilor respondenţilor la întrebările legate de modelul IoTSRM2 (a se vedea Pasul I.2), şi K reprezintă cardinalitatea mulţimii de respondenţi la sondaj.

$$\text{Convert } (Response_i(Q_j))=R_{ij},$$

$$\text{where } R_{ij}=\begin{cases} 0, Response_i(Q_j)\text{="No, to a great extent"} \\ 30\%, Response_i(Q_j)\text{="No, to a certain extent"} \\ 70\%, Response_i(Q_j)\text{="Yes, to a certain extent"} \\ 100\%, Response_i(Q_j)\text{="Yes, to a great extent"} \end{cases} \quad (6.1)$$

$$i=[1..K],\ j=[6..35],\ \text{and } K=|\text{survey respondents}|$$

Ulterior, Pasul III.2 a implicat analiza tuturor răspunsurilor primite în cadrul sondajului pentru trei grupuri de organizaţii din cadrul sondajului (a se vedea Figura 6.3). Astfel, cu privire la analiza răspunsurilor primite în cadrul sondajului corespunzătoare părţii I a sondajului bazat pe modelul IoTSRM2, în primul rând, analiza I.A a urmărit să răspundă la întrebările RQ6.a, RQ6.b, şi RQ6.c. În al doilea rând, analiza I.B a urmărit să răspundă la întrebarea RQ3. În al treilea rând, analiza I.C a urmărit să răspundă la întrebările RQ4.a şi RQ4.b. În final, analiza I.D a urmărit să răspundă la întrebările RQ7.a, RQ7.b, şi RQ7.c.

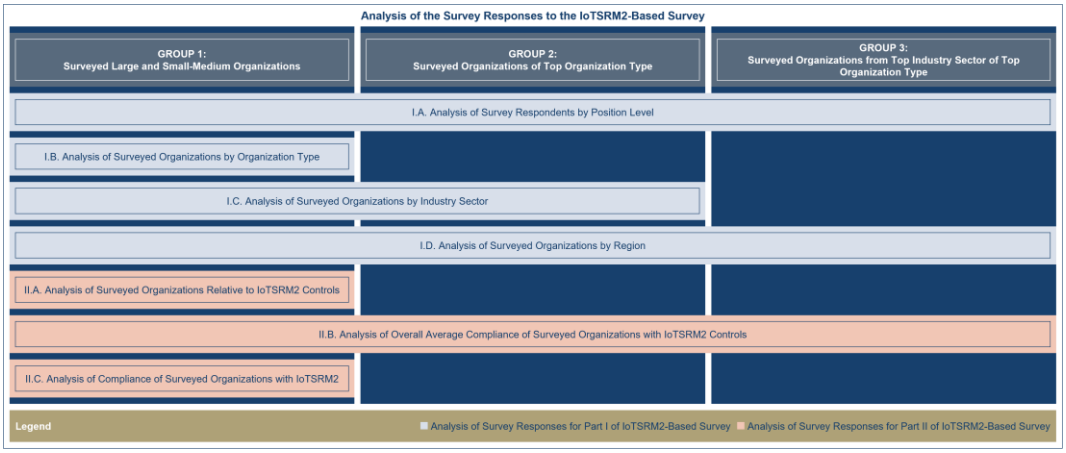

Figura 6.3. Schiţarea analizei răspunsurilor la sondajul bazat pe modelul IoTSRM2 [Pop+21b]

De asemenea, cu privire la analiza răspunsurilor primite în cadrul sondajului corespunzătoare părţii II a sondajului bazat pe modelul IoTSRM2, în primul rând, analiza II.A a urmărit să răspundă la întrebarea RQ1. Pentru fiecare întrebare legată de modelul IoTSRM2, această analiză a implicat compararea procentelor aferente răspunsurilor de „Yes, to a certain extent" şi „Yes, to a great extent" cu procentele aferente răspunsurilor de „No, to a great extent" şi „No, to a certain extent". În al doilea rând, analiza II.B a urmărit să răspundă la întrebările RQ5a, RQ5.b şi RQ5.c. Pentru fiecare grup de organizaţii din cadrul sondajului, această analiză a implicat pentru fiecare control şi întrebare legate de modelul IoTSRM2 determinarea mediei totale a scorului de conformitate cu modelul IoTSRM2 folosind Ecuaţiile (6.2) şi (6.3) care se bazează pe răspunsurile la sondaj şi pe ponderile ajustate associate. În Ecuaţia (6.2), $\text{Compliance}_i(C_j)$ reprezintă scorurile de conformitate ale organizaţiilor din cadrul sondajului cu controalele modelului IoTSRM2, C_j reprezintă controalele modelului IoTSRM2 care corespund la întrebările legate de modelul IoTSRM2, Adjusted weight (C_j) reprezintă ponderile ajustate corespunzătoare controalelor modelului IoTSRM2, iar R_{ij} şi K sunt descrise mai sus (a se vedea Pasul III.1).

$$\text{Compliance}_i(C_j) = R_{ij} * \text{Adjusted weight } (C_j)$$
$$\text{where } i=[1..K],\ j=[6..35],\ \text{and } K=|\text{survey respondents}| \tag{6.2}$$

Mai departe, valorile mediilor totale de conformitate au fost calculate utilizând Ecuaţia (6.3), unde L_k reprezintă cardinalitatea mulţimii de respondenţi la sondaj corespunzătoare fiecărui Group k de organizaţii din cadrul sondajului (a se vedea „Group 1" – grupul 1, „Group 2" – grupul 2, şi „Group 3" – grupul 3 în Figura 6.3), iar $\text{Compliance}_i(C_j)$ şi C_j sunt descrise mai sus.

$$\text{Overall average compliance } (C_j) = \frac{\sum_{i=1}^{L_k} \text{Compliance}_i(C_j)}{L_k},$$
$$\text{where } i=[1..L_k],\ j=[6..35],\ k=[1..3], \tag{6.3}$$
$$\text{and } L_k = |\text{survey respondents for Group k of surveyed organizations}|$$

În al treilea rând, analiza II.C a urmărit să răspundă la întrebarea RQ2. Pentru fiecare organizaţie din cadrul sondajului, acestă analiză a implicat determinarea scorului de conformitate cu modelul IoTSRM2 folosind Ecuaţia (6.4), în care IoTSRM2 compliance score_i reprezintă scorurile de conformitate cu modelul IoTSRM2 ale organizaţiilor din cadrul sondajului, iar $\text{Compliance}_i(C_j)$, C_j, şi K sunt descrise mai sus.

$$\text{IoTSRM2 compliance score}_i = \sum_{j=6}^{35} \text{Compliance}_i(C_j), \tag{6.4}$$

where i=[1..K], j = [6..35], K=|survey respondents|

În plus, acest pas a implicat elaborarea unei convenţii de denumire pentru organizaţiile din cadrul sondajului în vederea facilitării analizei II.C şi pentru a le distinge pe aceste cu o mai mare uşurinţă luând în considerare caracterul anonim al sondajului bazat pe modelul IoTSRM2.

În ultimul rând, Pasul III.3 a oferit structura de raportare pentru constatările sondajului bazat pe modelul IoTSRM2 şi a implicat raportarea rezultatelor sondajului în cauză pentru fiecare din cele trei grupuri de organizaţii din cadrul sondajului (a se vedea Pasul III.2).

Ulterior, **Capitolul 6.3** prezintă rezultatele sondajului bazat pe modelul IoTSRM2 pentru cele trei grupuri de organizaţii din cadrul sondajului (şi anume organizaţiile mari şi mici şi mijlocii din cadrul sondajului, organizaţiile mari din cadrul sondajului, şi organizaţiile mari din sectorul TMT – Tehnologie, Media și Telecomunicații – din cadrul sondajului) care arată starea actuală a strategiilor de management al riscului securităţii cibernetice pentru IoT din organizaţiile incluse în sondaj faţă de modelul IoTSRM2.

Aşadar, în ceea ce priveşte rezultatele pentru toate organizaţiile din cadrul sondajului, în primul rând, acestea au relevat faptul că poziţiile "C-level executive and/or board member" (director la nivel C şi/sau membru al consiliului de administrație) şi "Consulting practice leader and/or principal" (lider şi/sau director al unei practici de consultanţă) sunt cele mai frecvente poziţii ale respondenţilor la sondaj pentru organizaţiile în cauză. În al doilea rând, aceste rezultate au relevat faptul că tipul de organizaţie numit „Large Organizations" (organizaţii mari) este cel mai frecvent tip de organizaţie pentru organizaţiile în cauză din cadrul sondajului. În al treilea rând, aceste rezultate au relevat faptul că sectorul „Technology, Media, & Telecom (TMT)" este cel mai frecvent sector industrial pentru organizaţiile în cauză din cadrul sondajului. În al patrulea rând, aceste rezultate au relevat faptul că regiunea „North/South America" (America de Nord/Sud) este cea mai frecventă regiune în care îşi au sediul organizaţiile în cauză din cadrul sondajului. În al cincilea rând, cu privire la tendinţa globală a strategiilor de management al riscului securităţii cibernetice pentru IoT ale organizaţiilor din cadrul sondajului faţă de modelul IoTSRM2, aceste rezultate au relevat faptul că 18 controale şi întrebări legate de modelul IoTSRM2 corespund grupului de opţiuni de răspuns „No, to a certain and great extent", iar celelalte 12 controale şi întrebări legate de modelul IoTSRM2 corespund grupului de opţiuni de răspuns "Yes, to a certain and great extent" (a se vedea Figura 6.4). De exemplu, aceste rezultate au sugerat, printre altele, faptul că majoritatea organizaţiilor se descurcă cel mai bine când vine vorba despre controlul denumit „Resiliency requirements" (cerinţe de rezilienţă) şi se descurcă cel mai rău când vine vorba despre controalele denumite „IoT security training and awareness plan" (planul pentru formare şi conştientizare în domeniul securităţii cibernetice pentru IoT) and „IoT End-of-Life plan" (planul pentru IoT la sfârşitul ciclului de viaţă).

Tot legat de rezultatele pentru toate organizaţiile din cadrul sondajului, cu privire la media totală a scorului de conformitate cu modelul IoTSRM2 al organizaţiilor din cadrul sondajului pentru fiecare control al modelului IoTSRM2 în parte, rezultatele au arătat faptul că scorul mediu total de conformitate cu modelul IoTSRM2 mai mic decât 50% corespunde la 19 controale ale modelului IoTSRM2 şi că scorul mediu total de conformitate cu modelul IoTSRM2 mai mare sau egal cu 50% corespunde la 11 controale ale modelului IoTSRM2 (a se vedea Figura 6.5). De exemplu, rezultatele au arătat, printre altele, faptul că majoritatea organizaţiilor se descurcă cel mai bine când vine vorba despre controlul denumit „Resiliency requirements" şi se descurcă cel mai rău când vine vorba despre controalele denumite "IoT security training and awareness plan" şi "IoT supplier contract management plan" (planul pentru gestionarea contractelor cu furnizorii de IoT).

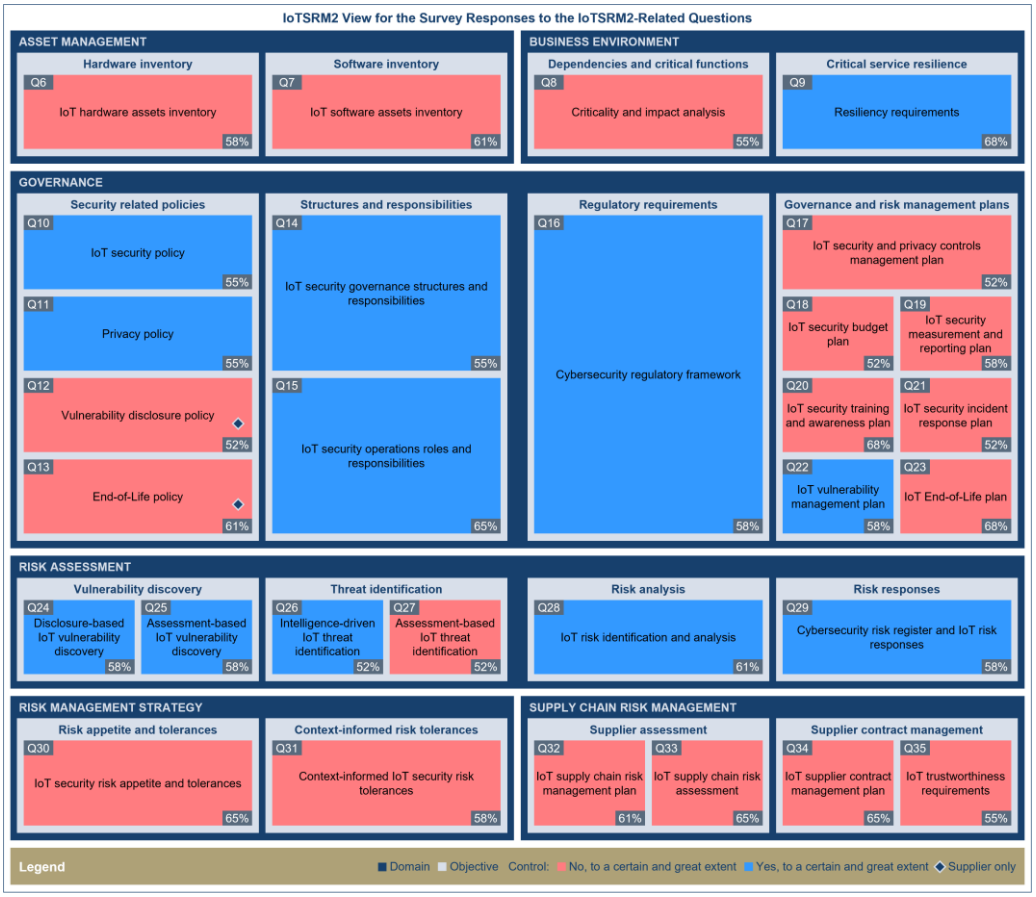

Figure 6.4. Privire de ansamblu bazată pe IoTSRM2 a răspunsurilor la sondaj [Pop+21b]

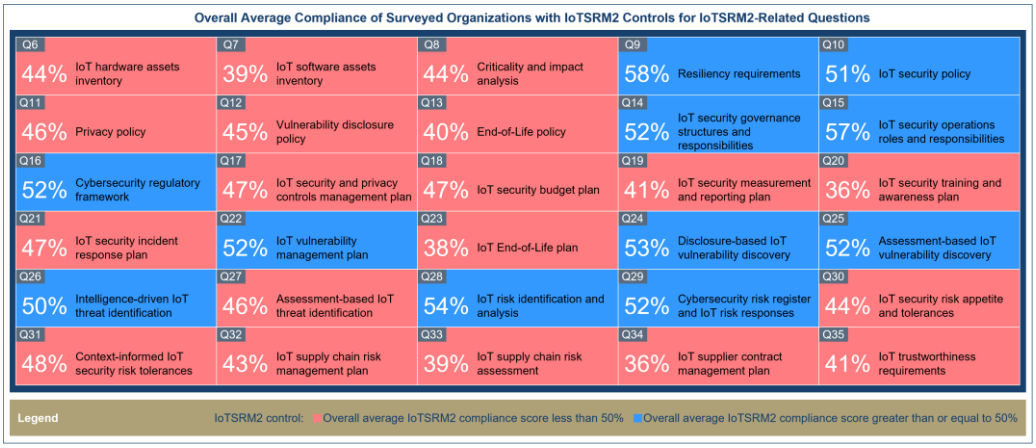

Figura 6.5. Media totală de conformitate cu controalele IoTSRM2 bazată pe răspunsurile la sondaj [Pop+21b]

Cu privire la scorul de conformitate cu modelul IoTSRM2 al fiecăreia dintre aceste organizaţii din cadrul sondajului, rezultatele sondajului arată că scorul de conformitate cu modelul IoTSRM2 mai mic decât 50% corespunde la 19 organizaţii din cadrul sondajului şi scorul de conformitate cu modelul IoTSRM2 mai mare sau egal cu 50% corespunde la 12 organizaţii din cadrul sondajului (a se vedea Figura 6.6). De exemplu, aceste rezultate arată, printre altele, faptul că primele trei scoruri de conformitate cu modelul IoTSRM2 corespund la organizaţiile de tip „Large Organizations” (excepţie făcând una dintre ele) şi ultimele trei scoruri de conformitate cu modelul IoTSRM2 corespund la organizaţiile de tip „Small-Medium Organizations” (organizaţii mici şi mijlocii).

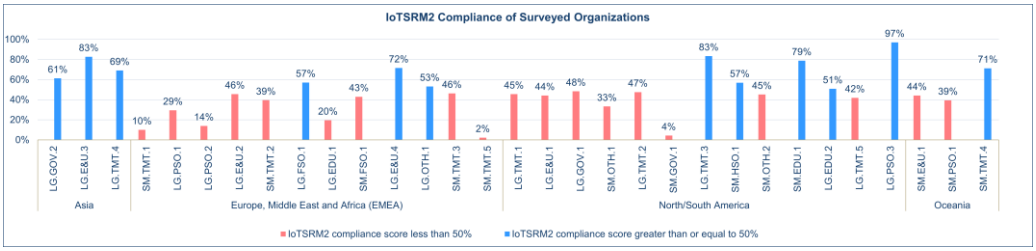

Figura 6.6. Conformitatea cu modelul IoTSRM2 a organizaţiilor din cadrul sondajului [Pop+21b]

În plus, în ceea ce priveşte rezultatele pentru organizaţiile mari din cadrul sondajului, în primul rând, aceste rezultate au relevat faptul că poziţia "Consulting practice leader and/or principal" este cea mai frecventă poziţie a respondenţilor la sondaj pentru organizaţiile în cauză. În al doilea rând, aceste rezultate au relevat faptul că sectorul „Technology, Media, & Telecom (TMT)" este cel mai frecvent sector industrial pentru organizaţiile mari din cadrul sondajului. În al treilea rând, aceste rezultate au relevat faptul că regiunea „North/South America" este cea mai frecventă regiune în care îşi au sediul organizaţiile mari din cadrul sondajului. În al patrulea rând, cu privire la media totală a scorului de conformitate cu modelul IoTSRM2 al acestor organizaţii din cadrul sondajului pentru fiecare control al modelului IoTSRM2 în parte, rezultatele au arătat faptul că scorul mediu total de conformitate cu modelul IoTSRM2 mai mic decât 50% corespunde la 10 controale ale modelului IoTSRM2 şi că scorul mediu total de conformitate cu modelul IoTSRM2 mai mare sau egal cu 50% corespunde la 20 controale ale modelului IoTSRM2 (a se vedea Figura 6.7). De exemplu, rezultatele au arătat, printre altele, faptul că majoritatea organizaţiilor se descurcă cel mai bine când vine vorba despre controlul denumit „Resiliency requirements" şi se descurcă cel mai rău când vine vorba despre controlul denumit „IoT software assets inventory" (gestionarea inventarului activelor de software IoT).

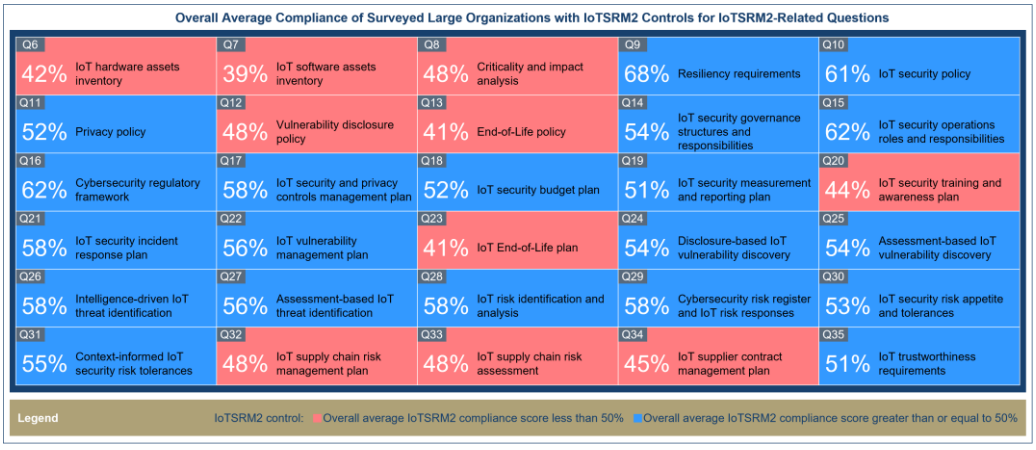

Figura 6.7. Media totală de conformitate cu controalele IoTSRM2 bazată pe răspunsurile la sondaj corespunzătoare organizaţiilor mari [Pop+21b]

Mai mult, în ceea ce priveşte rezultatele pentru organizaţiile mari din sectorul TMT din cadrul sondajului, în primul rând, acestea au relevat faptul că poziţiile "C-level executive and/or board member" şi "Consulting practice leader and/or principal" sunt cele mai frecvente poziţii ale respondenţilor la sondaj pentru organizaţiile în cauză. În al doilea rând, aceste rezultate au relevat faptul că regiunea „North/South America" este cea mai frecventă regiune în care îşi au sediul organizaţiile mari din sectorul TMT inclused în sondaj. În al treilea rând, cu privire la media totală a scorului de conformitate cu modelul IoTSRM2 al acestor organizaţii din cadrul sondajului pentru fiecare control al modelului IoTSRM2 în parte, rezultatele au arătat faptul că scorul mediu total de conformitate cu modelul IoTSRM2 mai mic decât 50% corespunde la 9 controale ale modelului IoTSRM2 şi că scorul mediu total de conformitate cu modelul IoTSRM2 mai mare sau egal cu 50% corespunde la 21 controale ale modelului IoTSRM2 (a se vedea Figura 6.8). De exemplu, rezultatele au arătat, printre altele, faptul că majoritatea organizaţiilor se descurcă cel mai bine când vine vorba despre controlul denumit „IoT security policy" (politica de securitate cibernetică pentru IoT) şi se descurcă cel mai rău când vine vorba despre controlul denumit „Criticality and impact analysis" (analiza importanţei şi a impactului).

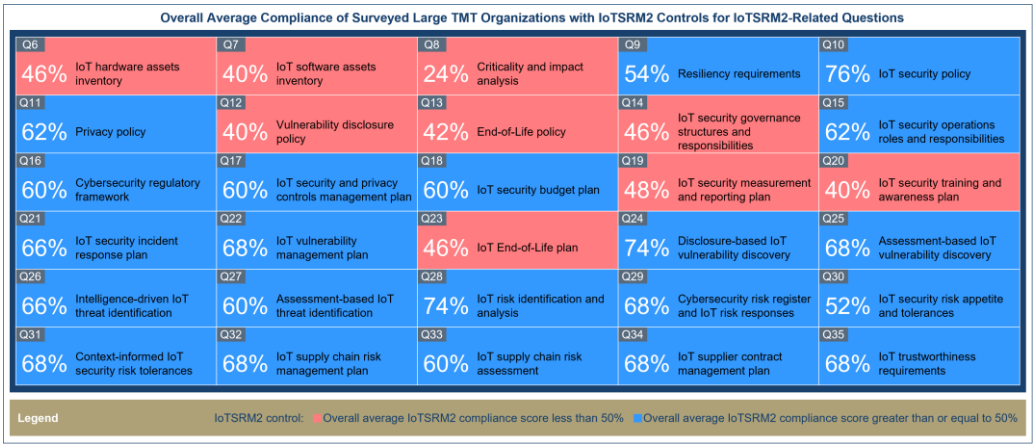

Figura 6.8. Media totală de conformitate cu controalele IoTSRM2 bazată pe răspunsurile la sondaj corespunzătoare organizaţiilor mari din sectorul TMT [Pop+21b]

În continuare, **Capitolul 6.4** descrie lucrările conexe. În primul rând, capitolul subliniază lipsa lucrărilor de cercetare care să se axeze pe determinarea stadiului actual al strategiilor de management al riscului securităţii cibernetice pentru IoT din organizaţii. În al doilea rând, acesta oferă cele 12 lucrări conexe care au fost selectate pe baza a trei criterii de selecţie şi a unei condiţii, şi anume să fie lucrări de cercetare în limba engleză bazate pe interviuri, sondaje, sau experimente atât din mediul academic, cât şi din industrie, care abordează cel puţin într-o anumită măsură strategia de management al riscului securităţii cibernetice pentru IoT din organizaţii. În al treilea rând, capitolul discută studiul de sondaj bazat pe modelul IoTSRM2 şi cele 12 lucrări conexe selectate pe baza a şapte criterii de evaluare şi trei tipuri de aplicabilitate pentru fiecare criteriu de evaluare (şi anume criteriul de evaluare se aplică pe deplin, criteriul de evaluare se aplică într-o anumită masură, şi criteriul de evaluare nu se aplică). Astfel, legat de criteriul de evaluare E1, şi anume „The research study is focused on determining the current state of IoT security risk management strategies in organizations" (studiul de cercetare se axează pe determinarea stadiului actual al strategiilor de management al riscului securităţii cibernetice pentru IoT în organizaţii), acesta se aplică pe deplin la studiul de sondaj bazat pe modelul IoTSRM2 şi se aplică într-o anumită măsură la toate cele 12 lucrări conexe selectate. Legat de criteriul de evaluare E2, şi anume „The methodology for achieving the intended purpose of the research study is clearly described" (metodologia pentru realizarea scopului urmărit de studiul de cercetare este descrisă în mod clar), acesta se aplică pe deplin la o lucrare conexă şi la studiul de sondaj bazat pe modelul IoTSRM2 şi se aplică într-o anumită masură la cinci lucrări conexe. Legat de criteriul de evaluare E3, şi anume „The underlying design best practice of the research method of the methodology, is clearly documented" (buna practică care stă la baza metodei de cercetare a metodologiei este descrisă în mod clar), acesta se aplică pe deplin la studiul de sondaj bazat pe modelul IoTSRM2 şi se aplică într-o anumită masură la o lucrăre conexă. Legat de criteriul de evaluare E4, şi anume „Provides results for organizations of a specific organization size" (oferă rezultate pentru organizaţii de o anumită dimensiune), acesta se aplică pe deplin la trei lucrări conexe şi la studiul de sondaj bazat pe modelul IoTSRM2 şi nu se aplică la celelalte lucrări conexe. Legat de criteriul de evaluare E5, şi anume „Provides results for organizations from a specific industry sector" (oferă rezultate pentru organizaţii dintr-un sector anume de activitate), acesta se aplică pe deplin la patru lucrări conexe şi la studiul de sondaj bazat pe modelul IoTSRM2 şi nu se aplică la celelalte lucrări conexe. Legat de criteriul de evaluare E6, şi anume „The results reveal the level of compliance of each subject with a reference model" (rezultatele arată nivelul de conformitate a fiecărui subiect abordat cu un model de referinţă), acesta se aplică pe deplin la studiul de sondaj bazat pe modelul IoTSRM2 şi se aplică într-o anumită masură la o lucrăre conexă. În sfârşit, legat de criteriul de evaluare E7, şi anume „The findings resemble the results of the IoTSRM2-based survey" (concluziile se aseamănă cu rezultatele sondajului bazat pe modelul IoTSRM2), acesta se aplică pe deplin la studiul de sondaj bazat pe modelul IoTSRM2 şi se aplică într-o anumită masură la opt din cele 12 lucrări conexe selectate.

Capitolul 7. Concluzii Finale

Capitolul 7 a prezentat concluziile finale ale tezei, contribuţiile aduse, şi posibilele direcţii de dezvoltare. Astfel, teza prezintă mai multe contribuţii care sunt grupate în trei categorii: contribuţii teoretice, contribuţii teoretice cu aplicabilitate în practică, şi contribuţii practice.

În primul rând, **contribuţiile teoretice** revendicate sunt următoarele:

- Definirea termenilor de „standard”, „metodă”, şi „metodologie” în vederea stabilirii distincţiei între aceşti termeni;
- Definirea termenului de „cybersecurity risk management framework” (cadru de management al riscului de securitate cibernetică) pentru a permite o înţelegere comună a acestui termen;
- Elaborarea unei taxonomii ierarhice noi care clasifică bunele practici de securitate cibernetică pentru internetul obiectelor (IoT) în funcţie de aplicabilitatea acestora la anumite grupuri de public ţintă şi de aplicabilitatea acestora la anumite tipuri de bune practici;
- Compararea metodei propuse de „rating” (clasificare) a ameninţărilor cibernetice cu lucrările conexe;
- Analizarea lucrărilor conexe relevante pentru evaluarea legilor şi reglementărilor de securitate cibernetică;
- Analizarea lucrărilor conexe relevante pentru evaluarea cadrelor de management al riscului de securitate cibernetică, care a studiat în profunzime studiile anterioare având un domeniu de aplicare mai restrâns sau parţial diferit;
- Analizarea comparativă a lucrărilor conexe modelului de referinţă propus pe baza unui set propus de criterii de evaluare;
- Analizarea comparativă a lucrărilor conexe studiului de sondaj bazat pe modelul IoTSRM2 în funcţie de un set propus de criterii de evaluare.

În al doilea rând, **contribuţiile teoretice cu aplicabilitate în practică** revendicate sunt următoarele:

- Identificarea, categorisirea, şi descrierea standardelor şi metodologiilor relevante pentru managementul securităţii cibernetice pe baza studiului literaturii de specialitate;
- Determinarea şi categorisirea ameninţărilor cibernetice curente în 13 categorii de ameninţări cibernetice actuale împreună cu descrierea acestora pe baza unei cercetări a 17 surse pertinente şi renumite;
- Prezentarea unei imagini de ansamblu a legilor şi reglementărilor privind securitatea cibernetică legate de două domenii ale acestora din trei jurisdicţii separate;
- Identificarea, categorisirea, şi descrierea cadrelor relevante pentru managementul riscului de securitate cibernetică pe baza studiului literaturii de specialitate;
- Identificarea, clasificarea, şi descrierea bunelor practici de securitate cibernetică pentru IoT pe baza studiului literaturii de specialitate şi pe baza taxonomiei ierarhice propuse;
- Proiectarea unei metode noi de „rating” (clasificare) a ameninţărilor cibernetice şi dezvoltarea unui instrument de „rating” (clasificare) a ameninţărilor;
- Proiectarea unei metode noi pentru evaluarea unor legi şi reglementări esenţiale selectate privind securitatea cibernetică;
- Proiectarea unei metodologii în trei etape care implică identificarea, analiza, şi compararea cadrelor de management al riscului de securitate cibernetică din sfera de aplicare a metodologiei propuse pentru evaluarea cadrelor;
- Elaborarea unei structuri ierarhice pentru evaluarea cadrelor de management al riscului de securitate cibernetică din sfera de aplicare a metodologiei propuse pentru evaluarea cadrelor, care cuprinde şapte dimensiuni şi 13 criterii de evaluare;
- Definirea a şase valori lingvistice în vederea clasificării („rating”) cadrelor de management al riscului de securitate cibernetică din sfera de aplicare a metodologiei propuse pentru evaluarea cadrelor, faţă de criteriile de evaluare;
- Proiectarea unei metodologii pentru dezvoltarea modelului de referinţă pentru strategia de management al riscului securităţii cibernetice pentru IoT pe baza bunelor practici;

- Proiectarea unei metodologii pentru determinarea stadiului actual al strategiilor de management al riscului securităţii cibernetice pentru IoT din organizaţiile din cadrul sondajului faţă de modelul IoTSRM2.

În al treilea rând, **contribuţiile practice** revendicate sunt următoarele:

- Aplicarea metodei propuse de „rating" (clasificare) a ameninţărilor cibernetice la 13 categorii de ameninţări cibernetice în vederea evaluării acestora;
- Evaluarea critică a celor 13 categorii de ameninţări cibernetice în funcţie de gradele posibile de aplicabilitate la un anumit tip de „cyber harm" (prejudiciu cibernetic);
- Evaluarea critică a legilor şi reglementărilor de securitate cibernetică din sfera de aplicare a metodei propuse pentru evaluarea legislaţiilor în vederea stabilirii punctelor comune între acestea din perspectiva înţelegerii organizaţionale în ceea ce priveşte gestionarea riscului de securitate cibernetică;
- Evaluarea critică a opt cadre de management al riscului de securitate cibernetică pe baza metodologiei propuse pentru evaluarea cadrelor;
- Dezvoltarea modelului de referinţă pentru strategia de management al riscului securităţii cibernetice pentru IoT pe baza metodologiei propuse;
- Evaluarea critică a unor referinţe informative selectate ale modelului IoTSRM2 pe baza legăturii lor cu modelul de referinţă propus;
- Conceperea, crearea, testarea, şi distribuirea sondajului bazat pe modelul IoTSRM2 pe baza metodologiei propuse;
- Determinarea stadiului actual al strategiilor de management al riscului securităţii cibernetice pentru IoT din organizaţiile din cadrul sondajului faţă de modelul IoTSRM2 prin analizarea răspunsurilor la sondaj şi prin raportarea rezultatelor sondajului bazat pe modelul IoTSRM2.

Bibliografie Selectivă

[Age20a] AgeLight LLC. (2020a). *IoT Safety Architecture & Risk Toolkit, version 4.0*. AgeLight LLC. Retrieved February 23, 2021, from https://www.agelight.com/iot

[Agr+18] Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), 1–15. https://doi.org/10.1093/cybsec/tyy006

[ATK18] A.T. Kearney. (2018). *Rising to the Challenge 2018 Views from the C-Suite An Annual Survey of Global Business Executives*. A.T. Kearney, Inc. Retrieved October 3, 2020, from https://www.kearney.com/web/global-business-policy-council/article?/a/2018-views-from-the-c-suite

[CSA19a] CSA. (2019a). *CSA IoT Security Controls Framework*. Cloud Security Alliance. Retrieved May 06, 2020, from https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework/

[Dil+99] Dillman, D.A., Tortora, R., & Bowker, D. (1999). *Principles for constructing Web surveys*. Pullman: Washington State University, Social and Economic Sciences Research Center.

[ENI18b] ENISA. (2018b). *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*. The European Union Agency for Cybersecurity. Retrieved July 20, 2020, from https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

[ENI20a] ENISA. (2020a). *Procurement Guidelines for Cybersecurity in Hospitals Good practices for the security of Healthcare services*. The European Union Agency for Cybersecurity. Retrieved January 05, 2021, from https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

[Giu+21] Giuca, O., **Popescu, T.M**., Popescu, A.M., Prostean, G., & Popescu, D.E. (2021). A Survey of Cybersecurity Risk Management Frameworks. In V. Balas, L. Jain, M. Balas & S. Shahbazova (Eds.), *Soft Computing Applications. SOFA 2018. Advances in Intelligent Systems and Computing* (Vol. 1221, pp. 240-272). Cham: Springer. https://doi.org/10.1007/978-3-030-51992-6_20

[IoT16] IoTAC, (2016), 'IoT Security Guidelines Ver. 1.0,' [Online], *Japan's IoT Acceleration Consortium*, [Retrieved August 13, 2020], Available: http://www.iotac.jp/wp-content/uploads/2016/01/IoT-Security-Guidelines_ver.1.0.pdf

[IoT20a] IoTSF. (2020a). *IoT Security Compliance Framework Release 2.1*. IoT Security Foundation. Retrieved July 20, 2020, from https://www.iotsecurityfoundation.org/best-practice-guidelines/

[ITU12] ITU-T. (2012). *Overview of the Internet of Things*. ITU Telecommunication Standardization Sector. Retrieved September 05, 2021, from https://www.itu.int/rec/T-REC-Y.2060-201206-I/en

[ITU17] ITU. (2017). *Global Cybersecurity Index (GCI) 2017*. ITU. Retrieved November 19, 2018, from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[Nat17] National Academy of Engineering. (2017). *NAE GRAND CHALLENGES FOR ENGINEERING*. National Academy of Engineering. Retrieved May 28, 2019, from http://www.engineeringchallenges.org/challenges/11574.aspx

[NIS18a] NIST. (2018a). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. National Institute of Standards and Technology. Retrieved February 10, 2019, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[NIS20a] NIST. (2020a). *Foundational Cybersecurity Activities for IoT Device Manufacturers*. National Institute of Standards and Technology. Retrieved January 07, 2021, from https://doi.org/10.6028/NIST.IR.8259

[Pop+19a] **Popescu, T.M.**, Popescu, A.M., Prostean, G., & Popescu, D.E. (2019a). Evaluation of legislations from the perspective of organizational understanding to managing cybersecurity risk. In K.S. Soliman (Eds.) *Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020* (pp. 4677-4689). ISBN: 978-0-9998551-2-6.

[Pop+19b] **Popescu, T.M.**, Popescu, A.M., Prostean, G., & Popescu, D.E. (2019b). Cybersecurity Threat Rating Method Based on Potential Cyber Harm', In: Soliman K. S. (Eds.) *Proceedings of the 34th International Business Information Management Association Conference (IBIMA). Vision 2025: Education Excellence and Management of Innovations through Sustainable Economic Competitive Advantage* (pp. 5909- 5920). ISBN: 978-0-9998551-3-3.

[Pop20] **Popescu, T.M.** (2020). *Cybersecurity Risk Management* (Ph.D. Report 1). Politehnica University of Timisoara, Timisoara, Romania.

[Pop21] **Popescu, T.M.** (2021). *IoT Security Risk Management* Strategy (Ph.D. Report 2). Politehnica University of Timisoara, Timisoara, Romania.

[Pop+21a] **Popescu, T.M.**, Popescu, A.M., & Prostean, G. (2021a). IoT Security Risk Management Strategy Reference Model (IoTSRM2). *Future Internet*, *13* (6), 148. https://doi.org/10.3390/fi13060148

[Pop+21b] **Popescu, T.M.**, Popescu, A.M., & Prostean, G. (2021b). Leaders' Perspectives on IoT Security Risk Management Strategies in Surveyed Organizations Relative to IoTSRM2. Applied Sciences, 11 (19), 9206. https://doi.org/10.3390/app11199206