# 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 şi managementul riscurilor din perspectiva protecției datelor personale, atât în cazul unor proiecte noi (privacy by design), cât şi 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 şi proceselor ce pot fi stabilite în interiorul şi în exteriorul organizației. Scopul este de a identifica în totalitate riscurile şi a minimiza impactul acestora.

Vom exemplifica situații frecvent întâlnite în practică pentru riscurile IT şi riscurile privind datele personale, pentru a evidenția paşii 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 şi rolul determinant al acestuia în toate activitățile organizației, inclusiv a celor de management al riscului, precum şi cu privire la măsurile care ar trebui luate în vederea creşterii 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 EBA[1] referitoare la cloud computing[2], Cloud Act adoptat în Statele Unite ale Americii[3]), securitatea informatică (Directiva NIS adoptată de UE[4]), 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 Norma[5] nr. 6/2015 privind gestionarea riscurilor operaționale generate de sistemele informatice. Ulterior, a fost modificată şi îmbunătățită prin Norma nr. 4/2018[6]. Norma stabileşte procese şi indicatori pentru evaluarea, supravegherea şi controlul riscurilor operaționale IT.

Strâns legat de riscurile operaționale privind sistemele informatice, trebuie avute în vedere şi 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, „Recommandations 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 şi a sistemelor informatice în Uniune.

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

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

confidenţialitatea, integritatea şi disponibilitatea datelor, precum şi în ceea ce priveşte administrarea accesului la date şi implicarea altor societăţi (de exemplu, sub-contractanţi, furnizori) în prelucrarea datelor.

Pentru aspectele legate de protecţia datelor personale, prima legislaţie 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 şi există şi altă legislaţie relevantă, cum ar fi Directiva 2002/58/CE privind prelucrarea datelor personale şi protejarea confidenţialităţii în sectorul comunicaţiilor publice sau Convenţia Consiliului Europei nr. 108 referitoare la protecţia 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 organizaţii. Relevant în acest sens, la nivel european Grupul de Lucru „Articolul 29" a emis diferite ghiduri pentru aspecte punctuale legate de protecţia datelor personale [7]. De asemenea, au fost emise de către Grupul de Lucru „Articolul 29" şi, apoi, de către EDPB[8] ghiduri pentru aspecte specifice reglementate de GDPR.

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

La nivel european, paşi recenţi au fost făcuţi în direcţia standardizării, mai ales prin Regulamentul EU adoptat de curând cu privire la ENISA şi certificarea securităţii informatice şi a tehnologiilor de comunicare[9]. Această reglementare are relevanţă şi prin prisma administrării riscului, stabilind realizarea unui cadru pentru securitatea informatică a produselor, serviciilor şi proceselor.

În România, pentru sectorul bancar, un cod de conduită pentru prelucrarea datelor personale este în discuţie între entităţile din domeniu şi Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal. Însă proiectul codului de conduită nu conţine aspecte legate de identificarea, administrarea şi reducerea riscurilor.

Astfel, din perspectiva conformităţii cu legislaţia în vigoare şi luând în considerare situaţiile practice din domeniu, ghidurile menţionate mai sus reprezintă un punct de pornire pentru analiza riscurilor prin prisma protecţiei datelor personale.

Încă de la început trebuie menţionat faptul că riscul nu presupune doar existenţa unor posibile ameninţări, ci şi a unor oportunităţi ce pot oferi un avantaj competitiv. Abilitatea de a identifica şi de a distinge situaţiile favorabile de cele potenţial nefavorabile şi de a acţiona în concordanţă este indispensabilă pentru supravieţuirea

[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 şi privind certificarea securităţii cibernetice pentru tehnologia informaţiei şi comunicaţiilor (Regulamentul privind securitatea cibernetică).

şi dezvoltarea afacerii, fiind necesare mecanisme cu ajutorul cărora potenţialele riscuri să fie identificate şi să fie ţinute 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 ţine cont de un factor critic în tot acest tablou, şi anume cel uman. Abordarea corectă şi preventivă în această privinţă este la fel de importantă, iar experienţa ne-a dovedit frecvent că măsurile de prevenire eficiente au drept consecinţă reducerea costurilor operaţionale. Lucrarea va înfăţişa aceste concepte precum şi bunele practici ce pot fi adoptate pentru a obţine un mediu controlabil.

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

Pentru a oferi un set complet de informaţii care să poată fi utilizate şi să producă rezultate imediat, lucrarea îşi propune să prezinte câteva tehnici de bază privind optimizarea proceselor. Vom prezenta cunoştinţele minime necesare pentru identificarea, definirea, implementarea, evaluarea şi optimizarea fluxurilor de informaţii care constituie procesele operaţionale. Acestea vor acoperi atât aspectele operaţionale din organizaţie, cât şi aspectele interacţiunii acesteia cu persoanele fizice ale căror date personale sunt prelucrate (de exemplu, clienţi), ori cu furnizori de servicii (de exemplu, sub-contractanţi, producători).

Cititorul va avea la dispoziţie informaţii cu ajutorul cărora să înţeleagă modul în care mai multe standarde şi practici pot fi utilizate pentru a realiza din procesele şi elementele de control implementate un ecosistem informatic orientat către performanţă şi cu posibilitatea de optimizare continuă, pentru a reduce cât mai mult nivelul riscului operaţional.

În managementul riscurilor este crucial ca evaluarea riscurilor şi identificarea eventualelor vulnerabilităţi să se realizeze în TOATE activităţile organizaţiei. Doar astfel este posibilă luarea unor măsuri corecte care să ajute la menţinerea sub control a riscurilor operaţionale.

# 2. Managementul riscului

În contextul în care atât organizaţiile cât şi 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 organizaţiei. Managementul riscului ne oferă posibilitatea de a echilibra balanţa între riscuri şi oportunităţi, însă pentru aceasta trebuie să fim capabili să integrăm această practică în toate activităţile şi procesele noastre. Astfel, responsabilii cu implementarea procesului de management al riscului trebuie să aibă o participare activă şi să se asigure că toate riscurile sunt identificate, evaluate, monitorizate şi, unde este cazul, soluţionate/remediate.

Managementul riscului ne vorbeşte, aşa cum spuneam, despre echilibru şi despre abilitatea de a pune în balanţă riscurile şi recompensele/beneficiile. Nu în ultimă instanţă, managementul riscului presupune şi identificarea oportunităţilor pe care organizaţiile ar trebui să le ia în considerare şi să le fructifice. Nu degeaba în limba chineză, limba unei civilizaţii ce a dăruit umanităţii un tezaur de nepreţuit, semnul ce defineşte criza înseamnă atât oportunitate cât şi risc.

## A. Cum a început?

Studiul managementului riscului a început efectiv abia după cel de-al Doilea Război Mondial, deşi subiectul a fost asociat de mult timp cu asigurările menite să protejeze indivizii şi companiile împotriva accidentelor[10]. Rădăcinile acestui domeniu sunt legate de naşterea teoriei probabilităţilor. De mii de ani, de la apariţia jocurilor de noroc, riscul i-a îngrijorat şi în acelaşi timp i-a fascinat pe oameni. În secolul al XVI-lea, învăţatul pluridisciplinar Gerolamo Cardano[11] definea şansa ca pe raportul dintre numărul de rezultate favorabile şi numărul total de rezultate. În secolul al XVII-lea, matematicienii Fermat şi Pascal deja corespondau despre doctrina probabilităţilor, iar peste mai puţin de un secol, în Japonia anului 1730, este atestat primul contract tip „future" pe preţul 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", şi până în zilele noastre, când reglementările legate de managementul riscului includ deja acordurile Basel şi 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 şi 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 şi 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, şi 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) şi probabilitatea ca acel eveniment să se materializeze.

Astfel, avem:

***R = P x I***

Unde:

R = risc

P = probabilitate

I = impact potențial

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

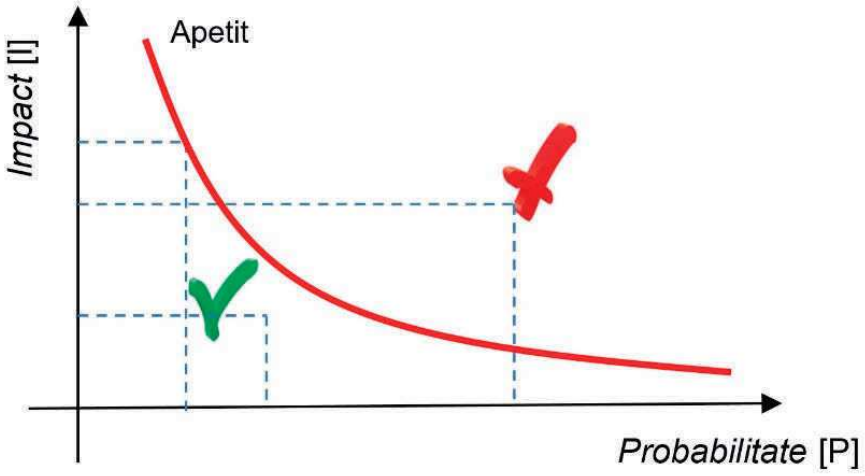


***Figura 2.1.*** *– Definiția riscului*

Există o relaţie de directă proporţionalitate între risc şi impact şi probabilitate – pe măsură ce impactul potenţial şi probabilitatea cresc, şi riscul la care suntem expuşi creşte. Privind graficul de mai sus, se poate intui că pentru valori mari ale probabilităţii, ale impactului sau ale produsului lor, riscul depăşeşte 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 îşi asume un anumit risc deoarece crede că merită şi beneficiile aşteptate depăşesc eventualele consecinţe negative, considerate relativ improbabile. Apetitul pentru risc va fi descris pe larg în capitolul dedicat. Într-o organizaţie, el trebuie definit în legătură cu standardele minime de risc informatic şi cu strategia afacerii.

Pentru managementul riscului informatic, este utilă şi o altă definiţie, echivalentă, aşa cum este prezentată de ***NIST SP 800-30***. Riscul este o funcţie de probabilitatea ca o ameninţare să exploateze o vulnerabilitate şi de impactul pe care acest eveniment l-ar avea asupra organizaţiei. Această definiţie se poate exprima şi ca o proporţionalitate directă, în următorul mod:

***R = A x V x I***

Unde:

R = risc

A = ameninţarea

V = vulnerabilitatea

I = impactul potenţial

### C. Procesul de management al riscului

Putem privi procesul de management[12] 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 înţelegere a contextului şi 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.

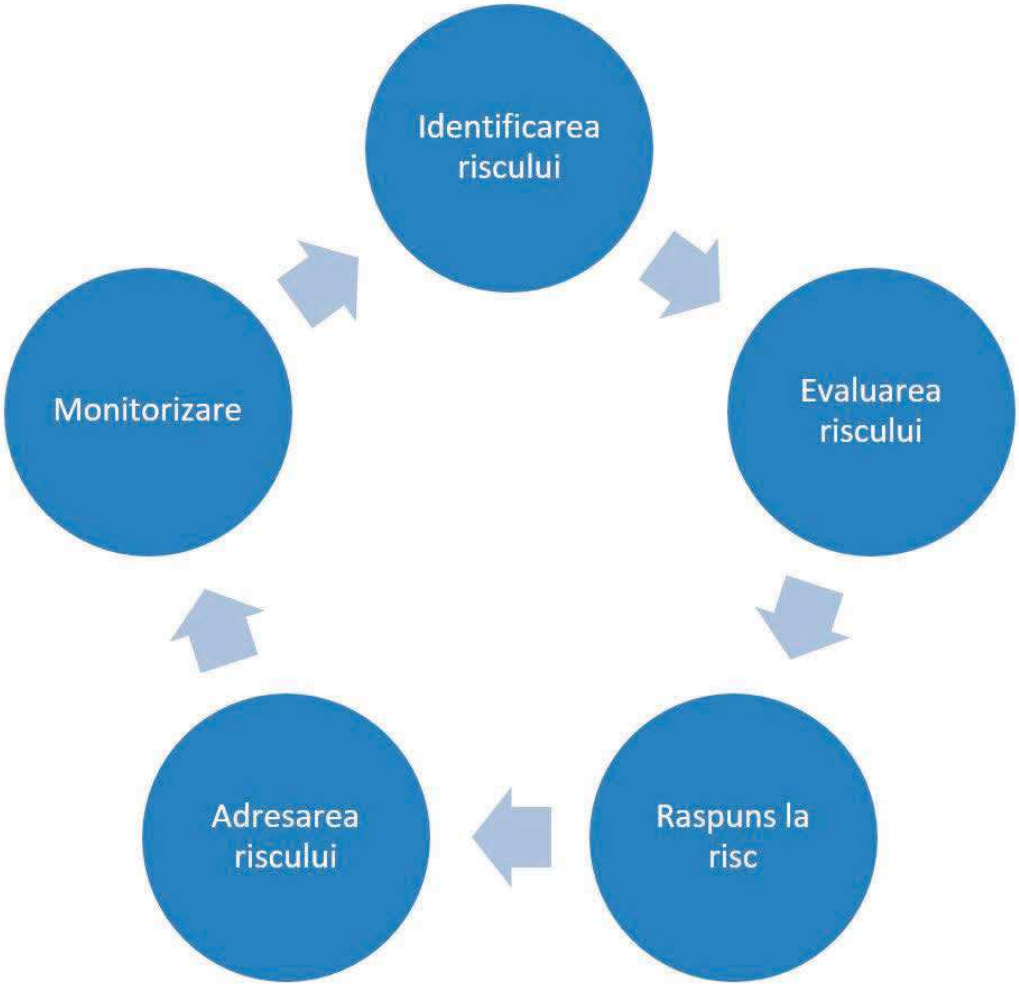


***Figura 2.2. –*** *Procesul de management al riscului*

## D. Tipuri de risc

Există mai multe metode de a împărți riscurile în categorii precum interne și externe (mai precis, endogene și exogene[13]), 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 şi regulilor în vigoare, acestea sunt supuse schimbării şi există riscul apariţiei de noi reguli în viitor, cu care firma trebuie să se conformeze, alocând noi resurse şi fonduri, în loc sa le investească în schimbări care o avantajează. Se adaugă riscul de amenzi sau procese civile, care ridică miza chiar mai mult. Din perspectiva conformităţii cu dispoziţiile legale, riscurile privind datele personale sunt reflectate în mare parte în riscul de conformitate.

Riscul **operaţional** priveşte înspre activităţile de zi cu zi ale organizaţiei, care şi ele pot eşua sau produce erori. Ele pot fi cauzate de oameni, procese sau sisteme din interiorul firmei dar şi de evenimente externe precum o pană de curent ori un dezastru natural. De cele mai multe ori riscul generat de tehnologia informaţiei (sau riscul IT) este inclus în această categorie, dar nu ar trebui scăpate din vedere interdependenţele cu toate celelalte categorii. Adesea, anumite riscuri legate de protecţia datelor personale sunt incluse în această categorie.

Riscul de **imagine** (sau reputaţional) poate fi rezultatul publicităţii negative, al unui produs defect ori al unui proces intentat firmei. Reputaţia bună se construieşte într-un timp îndelungat dar se poate pierde într-o singură zi. Un exemplu frecvent, de răsunet şi relevant pentru securitatea informaţiei este o scurgere de date despre clienţii firmei din cauza unui atac cibernetic. Aceasta poate genera o problemă mare de reputaţie, uneori chiar fatală afacerii.

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

Vom reveni asupra interdependenţelor dintre riscurile IT şi categoriile de riscuri de mai sus în capitolele ulterioare, accentuând implicaţiile asupra securităţii informaţiei.

# 3. Managementul riscului pentru sisteme informatice

Managementul Riscului Informatic (MRI)[14] poate fi definit ca ansamblul eforturilor depuse în vederea combaterii ameninţărilor, a vulnerabilităţilor şi a consecinţelor datorate datelor neprotejate. Acest concept cuprinde managementul riscului în protecţia datelor.

Pentru a simplifica lucrurile, vom folosi definiţiile care urmează. **Informaţia**[15] este componenta unui proces din activitatea organizaţiei (flux de informaţii) susţinut de tehnologie. Întreg ansamblul de procese din activitatea organizaţiei, tehnologia pe care acesta se sprijină, roluri şi responsabilităţi pentru transformarea informaţiei (adică de realizarea activităţilor procesului) îl denumim **sistem informatic**[16].

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

Evoluţia tehnologiei şi creşterea mobilităţii utilizatorilor determină ca delimitarea între viaţa profesională şi cea personală să fie din ce în ce mai greu de realizat. În acest sens, este necesar să întreprindem acţiuni care să ia în seamă ambele perspective, atât cea profesională cât şi cea personală, fără însă a le afecta independenţa. Suntem în situaţia unei schimbări de paradigmă privind securitatea informaţiei şi de aceea este necesar să avem o abordare holistică privind managementul riscului.

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

---

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

[15] Informaţie – definiţie – *https://ro.wikipedia.org/wiki/Informa%C8%9Bie*, accesat la 10 octombrie 2019.

[16] Sistem informatic – definiţie – *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 şi procesul de managementul riscului propriu-zis. Este necesară o abordare simplificată, fără a afecta însă eficacitatea metodelor şi luând în calcul faptul că protecţia datelor este componentă a managementului securităţii informaţiei (acesta din urmă deţinând cel mai complet şi cel mai matur set de practici pentru protecţia datelor). Astfel, vom construi în continuare un sistem de management pentru managementul riscului bazat pe bunele practici din managementul securităţii informaţiei într-un mod eficient, robust, aliniat la standardele internaţionale şi în conformitate cu legislaţia în vigoare (GDPR sau Regulamentul UE 679/2016).

## ➥ 3.1. Securitatea Informaţiei

Să începem prin a pune în evidenţă ce este securitatea informaţiei, care sunt ariile sale de activitate şi care sunt diferenţele faţă de securitatea IT, cu care este adesea confundată.

Securitatea informaţiei se ocupă cu protejarea informaţiei şi a sistemelor informatice de accesul neautorizat, folosirea, dezvăluirea, întreruperea, modificarea neautorizată sau distrugerea. Este o disciplină aplicabilă oricărui domeniu de activitate. *Securitatea informaţiei poate fi obţinută prin implementarea unui set adecvat de politici, practici, proceduri, structuri organizaţionale, funcţii, aplicaţii software şi echipamente tehnice care, **împreună**, asigură atingerea obiectivelor de protecţie a informaţiei*.

Securitatea informaţiei cuprinde arii de activitate precum:

– cadru de lucru pentru securitate (în engleză: *security framework*).
– dezvoltare de politici.
– campanii de conştientizare.
– dezvoltare de proceduri de securitate.
– continuitatea afacerii.
– sistemul de management al securităţii informaţiei.
– analiza de risc.
– ghid de bune practici.
– confidenţialitatea datelor.
– management în situaţii de criză.
– plan de securitate a informaţiei.
– conformitate.
– implementare model de guvernanţă.
– şi altele.