



Cuprins

Cuvânt-înainte	5
1. Introducere	9
2. Managementul riscului	13
3. Managementul riscului pentru sisteme informatice	18
3.1. Securitatea Informației.....	19
3.2. Metodă eficientă de protecție a datelor – Abordarea managementului securității prin managementul riscurilor	23
3.3. Construirea unui program de măsurare a performanțelor în securitatea informației.....	67
4. Metode și standarde internaționale pentru managementul riscurilor	74
5. Managementul riscurilor IT	80
5.1. Procesul de management al riscurilor IT.....	81
5.2. Analiza de Risc	99
5.2.1. Etapele analizei de risc.....	100
5.2.2. Analiza Modurilor de Defectare și a Efectelor lor (AMDE) – (Failure Mode and Effects Analysis – FMEA)	104
5.3. Aspecte specifice privind protecția datelor personale în contextul identificării și evaluării riscului	116
5.3.1. Conceptul de ‘date personale’	119
5.3.2. Stadiile supuse analizei de risc	123
5.3.3. Tipologii de prelucrare esențiale de analizat.....	125
5.3.4. Aspecte de analizat pentru orice flux de date.....	129
5.3.5. Metodologie pentru realizarea analizei de risc (DPIA) și identificarea interesului legitim	148
5.4. Răspunsul la risc.....	154
5.4.1. Tipurile de răspuns la risc	155
5.4.2. Integrarea aspectelor de protecție a datelor în procesele existente de răspuns la risc	158
5.4.3. Corelarea răspunsului la risc între cerințele de protecție a datelor personale și cele de securitate IT	160
5.4.4. Asigurarea unor abordări unitare în cadrul grupului	162
5.5. Monitorizarea riscurilor și a răspunsului la riscuri.....	163
5.6. Implementarea controalelor în sistemele informatice.....	167

5.7. Integrarea procesului de management al riscurilor în procesele IT	177
5.7.1. Modelul de management prin procese și adoptarea managementului de risc în IT	177
5.7.2. Îndeplinirea obligațiilor de răspuns la solicitările persoanelor vizate și a obligațiilor referitoare la investigații (pentru protecția datelor personale)	181
5.7.3. Analiza transferului datelor personale în contextul mai multor sisteme IT interne și/sau externe	181
5.7.4. Integrarea protecției datelor în procesul de dezvoltare software.....	182
5.8. Riscuri specifice în cazul utilizării unei organizații terțe.....	189
6. Registrul Riscurilor	194
7. Rolul liniilor de apărare într-o organizație și asigurarea conformității	203
7.1. Rolul liniilor de apărare într-o organizație	203
7.1.1. Prima Linie de Apărare – Managementul Operațional	206
7.1.2. A doua linie de apărare – Funcțiile de conformitate și managementul riscurilor	207
7.1.3. A treia linie de apărare – Auditul intern	208
7.1.4. Liniile de apărare pentru protecția datelor personale	209
7.2. Asigurarea conformității	210
8. Standarde minime de risc informatic aliniate cu strategia afacerii și cu apetitul definit pentru risc	216
9. Factorul uman.....	222
10. Reziliența – Strategii împotriva evenimentelor necunoscute sau cu un nivel ridicat de incertitudine	230
11. Concluzii.....	234
12. Termeni, definiții	236
Bibliografie selectivă	240



1. Introducere

Societatea noastră a trecut în ultimele decade printr-un proces de dezvoltare foarte dinamic, resimțit în toate aspectele vieții, iar un rezultat direct al acestei dezvoltări a fost evoluția tehnologiei. Drept consecință, se produce o schimbare a modalității de comunicare/transmitere a datelor în interiorul și în afara organizației – noțiunea de distanță a fost anulată.

Pentru a realiza această adaptare continuă la condițiile de piață, soluțiile IT și procesele din cadrul organizației devin mai complexe și necesită ajustări frecvente. În plus, diversitatea pericolelor care amenință datele și buna funcționare a mediului nostru de afaceri ne obligă să punem în practică metode și tehnici de protecție și contracarare a eventualelor atacuri. Odată cu creșterea complexității metodelor de protecție, devine din ce în ce mai greu să gestionăm mediul nostru operațional și atunci este necesară o abordare unitară.

La această evoluție se adaugă și rigori sporite din perspectiva legislației pentru a proteja aspectele ce țin de protecția consumatorilor, protecția datelor, stabilitatea segmentului de piață în care organizația își desfășoară activitatea. Pentru sectorul financiar-bancar, aceste schimbări tehnologice au adus modificări semnificative în ceea ce privește abordarea pe piață, procesele interne și legislația aplicabilă, fiind introduse recent o serie de obligații suplimentare, în special în ceea ce privește protecția datelor și a sistemele informatice.

Având în vedere aceste schimbări frecvente, organizațiile trebuie să aibă implementate metodologii de analiză a riscului (pentru a prioritiza ordinea în care vor fi abordate riscurile) și procese interne ce acoperă toate etapele ciclului de management al riscului. Concomitent, cerințele legislative și ale organismelor de reglementare trebuie respectate și, prin urmare, este necesar să fie implementate și integrate cu procesele organizației.

Pentru a armoniza și integra analiza și managementul riscurilor cu cerințele și practicile autorităților locale în domeniul financiar-bancar, este necesară o metodologie de creare, monitorizare și eficientizare a proceselor legate de riscuri.

Această carte vine în întâmpinarea tuturor acestor necesități ale organizațiilor, prezentând un set cât mai complet și actual de informații ce vor ajuta la identificarea, evaluarea și monitorizarea riscurilor, precum și la dezvoltarea unor controale adresate acestora. Integrarea riscului IT în procesul general de management al riscului este un alt aspect important ce va fi tratat pe parcursul lucrării, oferind astfel informații importante ce fac posibilă o implementare eficientă.

Corelat cu riscul IT, vom prezenta și managementul riscurilor din perspectiva protecției datelor personale, atât în cazul unor proiecte noi (privacy by design), cât și în cazul modificării proiectelor existente sau monitorizării activității de prelucrare existentă. Abordarea managementului riscului va include toate etapele relevante, de la identificare, evaluare, remediere până la monitorizare, concentrându-se asupra mecanismelor de cooperare și proceselor ce pot fi stabilite în interiorul și în exteriorul organizației. Scopul este de a identifica în totalitate riscurile și a minimiza impactul acestora.

Vom exemplifica situații frecvent întâlnite în practică pentru riscurile IT și riscurile privind datele personale, pentru a evidenția pașii ce pot fi urmați în stabilirea unor procese clare pentru adaptarea la noile cerințe legale.

Pentru a completa întreaga suită de noțiuni necesare unei organizații în vederea unui management de risc eficient, am prezentat aspecte legate de factorul uman și rolul determinant al acestuia în toate activitățile organizației, inclusiv a celor de management al riscului, precum și cu privire la măsurile care ar trebui luate în vederea creșterii rezilienței organizației.

În afară de legislația existentă, au fost introduse norme noi pentru a reglementa aspectele legate de schimbările tehnologice referitoare la: utilizarea soluțiilor de cloud computing (ghidurile EBA¹ referitoare la cloud computing², Cloud Act adoptat în Statele Unite ale Americii³), securitatea informatică (Directiva NIS adoptată de UE⁴), serviciile oferite la distanță (Directiva serviciilor de plată, dispoziții legate de securitatea serviciilor de tip internet-banking).

Specific pentru aspectele legate de risc, în contextul reglementărilor legale în vigoare, Autoritatea de Supraveghere Financiară a stabilit în 2015 un set de cerințe minimale obligatorii elaborat sub denumirea de Norma⁵ nr. 6/2015 privind gestionarea riscurilor operaționale generate de sistemele informatice. Ulterior, a fost modificată și îmbunătățită prin Norma nr. 4/2018⁶. Norma stabilește procese și indicatori pentru evaluarea, supravegherea și controlul riscurilor operaționale IT.

Strâns legat de riscurile operaționale privind sistemele informatice, trebuie avute în vedere și riscurile privind prelucrarea datelor personale. Aceste două tipuri de riscuri sunt corelate într-o anumită măsură, în special în aspecte ce țin de

¹ European Banking Authority.

² EBA/REC/2017/03, „Recommendations on outsourcing to cloud service providers”.

³ The Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943) <https://www.congress.gov/bill/115th-congress/house-bill/4943/text>, accesat la data de 4 octombrie 2019.

⁴ Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune.

⁵ Norma nr. 6/2015 privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entitățile reglementate, autorizate/avizate și/sau supravegheate de ASF și Ghidul de îndrumare aferent.

⁶ Norma nr. 4/2018 privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entitățile autorizate/avizate/înregistrate, reglementate și/sau supravegheate de către Autoritatea de Supraveghere Financiară.

confidențialitatea, integritatea și disponibilitatea datelor, precum și în ceea ce privește administrarea accesului la date și implicarea altor societăți (de exemplu, sub-contractanți, furnizori) în prelucrarea datelor.

Pentru aspectele legate de protecția datelor personale, prima legislație la nivel european a fost adoptată în 1995 prin Directiva 95/46/EC (fiind implementată în România în 2001 prin Legea nr. 677/2001). Desigur, pentru aspecte specifice a existat și există și altă legislație relevantă, cum ar fi Directiva 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice sau Convenția Consiliului Europei nr. 108 referitoare la protecția persoanelor fizice prin prisma procesării automate a datelor personale, ratificată de România în 2002.

De-a lungul timpului, au fost emise ghiduri pentru aspecte a căror interpretare unitară a fost necesară din cauza interpretărilor distincte puse în practică de către organizații. Relevant în acest sens, la nivel european Grupul de Lucru „Articolul 29” a emis diferite ghiduri pentru aspecte punctuale legate de protecția datelor personale⁷. De asemenea, au fost emise de către Grupul de Lucru „Articolul 29” și, apoi, de către EDPB⁸ ghiduri pentru aspecte specifice reglementate de GDPR.

În plus, relevante pentru conformitate cu legislația în domeniu sunt standardele menționate în Capitolul 4 al lucrării, care abordează în special realizarea unui cadru de conformitate cu prevederile privind protecția datelor.

La nivel european, pași recenti au fost făcuți în direcția standardizării, mai ales prin Regulamentul EU adoptat de curând cu privire la ENISA și certificarea securității informatice și a tehnologiilor de comunicare⁹. Această reglementare are relevanță și prin prisma administrării riscului, stabilind realizarea unui cadru pentru securitatea informatică a produselor, serviciilor și proceselor.

În România, pentru sectorul bancar, un cod de conduită pentru prelucrarea datelor personale este în discuție între entitățile din domeniu și Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal. Însă proiectul codului de conduită nu conține aspecte legate de identificarea, administrarea și reducerea riscurilor.

Astfel, din perspectiva conformității cu legislația în vigoare și luând în considerare situațiile practice din domeniu, ghidurile menționate mai sus reprezintă un punct de pornire pentru analiza riscurilor prin prisma protecției datelor personale.

Încă de la început trebuie menționat faptul că riscul nu presupune doar existența unor posibile amenințări, ci și a unor oportunități ce pot oferi un avantaj competitiv. Abilitatea de a identifica și de a distinge situațiile favorabile de cele potențial nefavorabile și de a acționa în concordanță este indispensabilă pentru supraviețuirea

⁷ Grupul de Lucru Articolul 29, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm, accesat la data 4 octombrie 2019.

⁸ European Data Protection Board.

⁹ Regulamentul (UE) 2019/881 privind ENISA și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor (Regulamentul privind securitatea cibernetică).

și dezvoltarea afacerii, fiind necesare mecanisme cu ajutorul cărora potențialele riscuri să fie identificate și să fie ținute sub control.

Indiferent de gradul de maturitate la care procesul de management al riscului a ajuns, acesta se poate dovedi foarte ineficient dacă nu se ține cont de un factor critic în tot acest tablou, și anume cel uman. Abordarea corectă și preventivă în această privință este la fel de importantă, iar experiența ne-a dovedit frecvent că măsurile de prevenire eficiente au drept consecință reducerea costurilor operaționale. Lucrarea va înfățișa aceste concepte precum și bunele practici ce pot fi adoptate pentru a obține un mediu controlabil.

Managementul organizației cu ajutorul unor procese clar definite, bazate pe bunele practici folosite de întreprinderi și instituții mature, este cel care face posibilă înțelegerea riscurilor și reducerea lor prin instaurarea controalelor potrivite. În lipsa acestora, este evident că misiunea reducerii riscurilor ar fi imposibilă. Operațiunile organizației, precum și implementarea schimbărilor necesare nu se pot realiza în absența unor procese potrivite cu obiectivele dorite.

Pentru a oferi un set complet de informații care să poată fi utilizate și să producă rezultate imediat, lucrarea își propune să prezinte câteva tehnici de bază privind optimizarea proceselor. Vom prezenta cunoștințele minime necesare pentru identificarea, definirea, implementarea, evaluarea și optimizarea fluxurilor de informații care constituie procesele operaționale. Acestea vor acoperi atât aspectele operaționale din organizație, cât și aspectele interacțiunii acestora cu persoanele fizice ale căror date personale sunt prelucrate (de exemplu, clienți), ori cu furnizori de servicii (de exemplu, sub-contractanți, producători).

Cititorul va avea la dispoziție informații cu ajutorul cărora să înțeleagă modul în care mai multe standarde și practici pot fi utilizate pentru a realiza din procesele și elementele de control implementate un ecosistem informatic orientat către performanță și cu posibilitatea de optimizare continuă, pentru a reduce cât mai mult nivelul riscului operațional.

În managementul riscurilor este crucial ca evaluarea riscurilor și identificarea eventualelor vulnerabilități să se realizeze în TOATE activitățile organizației. Doar astfel este posibilă luarea unor măsuri corecte care să ajute la menținerea sub control a riscurilor operaționale.



2. Managementul riscului

În contextul în care atât organizațiile cât și procesele pe care acestea le implementează sunt din ce în ce mai complexe, avem nevoie de un sistem de management cu ajutorul căruia să gestionăm riscurile organizației. Managementul riscului ne oferă posibilitatea de a echilibra balanța între riscuri și oportunități, însă pentru aceasta trebuie să fim capabili să integrăm această practică în toate activitățile și procesele noastre. Astfel, responsabilii cu implementarea procesului de management al riscului trebuie să aibă o participare activă și să se asigure că toate riscurile sunt identificate, evaluate, monitorizate și, unde este cazul, soluționate/remediate.

Managementul riscului ne vorbește, așa cum spuneam, despre echilibru și despre abilitatea de a pune în balanță riscurile și recompensele/beneficiile. Nu în ultimă instanță, managementul riscului presupune și identificarea oportunităților pe care organizațiile ar trebui să le ia în considerare și să le fructifice. Nu degeaba în limba chineză, limba unei civilizații ce a dăruit umanității un tezaur de neprețuit, semnul ce definește criza înseamnă atât oportunitate cât și risc.

A. Cum a început?

Studiul managementului riscului a început efectiv abia după cel de-al Doilea Război Mondial, deși subiectul a fost asociat de mult timp cu asigurările menite să protejeze indivizii și companiile împotriva accidentelor¹⁰. Rădăcinile acestui domeniu sunt legate de nașterea teoriei probabilităților. De mii de ani, de la apariția jocurilor de noroc, riscul i-a îngrijorat și în același timp i-a fascinat pe oameni. În secolul al XVI-lea, învățatul pluridisciplinar Gerolamo Cardano¹¹ definea șansa ca pe raportul dintre numărul de rezultate favorabile și numărul total de rezultate. În secolul al XVII-lea, matematicienii Fermat și Pascal deja corespundau despre doctrina probabilităților, iar peste mai puțin de un secol, în Japonia anulului 1730, este atestat primul contract tip „future” pe prețul orezului. În 1864, la Chicago găsim primele asemenea contracte pentru mai multe produse agricole, la 1900, Louis Bachelier publică lucrarea „*Théorie*

¹⁰ Georges Dionne, „Risk Management: History, Definition and Critique”, CIRRELT-2013-17. Interuniversity Research Centre on Enterprise Networks, Logistics and Transportation (CIRRELT) and Department of Finance, HEC Montréal, 3000, Côte-Sainte-Catherine, Montréal, Canada.

¹¹ Gerolamo Cardano – „Wikipedia, the free encyclopedia” https://en.wikipedia.org/wiki/Gerolamo_Cardano accesat la 7 august 2019.

de la spéculation". Din secolul al XX-lea, când *American Association of University Teachers of Insurance* publică primul număr din revista „The Journal of Risk and Insurance”, și până în zilele noastre, când reglementările legate de managementul riscului includ deja acordurile Basel și Solvency, această disciplină a căpătat din ce în ce mai multă importanță.

În secolul al XXI-lea se spune că „Datele sunt noul aur”, ceea ce face din managementul riscului informatic o preocupare vitală oricărei organizații.

B. Ce este managementul riscului?

Conform standardului ISO31000, riscul se definește ca „efectul incertitudinii asupra obiectivelor”. Această exprimare a apărut în anul 2009 și a schimbat modul de percepție asupra riscului. Dacă anterior conceptul de risc, definit ca „probabilitatea unei pierderi”, indica doar consecințele negative ale incertitudinii, odată cu noua definiție s-a adăugat și sensul unor consecințe pozitive. Obiectivele pot avea, bineînțeles, diferite dimensiuni – financiare, ce țin de respectarea normelor în vigoare, de siguranță, de protecția mediului sau de sănătate, și pot fi aplicate la diferite niveluri: la nivel strategic, la nivel organizațional, la nivel de proiect, produs sau chiar de proces.

În general, riscul este caracterizat ca fiind produsul dintre consecințele unui eveniment (impactul) și probabilitatea ca acel eveniment să se materializeze.

Astfel, avem:

$$R = P \times I$$

Unde:

R = risc

P = probabilitate

I = impact potențial

În mare, relația dintre risc, probabilitate și impact poate fi descrisă de graficul de mai jos:

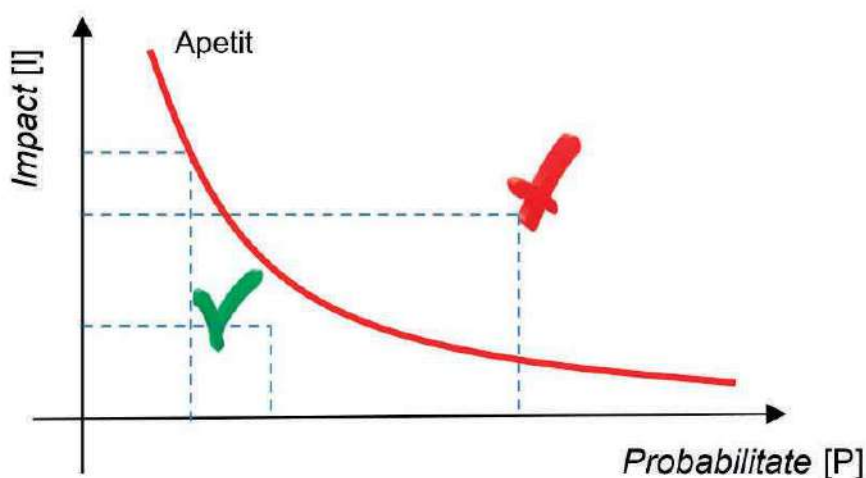


Figura 2.1. – Definiția riscului

Există o relație de directă proporționalitate între risc și impact și probabilitate – pe măsură ce impactul potențial și probabilitatea cresc, și riscul la care suntem expuși crește. Privind graficul de mai sus, se poate intui că pentru valori mari ale probabilității, ale impactului sau ale produsului lor, riscul depășește o valoare percepută drept limită acceptabilă. Această limită, reprezentată ca o curbă pe grafic, a fost numită „apetit” la risc. Este măsura în care cineva este dispus să își asume un anumit risc deoarece crede că merită și beneficiile așteptate depășesc eventualele consecințe negative, considerate relativ improbabile. Apetitul pentru risc va fi descris pe larg în capitolul dedicat. Într-o organizație, el trebuie definit în legătură cu standardele minime de risc informatic și cu strategia afacerii.

Pentru managementul riscului informatic, este utilă și o altă definiție, echivalentă, așa cum este prezentată de **NIST SP 800-30**. Riscul este o funcție de probabilitatea ca o amenințare să exploateze o vulnerabilitate și de impactul pe care acest eveniment l-ar avea asupra organizației. Această definiție se poate exprima și ca o proporționalitate directă, în următorul mod:

$$R = A \times V \times I$$

Unde:

R = risc

A = amenințarea

V = vulnerabilitatea

I = impactul potențial

C. Procesul de management al riscului

Putem privi procesul de management¹² al riscului ca fiind un cadru de lucru format din mai multe sub-procese sau etape pe care trebuie să le parcurgem continuu. Aceste sub-procese vor fi prezentate în detaliu în Capitolul 5, însă o introducere a imaginii de ansamblu este necesară pentru o mai bună înțelegere a contextului și a domeniului de aplicabilitate. **Figura 2.2.** prezintă imaginea de ansamblu a procesului de management al riscului.

¹² NIST Special Publication 800-30 – Guide for Conducting Risk Assessments.

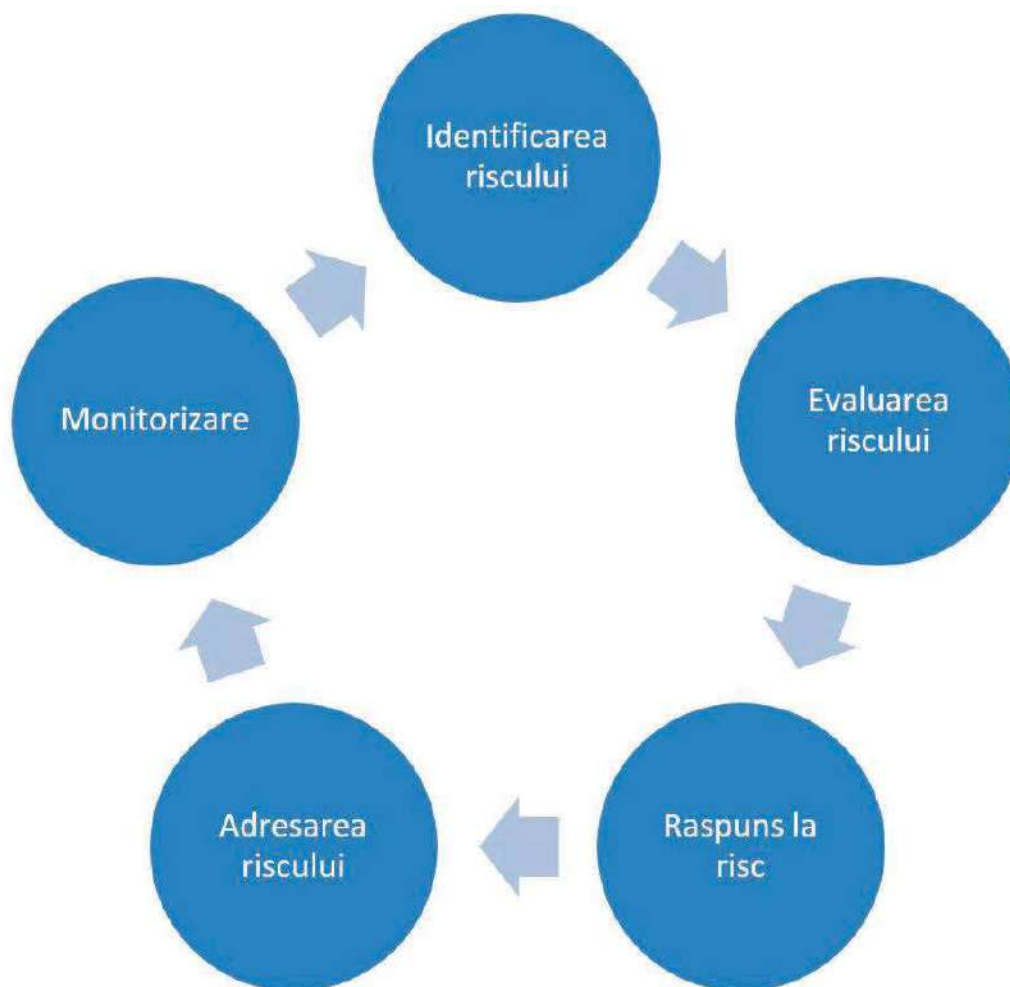


Figura 2.2. – Procesul de management al riscului

D. Tipuri de risc

Există mai multe metode de a împărți riscurile în categorii precum interne și externe (mai precis, endogene și exogene¹³), sau precum topuri ale celor mai importante x tipuri de risc care afectează o anumită industrie. Am ales categoriile principale de mai jos, considerându-le cele mai potrivite pentru studierea și încadrarea riscului informatic în industria financiară.

Riscul **strategic** se manifestă când strategia organizației devine ineficace, iar din această cauză afacerea are de suferit prin neatingerea obiectivelor. Cauzele din care acest risc poate să apară sunt multiple: intrarea pe piață a unui competitor nou și puternic, o tehnologie nouă, creșterea semnificativă a costului anumitor materiale etc.

Riscul de **conformitate** se referă la sistemul de reglementări din țara și din industria în care activează o organizație. Dacă nu sunt respectate, afacerea nu are viață

¹³ D. Anthony Miles, „Risk Factors and Business Models: Understanding the Five Forces of Entrepreneurial Risk and the Causes of Business Failure”, *Universal-Publishers*, (2011).

lungă. Chiar dacă la un moment dat firma se conformează tuturor legilor și regulilor în vigoare, acestea sunt supuse schimbării și există riscul apariției de noi reguli în viitor, cu care firma trebuie să se conformeze, alocând noi resurse și fonduri, în loc să le investească în schimbări care o avantajează. Se adaugă riscul de amenzi sau procese civile, care ridică miza chiar mai mult. Din perspectiva conformității cu dispozițiile legale, riscurile privind datele personale sunt reflectate în mare parte în riscul de conformitate.

Riscul **operațional** privește înspre activitățile de zi cu zi ale organizației, care și ele pot eșua sau produce erori. Ele pot fi cauzate de oameni, procese sau sisteme din interiorul firmei dar și de evenimente externe precum o pană de curent ori un dezastru natural. De cele mai multe ori riscul generat de tehnologia informației (sau riscul IT) este inclus în această categorie, dar nu ar trebui scăpate din vedere interdependențele cu toate celelalte categorii. Adesea, anumite riscuri legate de protecția datelor personale sunt incluse în această categorie.

Riscul de **image** (sau reputațional) poate fi rezultatul publicității negative, al unui produs defect ori al unui proces intentat firmei. Reputația bună se construiește într-un timp îndelungat dar se poate pierde într-o singură zi. Un exemplu frecvent, de răsunet și relevant pentru securitatea informației este o scurgere de date despre clienții firmei din cauza unui atac cibernetic. Aceasta poate genera o problemă mare de reputație, uneori chiar fatală afacerii.

Riscul **financiar** este legat și de celelalte categorii prin impactul costurilor sau al veniturilor compromise de acestea, dar se referă în special la fluxurile de bani care intră și ies din firmă, de exemplu, din perspectiva unei pierderi financiare bruște.

Vom reveni asupra interdependențelor dintre riscurile IT și categoriile de riscuri de mai sus în capitolele ulterioare, accentuând implicațiile asupra securității informației.



3. Managementul riscului pentru sisteme informatice

Managementul Riscului Informatic (MRI)¹⁴ poate fi definit ca ansamblul eforturilor depuse în vederea combaterii amenințărilor, a vulnerabilităților și a consecințelor datorate datelor neprotejate. Acest concept cuprinde managementul riscului în protecția datelor.

Pentru a simplifica lucrurile, vom folosi definițiile care urmează. **Informația**¹⁵ este componenta unui proces din activitatea organizației (flux de informații) susținut de tehnologie. Întreg ansamblul de procese din activitatea organizației, tehnologia pe care acesta se sprijină, roluri și responsabilități pentru transformarea informației (adică de realizarea activităților procesului) îl denumim **sistem informatic**¹⁶.

Atunci când sunt evaluate riscurile unui sistem informatic, analiza de risc pornește de la vulnerabilitățile acestuia. Sunt evaluate potențiale modalități de atac al sistemului informatic și, în cazul în care se observă că atacul ar putea avea succes, sunt luate măsurile necesare pentru a împiedica sau întârzia reușita acestuia. Dinamica incredibilă cu care noi tipuri de amenințări la adresa mediului nostru de activitate apar (aproape zilnic) ne obligă să luăm decizii din ce în ce mai dificile și fără vreun precedent pe a cărui similitudine să ne bazăm.

Evoluția tehnologiei și creșterea mobilității utilizatorilor determină ca delimitarea între viața profesională și cea personală să fie din ce în ce mai greu de realizat. În acest sens, este necesar să întreprindem acțiuni care să ia în seamă ambele perspective, atât cea profesională cât și cea personală, fără însă a le afecta independența. Suntem în situația unei schimbări de paradigmă privind securitatea informației și de aceea este necesar să avem o abordare holistică privind managementul riscului.

În acest context, avem nevoie de un sistem de lucru simplu și eficient care să ne asigure eficacitatea eforturilor de protecție a datelor. Practicile în acest domeniu ne

¹⁴ Managementul Riscului Informatic (MRI) – IT Risk – definiție – https://en.wikipedia.org/wiki/IT_risk; <http://www.opensecurityarchitecture.org/cms/definitions/it-risk>, accesat la 10 octombrie 2019.

¹⁵ Informație – definiție – <https://ro.wikipedia.org/wiki/Informa%C8%9Bie>, accesat la 10 octombrie 2019.

¹⁶ Sistem informatic – definiție – https://ro.wikipedia.org/wiki/Sistem_informatic, accesat la 10 octombrie 2019.

demonstrează că este necesar să stabilim principii solide pe care să se bazeze atât cadrul de lucru pentru managementul riscului (care se asigură de rafinarea continuă a procesului), cât și procesul de managementul riscului propriu-zis. Este necesară o abordare simplificată, fără a afecta însă eficacitatea metodelor și luând în calcul faptul că protecția datelor este componentă a managementului securității informației (acesta din urmă deținând cel mai complet și cel mai matur set de practici pentru protecția datelor). Astfel, vom construi în continuare un sistem de management pentru managementul riscului bazat pe bunele practici din managementul securității informației într-un mod eficient, robust, aliniat la standardele internaționale și în conformitate cu legislația în vigoare (GDPR sau Regulamentul UE 679/2016).

↳ 3.1. Securitatea Informației

Să începem prin a pune în evidență ce este securitatea informației, care sunt ariile sale de activitate și care sunt diferențele față de securitatea IT, cu care este adesea confundată.

Securitatea informației se ocupă cu protejarea informației și a sistemelor informatice de accesul neautorizat, folosirea, dezvăluirea, întreruperea, modificarea neautorizată sau distrugerea. Este o disciplină aplicabilă oricărui domeniu de activitate. *Securitatea informației poate fi obținută prin implementarea unui set adecvat de politici, practici, proceduri, structuri organizaționale, funcții, aplicații software și echipamente tehnice care, împreună, asigură atingerea obiectivelor de protecție a informației.*

Securitatea informației cuprinde arii de activitate precum:

- cadru de lucru pentru securitate (în engleză: *security framework*).
- dezvoltare de politici.
- campanii de conștientizare.
- dezvoltare de proceduri de securitate.
- continuitatea afacerii.
- sistemul de management al securității informației.
- analiza de risc.
- ghid de bune practici.
- confidențialitatea datelor.
- management în situații de criză.
- plan de securitate a informației.
- conformitate.
- implementare model de guvernare.
- și altele.