004.056.5+005.52:005.334

EVALUAREA RISCULUI SECURITĂȚII CIBERNETICE

Drd. Valentin BRICEAG, USM
valentinbriceag@gmail.com
Conf. univ. dr. Tudor BRAGARU, USM
theosnume@gmail.com

Moto: *„Dac-oi ști unde-oi cădea,*
oi așterne un sac cu paie”.
(folclor)

Pandemia COVID-19 a accelerat digitalizarea proceselor de afaceri, lucrul/accesul de la distanţă la date sensibile şi resurse corporative critice. Se observă extinderea rapidă a serviciilor de închiriere a componentelor IT (cloud computing), iar criminalitatea cibernetică urmează aceeaşi tendinţă: creşterea bruscă a atacurilor globale de tip ransomware, furtul şi divulgarea datelor cu caracter personal, atacurile pe siteurile de ştiri, atacurile de email de tip phishing etc. Creşterea criminalităţii cibernetice raportate de la începutul pandemiei este de cca 300%. Drept urmare, securitatea cibernetică a devenit foarte importantă pentru toate organizaţiile, de toate tipurile şi dimensiunile. Scopul lucrării constă în elucidarea tendinţelor moderne în evaluarea şi tratarea riscurilor de securitate cibernetică ale unei entităţi, care vizează automatizarea proceselor de securitate cibernetică pentru eliminarea sarcinilor repetitive şi reducerea influenţei factorului uman.

Cuvinte-cheie: *securitatea cibernetică, securitatea informaţiei, risc de securitate cibernetică, evaluarea riscurilor, telemuncă, ameninţări, vulnerabilităţi.*

JEL: N74, O33, Q55.

1. Introducere

De când a apărut COVID-19 şi majoritatea organizaţiilor au trecut la activităţi online în spaţiul cibernetic global, aproape fiecare companie este nevoită să evalueze şi să gestioneze riscurile cibernetice. Deoarece, după transferarea majorităţii activităţilor în online, la distanţă, de la domiciliu, când toată lumea este atât de interconectată, aproape toate organizaţiile au devenit o ţintă foarte atractivă pentru atacanţi. Există multe

004.056.5+005.52:005.334

CYBER SECURITY RISK ASSESSMENT

PhD candidate Valentin BRICEAG, USM
valentinbriceag@gmail.com
Assoc. Prof. PhD Tudor BRAGARU, USM
theosnume@gmail.com

Motto: *“If I knew where I’d fell, I’d lay*
a bag of straw”.
(folklore)

The COVID-19 pandemic has accelerated the digitization of business processes, remote work/ access to sensitive data and critical corporate resources. There is a fast expansion of cloud computing services. The cybercrime follows the same trend: the sudden rise of global ransomware attacks, theft and disclosure of personal data, attacks on news sites, phishing email attacks, etc. The cybercrime increase reported since the beginning of the pandemic is about 300%. As a result, cyber security has become very important for all organizations,of all types and sizes. This paper aims to elucidate modern trends in the assessment and treatment of cyber security risks of an entity, automatize the cyber security processes to remove repetitive tasks and reduce the influence of the human factor.

Keywords: *cyber security, information security, cyber security risk, risk assessment, telework, threats, vulnerabilities.*

JEL: N74, O33, Q55.

1. Introduction

Since the advent of COVID-19 the most organizations have moved to online activities in the global cyberspace, and almost every company has to assess and manage cyber risks. Since, after transferring most activities online, remotely, from home, when everyone is so interconnected, almost all organizations have become a very attractive target for attackers. There are many inherent risks in this regard, which, until the digital age and the COVID-19 pandemic, companies did not really face.

According to Hacking Statistics 2020 [1] and other alarming cyber security statistics [2],

riscuri inerente în acest sens, riscuri, cu care, până în era digitală şi cea a pandemiei COVID-19, companiile nu s-au confruntat cu adevărat.

Conform Hacking Statistics 2020 [1] şi altor statistici alarmante privind securitatea cibernetică [2], criminalitatea informatică constituie cea mai mare ameninţare pentru fiecare companie din lume. La fiecare 39 de secunde, are loc un atac cibernetic. Hackerii fură 75 de înregistrări în fiecare secundă. 73% dintre hackeri au declarat că securitatea tradiţională *firewall* şi *antivirus* sunt irelevante sau perimate. Hackerii creează zilnic 300.000 de noi programe *malware*. În medie, în fiecare zi, sunt piratate cca 30.000 de site-uri web noi. Circa 46% din web-aplicaţii au vulnerabilităţi critice. Fiecare două din trei întreprinderi mici şi mijlocii sunt atacate sistematic.

Recent, în Republica Cehă, un atac cibernetic a oprit toate intervenţiile chirurgicale urgente şi a redirecţionat pacienţii critici către un spital ocupat cu lupta cu COVID-19. În Germania, o companie de livrare a alimentelor a căzut victimă unui atac distribuit de refuz de serviciu (atac DDoS) etc. Printre alte constatări notabile privind tendinţele ameninţărilor, Webroot [3] menţionează că unu din 50 de site-uri este răuintenţionat; aproximativ 25% dintre acestea sunt găzduite de domenii de încredere; unu din trei site-uri de *phishing* utilizează protocolul HTTPS (Hyper Text Transfer Protocol/Secure), pentru a oferi încredere. Şi Verizon, în rapoartele sale din anul 2020 [4], trage alarma: majoritatea încălcărilor implică phishing-ul şi folosirea credenţialelor furate; peste 90% din programele *malware* sunt livrate prin e-mail şi cca 27% dintre incidentele *malware* pot fi atribuite *ransomware-ului*; 70% dintre încălcări au fost cauzate de străini; 86% dintre încălcări au fost motivate financiar; 43% dintre încălcări au constituit atacuri asupra aplicaţiilor web (în 2019, mai mult decât dublu faţă de anul 2018).

Ca urmare, se impun investigaţii sistematice ale SC şi o abordare modernă, proactivă pentru analiza, evaluarea şi tratarea riscurilor de SC, care au un impact negativ asupra activelor informaţionale valoroase pentru afacere. Acest subiect şi constituie laitmotivul prezentei lucrări.

2. Metode aplicate

Un risc este o funcţie a impactului şi a probabilităţii pentru un eveniment care poate împiedica realizarea obiectivelor şi proceselor de afaceri şi poate duce la unele pierderi. Este relativ uşor să evaluezi pierderile în urma unui incident

the cybercrime is the biggest threat to every company in the world. There is a cyber-attack every 39 seconds. Hackers steal 75 records each second. 73% of hackers declare the traditional *firewall* and *antivirus* security irrelevant or outdated. 300,000 new *malwares* are created every day. On average, about 30,000 new websites are hacked every day. 46% of web applications have critical vulnerabilities. Every two out of three small and medium-sized enterprises are attacked and many more besides.

Recently, in the Czech Republic, a cyber-attack stopped all urgent surgeries and redirected critical patients to a busy hospital struggling COVID-19. In Germany, a food delivery company felt victim to a distributed attack of work refusal etc. Among other remarkable findings on threat trends, Webroot [3] notes that one among 50 sites is malicious; about 25% of them are hosted on trusted domains; each of the three *phishing* sites uses the HTTPS (Hyper Text Transfer Protocol/ Secure) protocol to provide trust. And Verizon, in its 2020 statements [4], sounded the alarm: most infringements involve phishing and the use of stolen credentials; over 90% of *malware* is delivered via email and about 27% of *malware* incidents can be attributed to *ransomware*; 70% of contraventions were caused by foreigners; 86% of infractions were financially motivated; 43% of invasions were attacks on web applications (in 2019, more than double the 2018 outcomes).

As a result, systematic investigations of CS and a modern, proactive approach to the analysis, assessment and treatment of SC risks are required, which have a negative impact on information assets valuable to the business. This subject is the leitmotif of present paper.

2. Applied methods

A risk is a function of the impact and probability of an event that may impede the achievement of business objectives and processes and may lead to some losses. It is relatively easy to assess losses following a CS incident, but it is difficult to justify investing in controls before the incident occurs. A suitable solution for the inclusion of IS improvement investments in the acceptance area is the risk analysis.

There are a great variety of qualitative and quantitative methods and techniques for analysing

de SC, dar este dificil să justifici investiţiile în controale înainte de producerea incidentului. O soluţie potrivită pentru încadrarea în aria de acceptabilitate a investiţilor de îmbunătăţire a SI este analiza de riscuri.

Există o mare varietate de metode şi tehnici calitative şi cantitative de analiză a riscurilor de SI, pornind de la metode manuale şi şabloane Excel şi terminând cu instrumente software, care au la bază algoritmi complecşi de calcul, e.g. simularea Monte Carlo, tehnici de modelare bayesiană etc. Metodele manuale sunt transparente şi au avantajul că ajută să se înţeleagă mecanismele cauză-efect, facilitează luarea deciziilor în cunoştinţă de cauză, dar au un grad relativ ridicat de subiectivism şi necesită foarte multă muncă. Metodele automatizate sunt mult mai uşor de aplicat, deoarece reduc subiectivitatea asociată cu evaluările manuale ale riscurilor, dar ascund legăturile intime ale fenomenelor şi îngreunează luarea deciziilor în cunoştinţă de cauză.

Analiza de risc este un procedeu de identificare şi evaluare a factorilor, care pot produce prejudicii activităţii cu scopul de identificare a controalelor potrivite de atenuare a acestor riscuri inerente pentru a menţine impactul în limitele acceptabile (risc rezidual). Controalele şi acţiunile de atenuare sunt concepute pentru a reduce probabilitatea de apariţie a riscului sau a impactului riscului, care, deja, s-a produs. Cauzele riscurilor pot fi în situaţiile, condiţiile sau evenimentele interne/externe specifice care provoacă apariţia riscului. Cauzele sunt unice şi foarte specifice procesului, produsului, serviciului sau activităţii organizaţiei. Cauzele pot consta în controale slabe sau inadecvate, eşecuri accidentale sau intenţionate, factori extremi, precum concurenţa, cataclismele naturale etc. Riscurile pot fi evaluate la nivel de entitate, proces, produs/serviciu, cerinţe de reglementare sau activităţi de suport.

Cercetarea se concentrează pe metode de analiză calitativ-cantitativă a riscului securităţii informaţiei în baza standardelor ISO/IEC 27005 [12] şi ISO 31000 [13], având ca ţintă lupta cu complexitatea şi diminuarea influenţei factorului prin automatizarea analizei riscurilor în cea mai mare măsură posibilă.

3. Rezultate obţinute şi discuţii privind analiza şi evaluarea riscurilor cibernetice

3.1. Cadrul general de abordare a securităţii informaţiei/securităţii cibernetice

Securitatea informaţiei şi securitatea cibernetică sunt concepte cu sens foarte apropiat. Foarte

IS risks, starting with manual methods and Excel templates and ending with software tools, which are based on complex computational algorithms, e.g. Monte Carlo simulation, Bayesian modelling techniques etc. Manual methods are transparent and have the advantage that they help to understand the cause-and-effect mechanisms, facilitate informed decision-making, but have a relatively high degree of subjectivism and require a lot of work. Automated methods are much easier to apply, reduce the subjectivity associated with manual risk assessments, but hide the intimate links of phenomena and make it difficult to make informed decisions.

Risk analysis is a process of identifying and assessing factors that may harm the business in order to identify appropriate controls to mitigate these inherent risks in order to maintain the impact within acceptable limits (residual risk). Controls and mitigation actions are designed to reduce the likelihood of a risk or impact that has already occurred. The causes of the risks can be the specific internal/external situations, conditions or events that cause the risk. The causes are unique and very specific to the process, product, service or activity of the organization. The causes can be weak or inadequate controls, accidental or intentional failures, extreme factors such as competition, natural cataclysms, etc. Risks can be assessed at the level of the entity, process,

The research focuses on methods of qualitative-quantitative analysis of information security risk based on ISO/IEC 27005 [12] and ISO 31000 [13], aiming to combat the complexity and diminish the influence of the prime factor to automate risk analysis to the greatest extent possible.

3. Results obtained and discussions on the analysis and assessment of cyber risks

3.1. General framework for addressing information security/cyber security

Information security and cyber security are very close concepts. Briefly, cyber security is the security of information in cyberspace [5, 6]. According to the interpretation of some practitioners [5] *"For a corporation CS represents about 95% of IS; the difference between them is that IS also includes non-digital information (for example, on paper), while CS focuses only on information in digital form"*. Indeed, both con-

succint, securitatea cibernetică constituie securitatea informaţiei în spaţiul cibernetic [5, 6]. Conform interpretării unor practicieni [5] *„Pentru o corporaţie, SC reprezintă cca 95% din SI; diferenţa dintre ele denotă că SI include şi informaţii non-digitale (de exemplu, pe suport de hârtie), în timp ce SC se concentrează doar pe informaţii în formă digitală”*. Într-adevăr, ambele concepte se referă la conservarea *confidenţialităţii, integrităţii* şi *accesibilităţii (disponibilităţii)* informaţiei, cunoscute ca **asigurarea triadei CIA** *(din engleză, de la Confidentiality, Integrity, Availability)* [7]. Şi securitatea informaţiei şi securitatea cibernetică implică securitatea sistemelor informaţionale şi a infrastructurii de suport. Însă, SC are un sens mai larg, care denotă că *„orice securitate legată de spaţiul cibernetic, este un mediu complex ce apare în procesul de interacţiune a persoanelor, a software-ului şi a serviciilor Internet furnizate prin dispozitive tehnologice sau reţele integrate”* [8].

SC nu se concentrează doar pe protecţia CIA, ci şi pe protecţia mediilor de operare şi utilizare a sistemelor informaţionale şi a rezultatelor acestora *(programe, infrastructuri critice, reţele Intranet-Extranet-Internet, computere, servere şi alte elemente ale infrastructurii comune TIC, precum şi date, documente, informaţii),* care pot fi utilizate împreună pentru a spori beneficiile unei afaceri/organizaţii.

Motto-ul constitute laitmotivul evaluării şi tratării corespunzătoare a riscurilor de securitate cibernetică, iar relaţiile dintre securitatea cibernetică şi alte domenii de securitate pot fi văzute în figura 1.

cepts refer to the preservation of the confidentiality, integrity and accessibility (availability) of information, known as **ensuring the CIA triad** (*Confidentiality, Integrity, Availability*) [7]. Both information security and cyber security involve the security of information systems and support infrastructure. However, CS has a broader meaning of "*any security related to cyberspace, which is a complex environment that occurs in the process of interaction of people, software and Internet services provided through technological devices or integrated networks*" [8].

CS focuses not only on the protection of the CIA, but also on the protection of operating environments and use of information systems and their results (*programs, critical infrastructures, Intranet-Extranet-Internet networks, computers, servers and other elements of the common ICT infrastructure; data, documents, information*), which can be used together to enhance the benefits of a business/organization.

The motto is the leitmotif of the proper assessment and treatment of cyber security risks. For the relationship between cyber security and other areas of security see figure 1.

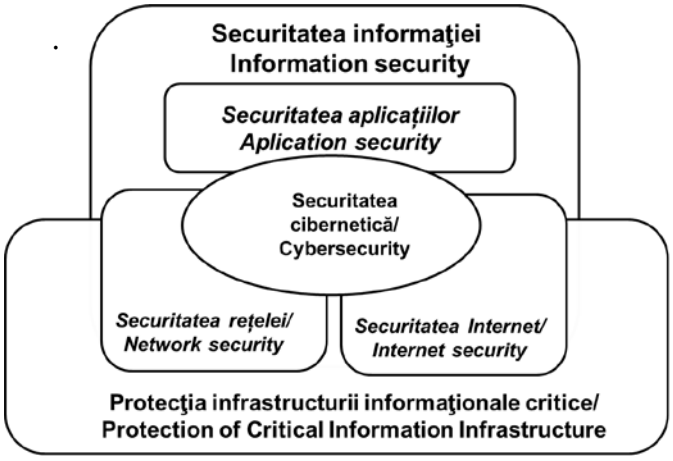

Figura 1. Relațiile dintre securitatea cibernetică și alte domenii de securitate/
Figure 1. Relationships between cyber security and other areas of security
Sursa: *elaborată de autori în baza [8]/* ***Source:*** *developed by the authors based on [8]*

În concluzie, oricare ar fi securitatea, a informaţiei sau cibernetică, şi oricare ar fi organizaţia (mărime, tip, industrie etc.), aceasta se poate călăuzi de *ISO/IEC 27001:2013* pentru analiza şi evaluarea riscurilor SC. Acest standard cere să fie definit procesul de evaluare a riscurilor *(clauza 6.1.2)*, dar nu impune metode concrete de gestionare *(măsurare-evaluare-tratare)* a riscurilor. Organizaţia ar trebui să selecteze metodele potrivite, raliate la propria metodologie generală de risc organizaţional. Totodată, *ISO/IEC 27001:2013* face referire la *ISO/IEC 27005:2018* ca standard de evaluare şi tratare a riscurilor de securitate a informaţiei, se aliniază la principiile şi liniile directoare generice furnizate de *ISO 31000:2018* şi cere să se ţină cont de consecinţele şi probabilitatea riscului. ISO 31000 [13], publicat pentru prima dată în 2009 şi revizuit în 2018, furnizează structura celor mai bune practici şi îndrumarea pentru toate operaţiunile legate de gestionarea riscurilor, oferă oportunitatea de a înţelege cauzele riscurilor şi de a identifica tratările necesare pentru a reduce impactul.

Standardul ISO/IEC 27032 [8], deşi este intitulat Ghid de cibersecuritate, în fapt, se referă *la securitatea în Internet.* Oferă recomandări privind separarea, cooperarea, coordonarea şi gestionarea eficientă a incidentelor de SC către persoanele implicate în spaţiul cibernetic.

3.1.1. Probleme majore ale securităţii informaţiei

Riscurile de SC sunt cauzate de *vulnerabilităţi* şi *ameninţări.* O **vulnerabilitate** este o *„slăbiciune”* a unui activ sau a unui control, care poate fi exploatat de o ameninţare. Este un defect, o imperfecţiune a proiectării sau implementării unui sistem informaţional şi/sau a mediului TIC, care ar putea fi exploatat intenţionat sau neintenţionat şi care ar putea afecta în mod negativ o organizaţie.

Problema cea mare constă în faptul că **numărul vulnerabilităţilor este în creştere continuă**, şi aproape că se dublează la fiecare doi ani. Conform *Tenable-2019* [9], dacă, în 2017, numărul CVE *(de la Common Vulnerabilities and Exposures)* era de 15.038, ceea ce este cu 53% mai mult decât în 2016, atunci, în 2018, numărul CVE a ajuns la 16,500. CVE [20] este un dicţionar global gestionat, care conţine cele mai frecvente vulnerabilităţi şi expuneri ale unui sistem informatic.

În consecinţă, examinarea tuturor vulnerabilităţilor constituie o sarcină destul de voluminoasă, deoarece fiecare organizaţie are o limită

In conclusion, whatever the security, information or cybernetics, and whatever the organization (size, type, industry, etc.), it can be guided by *ISO/IEC 27001:2013* for the analysis and assessment of risks. This standard requires the definition of the risk assessment process *(clause 6.1.2)*, but does not require concrete methods of risk management *(measurement-assessment-treatment)*. The organization should select the appropriate methods, related to its own general organizational risk methodology. At the same time, *ISO/IEC 27001:2013* refers to *ISO/IEC 27005:2018* as a standard for assessing and treating information security risks, aligns with the generic principles and guidelines provided in *ISO 31000:2018* and requires that the consequences and likelihood of risk be taken into account. ISO 31000 [13], first published in 2009 and revised in 2018, provides the structure of best practices and guidance for all risk management operations, provides an opportunity to understand the causes of risks and identify the treatments needed to reduce the impact.

ISO/IEC 27032 standard [8], although it is titled Cyber security guide, it actually refers to *Internet security*. It provides recommendations on the separation, cooperation, coordination and effective management of CS incidents to people involved in cyberspace.

3.1.1. Major information security issues

The risks of CS are caused by *vulnerabilities* and *threats.* A **vulnerability** is a "*weakness*" of an asset or control that can be exploited by a threat. It is a deficiency, a weakness in the design or implementation of an information system and/or the ICT environment, which could be exploited intentionally or unintentionally and which could negatively affect an organization.

The biggest problem is that **the number of vulnerabilities is constantly growing** and almost doubles every two years. According to *Tenable-2019* [9], in 2017 the CVE number *(Common Vulnerabilities and Exposures)* was 15,038, which is 53% more than in 2016, and in 2018 the CVE number reached 16,500. CVE [20] is a global managed dictionary containing the most common vulnerabilities and exposures of a computer system.

As a result, examining all vulnerabilities appears to be a quite bulky task. Each organization has an upper limit of capacity which can remedy vulnerabilities, depending on*: the busi-*

superioară a capacităţii cu care poate remedia vulnerabilităţile, în funcţie de: *apetitul afacerii pentru risc operaţional; capacitatea de a absorbi întreruperile ce ţin de remediere; eficienţă în remedierea platformei tehnice-tehnologice vulnerabile*. Soluţia potrivită ar fi **prioritizarea tratării vulnerabilităţilor**, dat fiind faptul că doar o mică parte dintre ele, de circa 2-3%, sunt exploatate şi, anume, acestea ar trebui abordate mai întâi. Cu toate acestea, dacă organizaţiile se concentrează doar asupra vulnerabilităţilor critice şi cu valori ridicate, atunci, rămân deschise atacatorilor vulnerabilităţile medii şi scăzute, care pot fi exploatate, în mod repetat şi, în consecinţă, pot duce la daune mari.

O altă problemă rezidă în faptul că, în prezent, **o companie este vulnerabilă la atacuri, deoarece fiecare angajat este vulnerabil,** dată fiind trecerea în masă la lucrul de la distanţă. Dar angajaţii nu raportează întotdeauna incidentele de SC. Conform raportului Webroot 2019 Inc. [10]: *35% dintre lucrătorii care au fost atacaţi nu se deranjează să-şi schimbe parolele după incident; 49% dintre angajaţi recunosc că fac clic pe linkuri din mesajele de la expeditori necunoscuţi în timpul muncii; 67% sunt siguri că au primit cel puţin un e-mail de phishing la locul de muncă; 40% dintre cei care au primit un e-mail de phishing nu l-au raportat*.

Activele corporative pasibile de ameninţările din spaţiul cibernetic (de către diverşi agenţi de ameninţare) pot fi **tangibile** şi **intangibile**. Cele mai răspândite **tipuri de active tangibile** sunt, dar fără a se limita la acestea:

- date, informaţii, de exemplu, documente, înregistrări, rapoarte;
- software, precum un program de calculator, un sistem de operare, o aplicaţie web;
- hardware, e.g. un computer, un suport amovibil de transport de date, un telefon mobil;
- conturi de acces la Internet şi alte servicii electronice, precum poşta electronică, plăţi electronice;
- angajaţii, cunoştinţele, calificările, abilităţile şi experienţa lor.

Activele intangibile ale organizaţiei se referă la cultura, reputaţia, imaginea sa.

Un **agent de ameninţare** este o persoană sau un grup de persoane, care au un rol în executarea sau susţinerea unui atac. După cum a fost menţionat anterior, înţelegerea motivelor *(politice, economice, religioase etc.*), a capacităţii cu care poate remedia vulnerabilităţile, în funcţie de: *apetitul afacerii pentru risc operaţional; capacitatea de a absorbi întreruperile ce ţin de remediere; eficienţă în remedierea platformei tehnice-tehnologice vulnerabile*. The right solution would be **to prioritize the treatment of vulnerabilities**, because only a small part of them, about 2-3%, are exploited, it should be addressed first. However, if organizations focus only on critical and high vulnerabilities, medium and low vulnerabilities remain open to assailants, which can be exploited repeatedly and briefly can lead to major damage.

Another problem is that nowadays **a company is vulnerable to attacks because every employee is vulnerable**, given the mass shift to remote work. But employees do not always report incidents of CS. According to the Webroot 2019 Inc. report. [10]: *35% of workers who have been attacked do not bother to change their passwords after the incident; 49% of employees admit to clicking on links in messages from unknown senders during work; 67% are sure they have received at least one phishing email at work; 40% of those who received a phishing email did not report it.*

Corporate assets, susceptible to cyberspace threats, can be **tangible** and **intangible**. The most common **types of tangible assets** include, but are not limited only to:

- data, information, for example- documents, records, reports;
- software, such as a computer program, an operating system, a web application;
- physical, for instance- a computer, a removable data carrier, a mobile phone;
- internet access and electronic services such as electronic mail, electronic payments;
- employees, their knowledge, qualifications, skills and experience.

The intangible assets of an organization refer to its culture, reputation, image, etc.

A threat agent could come from a person or group of people who have a role in executing or sustaining an attack. As mentioned above, understanding the reasons *(political, economic, religious, etc.),* the abilities *(knowledge, funding, etc.)* and the intentions *(fun, self-assertion, crime, etc.)* is essential in assessing security vulnerabilities and CS risks as well as the development and implementation of handling measures.

tăţilor *(cunoştinţe, finanţare etc.)* şi a intenţiilor *(distracţie, autoafirmare, criminalitate etc.)* este esenţială în evaluarea vulnerabilităţilor şi riscurilor de securitate cibernetică, precum şi pentru dezvoltarea şi implementarea măsurilor de tratare.

Multe dintre active pot aparţine simultan câtorva tipuri, pot avea concomitent câteva surse şi motive de ameninţări, pot utiliza capacitatea resurselor distribuite în Internet. De exemplu, un serviciu de plăţi electronice, mediat de TIC şi sisteme de operare, care rulează ca aplicaţie web pe Internet, poate fi blocat prin atacuri DDoS de criminali cu scopul de a câştiga bani şi/sau de a influenţa, din exterior, realizarea strategiei, politicii organizaţiei.

Ca urmare, pentru gestionarea cu succes a riscurilor, acestea trebuie să fie *personalizate*, *structurate* şi *cuprinzătoare, bazate pe cele mai bune informaţii disponibile, integrate, dinamice, cu luarea în considerare a factorului uman şi îmbunătăţite continuu, ţinând cont de schimbările permanente ale mediului*.

Gestiunea adecvată a riscurilor este importantă pentru:

- respectarea cerinţelor legale şi de reglementare aplicabile, de exemplu, *a cerinţelor Regulamentului general privind protecţia datelor (GDPR, General Data Protection Regulation, https://gdpr-info.eu/, UE), intrată în vigoare în 2018* şi *Legii Republicii Moldova nr.133 08.07.2011 Privind protecţia datelor cu caracter personal (modificată în 2018);*
- îmbunătăţirea detectării ameninţărilor, raportării obligatorii şi voluntare;
- creşterea probabilităţii de atingere a obiectivelor;
- minimizarea daunelor şi/sau a pierderilor, a numărului incidentelor de SC, ceea ce conduce la construirea unei baze de încredere pentru planificarea şi luarea deciziilor, îmbunătăţirea prevenirii pierderilor şi gestionarea eficientă a incidentelor de SC etc.

Pentru a gestiona eficient riscurile cibernetice în cadrul organizaţiei, este necesar **să se înţeleagă contextul organizaţiei**, să se identifice riscurile şi ameninţările, la care organizaţia este expusă, să se evalueze şi să se definească măsurile adecvate de tratare. Obiectivele gestionării cu succes a riscurilor de SC constau în reducerea riscului la un nivel acceptabil, respectarea criteriilor de risc specificate şi gestionarea continuă a acestor riscuri.

Many of the assets may belong to several types simultaneously, may simultaneously have several sources and threat reasons, may use the resources capacity distributed on the Internet. For example, an electronic payment service mediated by ICT and operating system running as a web application on the Internet, can be blocked by DDoS criminal attack in order to earn money and/or influence, an outside influence in the strategy implementation and policy organization.

As a result, for successful risk management, it must be *personalized, structured and extensive, based on the best available information, integrated, dynamic, taking into account the human factor and according to continuously environmental changes*.

Adequate risk management is important for, but not only limited to:

- meeting legal and regulation requirements, such as the request of *the General Data Protection Regulation (GDPR), https://gdpr-info.eu/EU), entered into force in 2018* and *the Law of the Republic of Moldova no.133 08.07.2011 Regarding the protection of personal data (amended in 2018);*
- improving threat detection, mandatory and voluntary reporting;
- increasing the probability of achieving the objectives;
- minimizing the damage and/or the loss, the number of CS incidents, which leads to building a reliable basis for planning and decision making, improving loss prevention and efficient management of CS incidents, etc.

In order to effectively manage cyber risks within the organization, it is necessary to **understand the organization's context**, identifying risks and threats to which the organization is exposed, assessing and defining appropriate treatment measures. The objectives of successful CS risk management are to reduce the risk to an acceptable level, to comply with the specified risk criteria and to continuously manage them.

The purpose of CS risk assessment is to continuously manage risks through identification of:

- critical assets that may adversely affect the achievement of the organization's objectives;

Scopul evaluării riscurilor privind SC constă în gestionarea continuă a riscurilor prin identificarea:

- activelor critice, care pot afecta negativ realizarea obiectivelor organizaţiei;
- severităţii vulnerabilităţilor şi ameninţărilor externe şi interne relevante pentru organizaţie;
- controalelor necesare pentru atenuarea riscurilor.

3.1.2. Fluxul general de analiză şi tratare

Gestiunea riscurilor constituie un proces ciclic, continuu şi sistematic (figura 2) cu responsabilităţi stabilite de identificare, evaluare/ măsurare, monitorizare, luare de decizii şi măsuri privind controlul sau asumarea expunerii la risc şi raportarea rezultatului acestor activităţi.

- the severity of external and internal vulnerabilities and threats relevant to the organization;
- necessary control for risk mitigation.

3.1.2. General flow of analysis and treatment

Risk management is a cyclical, continuous and systematic process (figure 2) with established responsibilities for identification, assessment/measurement, monitoring, decision-making and measures to control or assume risk exposure and reporting the outcome of these activities.

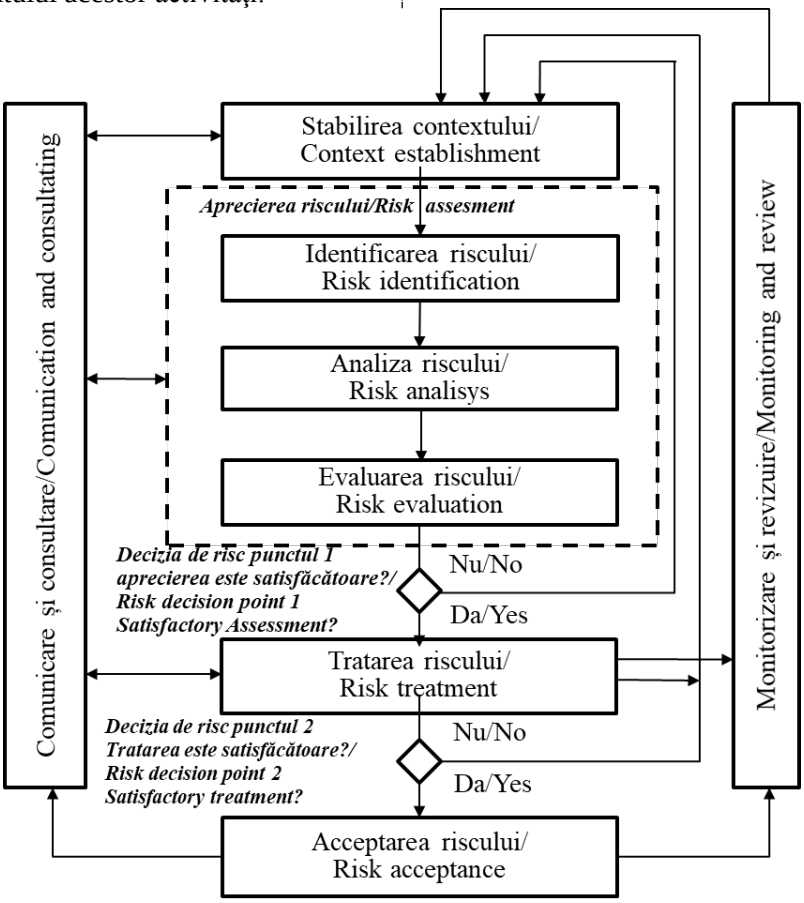

Figura 2. Procesul de gestiune a riscurilor/
Figure 2. Information security risk management process
Sursa: *elaborată de autori în baza [11]*/ ***Source:*** *developed by the authors based on [11]*

Evaluările riscurilor cibernetice ale unei companii sunt destinate identificării, estimării şi prioritizării riscurilor operaţiunilor organizaţionale (de îndeplinire a misiunii, funcţiilor organizaţiei în condiţii de păstrare a imaginii şi

A company's Cyber risk assessment is intended to identify, estimate and prioritize the risks of organizational operations (fulfilling the mission, functions of the organization while maintaining its image and reputation) and orga-

reputaţiei sale) şi activelor organizaţionale (de exemplu, date, informaţii, calculatoare, reţele şi alte dispozitive ale infrastructurii critice), ale persoanelor fizice şi altor organizaţii, rezultate din operarea şi utilizarea sistemelor informaţionale mediate de TIC.

Pentru multe organizaţii, evaluarea şi gestionarea riscurilor informaţionale/cibernetice constituie o parte crucială a strategiei de afaceri (de exemplu, pentru majoritatea e-afacerilor), pentru altele este o cerinţă obligatorie de conformitate a unor cerinţe/reglementări legale, atât de nivel local, ramural, cât şi global. De exemplu, pentru bănci şi efectuarea operaţiunilor cu carduri bancare, sunt cruciale cerinţele Standardului pentru securitatea industriei plăţilor cu carduri bancare PCI DSS:2018 [11], iar pentru spitale şi organizaţii medicale, sunt cruciale dispoziţiile de protejare şi menţinere a confidenţialităţii informaţiilor de sănătate HIPAA *(Health Insurance Portability and Accountability Act, o lege a SUA privind mobilitatea şi responsabilitatea în asigurări de sănătate, aplicată la nivel global de majoritatea statelor lumii).*

După cum se sugerează în figura 2, procesul de management al riscului SC poate fi repetat pentru activităţile de evaluare a riscului şi/sau de tratare a riscului. O abordare repetitivă asigură un echilibru între minimizarea timpului şi efortului necesar pentru identificarea controalelor, asigurând, în acelaşi timp, faptul că riscurile majore sunt evaluate în mod adecvat. Activităţile necesare pentru analiza riscurilor cibernetice, prezentate în figura 2, sunt descrise în detalii într-o serie de standarde, precum ISO/IEC 27005:2018 [12], ISO 31000:2018 [13], ISO/IEC 27001:2013 [14] etc.

Fluxul general de analiză şi tratare [12] include stabilirea contextului *(clauza 7)*, aprecierea riscului *(clauza 8)*, tratarea riscului *(clauza 9)*, acceptarea riscului *(clauza 10)*, comunicarea şi consultarea riscului *(clauza 11)*, monitorizarea şi revizuirea riscului *(clauza 12)*, rezumându-se, în general, la:

1) identificarea şi documentarea vulnerabilităţilor şi surselor de ameninţare;
2) identificarea evenimentelor ipotetice ale ameninţării (de exemplu: acces neautorizat, utilizarea frauduloasă a informaţiilor de către utilizatorii autorizaţi, scurgeri de date, expunere accidentală, pierderi de date, blocarea serviciilor etc.);

nizational assets (e.g. data, information, computers, networks and other critical infrastructure devices), of private people and other organizations, resulting from the operation and use of information systems.

For many organizations the assessment and management of information/cyber risk is a crucial part of the business strategy (for example, for most e-businesses), for others it is a mandatory requirement to comply with legal requirements/ regulations, both local, partially, as well as globally. For example, the bank performs bank card transactions and the requirements of the PCI DSS:2018 [11] are crucial; for the hospitals and medical organizations, dispositions to protect and maintain the confidentiality of health information HIPAA *(Health Insurance Portability and Accountability Act, a US law on mobility and risk in health insurance, enforced globally by most countries)* are crucial.

As figure 2 suggests, the CS risk management process may be repeated for risk assessment and/or risk treatment activities. A repetitive approach ensures a balance between minimizing the time and the effort required to identify controls, at the same time ensuring that major risks are properly assessed. The necessary activities analysing the cyber risks, presented in figure 2, are described detailed in a series of standards such as ISO/IEC 27005:2018 [12], ISO 31000:2018 [13], ISO/IEC 27001:2013 [14] etc.

The overall flow of analysis and treatment [11] includes the context setting *(clause 7)*, the risk assessment *(clause 8)*, management *(clause 9)*, acceptance *(clause 10)*, the risk communication and consultation *(clause 11)*, monitoring and review *(clause 12)* and generally summarizes:

1) vulnerabilities and sources of threat identification and documentation;
2) hypothetical threat events identification (e.g. unauthorized access, fraudulent use of information by authorized users, data leaks; accidental exposure, data loss, blocking of services, etc.);
3) vulnerabilities and favourable operating conditions identification (threats against valuable assets and/or critical, real digital infrastructure, etc.) and severity determination;
4) probability determination of such attacks being successful (taking into account the set

3) identificarea vulnerabilităţilor şi condiţiilor favorabile de exploatare (ameninţările împotriva activelor valoroase şi/sau a infrastructurii critice, digitale reale etc.) şi determinarea gravităţii acestora;
4) determinarea probabilităţii că astfel de atacuri să aibă succes (luând în considerare setul de vulnerabilităţi identificate şi condiţiile predispuse);
5) identificarea impactului posibil;
6) determinarea riscului inerent, al măsurilor de tratare şi acceptare a riscului rezidual după tratare.

3.2. Evaluarea riscului cibernetic

Abilitatea de a înţelege riscurile ne permite să acordăm prioritate resurselor şi să întreprindem măsuri de protecţie adecvate, proporţional cu valoarea acestor resurse, să cunoaştem de ce să ne păzim. Pentru a minimiza aceste riscuri, organizaţia trebuie, în primul rând, să conştientizeze SC, după care să-şi gestioneze adecvat riscurile. În cadrul cercetării, autorii întreprind anumite tentative de automatizare a gestiunii SC. Teza principală susţinută în cadrul cercetărilor se referă la automatizarea proceselor de gestionare a SC *(măsurare, evaluare, raportare)* şi a nivelului de maturitate al sistemului de management al securităţii informaţiei. Doar automatizarea operaţiilor rutinare privind inventarierea activelor, ameninţărilor şi riscurilor informaţionale, evidenţei dispozitivelor mobile şi/sau de domiciliu, cu acces la distanţă, evidenţa resurselor informaţionale critice/valoroase pentru afacere pot spori esenţial nivelul SC, iar maturitatea proceselor de evaluare-tratare a riscurilor, susţinută de măsurarea nivelului de maturitate [15] ar servi ca verigă centrală pentru planificarea-realizarea îmbunătăţirii continue a SC a unei organizaţii şi remedierii vulnerabilităţilor în timp util.

Înainte de a începe evaluarea riscului, este necesară inventarierea datelor valoroase, de care entitatea dispune, infrastructurii care trebuie protejată şi altele. Eventual, procesul poate fi demarat cu un audit de date sau al securităţii informaţiei. Un astfel de audit bine realizat identifică datele stocate de entitate şi valoarea acestora. Clauza 6.*1 ISO/IEC 27001:2013* impune existenţa unui proces *de evaluare a riscului; de identificare a criteriilor de evaluare a riscurilor; de identificare a „proprietarului riscului" şi de documentare a criteriilor de acceptare a riscurilor.* Pentru a realiza acest proces, practicienii pornesc de la clasificarea factorilor de risc (figura 3).

of vulnerabilities identified and the conditions predisposed);
5) possible impact identification;
6) inherent risk determination, handling measures and acceptance of residual risk after treatment.

3.2. Cyber risk assessment

The ability of understanding the risks allows us to give priority to resources and to take appropriate protection measures in proportion to the value of these resources, be acquainted with what to be aware of. To minimize these risks, the organization must first be aware of the CS, afterwards it must properly manage its risks. In the research, the authors make certain attempts to automatize the management of CS. The main thesis supported in the survey refers to the automatization of CS management processes (*measurement, evaluation, reporting*) and the level of maturity of the information security management system. Only automatization of routine operations regarding the inventory of the assets, threats and information risks, the mobile and/or home devices accounting, with remote access, the evidence of critical/valuable business information resources can significantly increase the CS level. The risk maturity assessment-treatment processes, supported by measuring the level of maturity [15] would serve as a central link for planning-achieving continuous improvement of an organization's CS and remedying vulnerabilities in a timely manner.

Before initiating the risk assessment, it is necessary to inventory the valuable data available to the entity, the facilities protection, etc. Eventually, the process can be started with a data or information security audit review. A well-performed audit review identifies the data stored by the entity and its value. Clause 6.1 *ISO/IEC 27001:2013* requires the existence of a *risk assessment process; to identify its assessment criteria; to determine the "risk owner" and to document the risk acceptance criteria.* In order to accomplish this process, practitioners start from the classification of risk factors (figure 3).

According to the clause *6.1.2 ISO/IEC 27001:2013*, the organization should establish and maintain:

- *risk assessment criteria (assignment of values);*

Conform clauzei *6.1.2 ISO/IEC 27001:2013,* organizaţia ar trebui să stabilească şi să menţină:

- *criteriile de evaluare a riscurilor (de atribuire a unor valori);*
- *criteriile de impact (determinare a consecinţelor);*
- *criteriile de acceptare a riscurilor (tratare),* iar evaluările de risc *trebuie să genereze rezultate consistente, valide şi comparabile la o evaluare repetată a riscului.*

- *impact criteria (determination of consequences);*
- *risk acceptance criteria (treatment),* and risk assessments *it must produce consistent, valid and comparable results in a repeated risk assessment.*

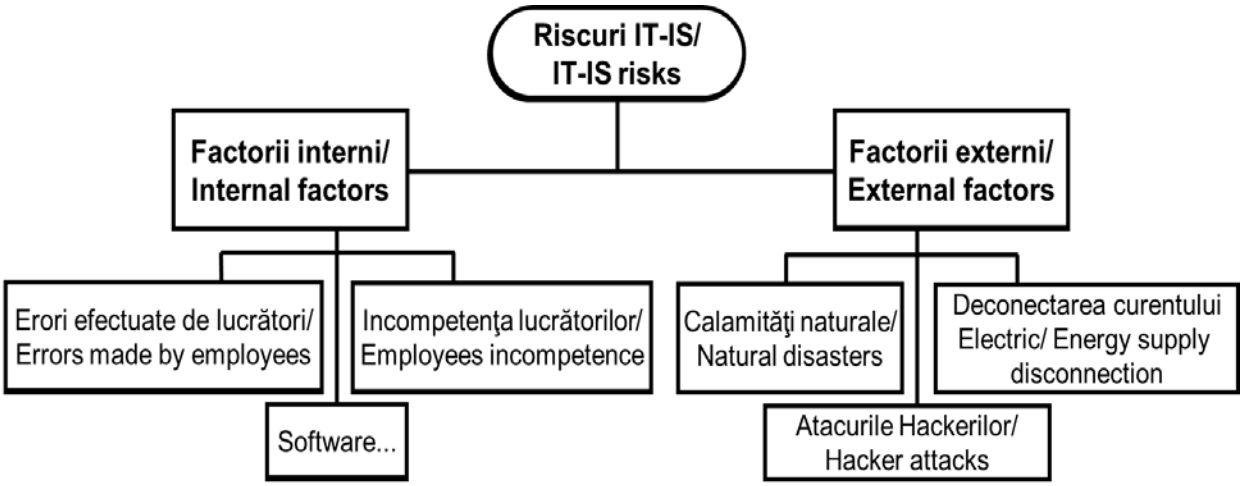

Figura 3. Factorii de risc și cauzele apariției riscurilor în adresa SC/
Figure 3. Risk factors and causes of the cybersecurity risks
Sursa: *elaborată de autori/* ***Source:*** *developed by the authors*

Criteriile de evaluare a riscului se pot baza pe valoarea strategică a proceselor şi activelor informaţionale ale afacerii; pe criticitatea bunurilor informaţionale implicate *(de exemplu, importanţa operaţională şi de afaceri pentru disponibilitate, confidenţialitate şi integritate);* pe aşteptările şi percepţiile părţilor interesate şi pe consecinţele negative asupra imaginii şi reputaţiei entităţii.

Criteriile de impact/consecinţă se referă la gradul de daune sau costuri pentru organizaţie cauzate de un eveniment de securitate a informaţiilor.

Criteriile de acceptare a riscului depind de politicile, obiectivele şi preocupările părţilor interesate ale organizaţiei; de operaţiunile IT/IS; de finanţe; de factorul uman şi de factorii sociali.

Fiecare organizaţie defineşte propriile scări ale nivelului de acceptare a riscurilor.

3.3. Măsurarea probabilităţii, impactului şi valorii riscului

Riscurile de securitate sunt analizate în funcţie de probabilitatea (posibilitatea) apariţiei

Evaluation risk criteria is based on the strategic value of business information processes and assets; on the criticality of the informational goods involved *(e.g. operational and business availability importance, confidentiality and integrity),* on the expectations and perceptions of stakeholders and the negative consequences on the entity's image and reputation.

Impact/consequence criteria refer to the damage degree or costs for the organization caused by an information security event.

Risk acceptance criteria depend on the policies, objectives and interests of the organization's stakeholders; IT/IS operations, finance, the human factor and social factors.

Each organization defines its own scale of risk level acceptance.

3.3. Measuring the probability, impact and risk value

Security risks are analysed according to the risk probability (possibility) and the severity/impact on the objectives, if the risk occurs. There are various *qualitative* and *quantitative*

riscului şi de gravitatea/impactul asupra obiectivelor, în cazul în care survine riscul. Există diverse *metode calitative* şi *metode cantitative* de analiză a riscurilor, inclusiv metode automatizate, care se bazează pe profiluri de risc. Detalii şi îndrumări privind selectarea şi aplicarea metodelor de evaluare a riscurilor în diverse situaţii pot fi observate în ISO 31010:2019. Risk management – Risk assessment techniques. Acest standard enumeră 41 de tehnici de evaluare a riscurilor (31 în prima ediţie din 2009), care ajută la luarea deciziilor în condiţii de incertitudine. Standardul este complet raliat la ISO 31000:2018 [13].

Evaluarea probabilităţii producerii unui eveniment poate fi *definită, determinată* sau *măsurată*, în mod obiectiv sau subiectiv, şi poate fi exprimată calitativ sau cantitativ. Adesea, în cadrul modelelor de risc, pentru a trece de la valori calitative la valori cantitative ale probabilităţii, impactului, valorii şi nivelului de risc, sunt utilizate valori semicantitative, descrise în tabelele 1-3. Utilizarea în întreaga organizaţie a tabelelor unice simplifică activităţile de evaluare a riscului.

risk methods analysis, including automated methods, which are based on risk profiles. Details and guidance on the selection and application of risk assessment methods in various situations see ISO 31010: 2019. Risk management – Risk assessment techniques. This standard lists 41 risk assessment techniques (31 in the first edition of 2009), which are helping in conditions of uncertainty on decision making. The standard is fully aligned with ISO 31000: 2018 [13].

Assessing the probability occurrence of an event can be *defined*, *determined* or *measured* objectively or subjectively and can be expressed qualitatively or quantitatively, frequently, within risk patterns, moving from qualitative values to quantitative probability values, impact, value and risk level, Semi-quantitative values are described, as presented in tables 1-3. The use of single tables across the organization simplifies risk assessment activities.

Tabelul 1/Table 1

Tabel de probabilitate a riscurilor informaționale/
Probability table of information security risks

Calificativul/Valoarea calitativă/ Qualifier/Qualitative value	**Valori semicantitative/ Semi-quantitative values**			**Descrierea/ Description**
1	2	3	4	5
Improbabil, foarte rar/ Unlikely, infrequent	<1%	1	0	Mai puțin de o dată la 100 ani/ Less than once every 100 years
Puțin probabil, probabilitate scăzută/ Unlikely, low probability	1-10%	2	2	La fiecare 5-10 ani/ Every 5-10 years
Posibil, probabilitate medie/ Possibly, average probability	10 -50%	3	5	O dată la 3-5 ani/ Once every 3-5 years
Probabil, probabilitate mare/ Probably high probability	50-84%	4	8	La fiecare 1-2 ani/ Every 1-2 years
Aproape sigur, cert/ Almost certain, certain	85 100%	5	10	Mai mult de o dată pe an/ More than once a year

Sursa: *elaborat de autori în baza ISO/IEC 27001, ISO/IEC 27005/*
Source: *developed by authors based on ISO/IEC 27001, ISO/IEC 27005*

Impactul reprezintă rezultatul negativ al unui eveniment, exprimat calitativ sau cantitativ, care afectează obiectivele trasate. Măsurarea

The impact is the negative result of an event, expressed qualitatively or quantitatively, which affects the objectives set. The measure-

consecinţelor, de asemenea, este orientată spre forma tabelară (tabelul 2) de trecere de la valori calitative la valori cantitative

ment of the consequences is also oriented towards the tabular form (table 2) of transition from qualitative values to quantitative values.

Tabelul 2 / Table 2

Magnitudinea/valoarea pe 3 niveluri a impactului vulnerabilității/riscului/
Magnitude/value on a 3-level vulnerability/risk impact

Valoarea calitativă/ Qualitative value	**Valori semicantitative/ Semiquantitative value**		**Descrierea impactului riscului/exploatării vulnerabilității/ Description of the risk impact/exploitation of the vulnerability**
Mare/ Hight	**3**	**10**	Poate rezulta în pierderi de mare valoare ale bunurilor sau resurselor; afecta în mod negativ misiunea, interesul sau reputația companiei. / It can result in high value losses of goods or resources; adversely affect the company's mission, interest or reputation.
Medie/ Medium	**2**	**5**	Poate rezulta în pierderi recuperabile ale bunurilor, resurselor; afecta negativ într-o măsură medie misiunea, interesul sau reputația companiei. / It can result in recoverable losses of goods, resources; adversely affect to a medium extent the company's mission, interest or reputation.
Mică/ Low	**1**	**1**	Poate rezulta în pierderi nesemnificative ale bunurilor, resurselor; afecta negativ, în mică măsură, misiunea, interesul sau reputația companiei. / It can result in insignificant loss of goods, resources; to a lesser extent adversely affect the company's mission, interest or reputation.

Sursa: *elaborat de autori în baza ISO/IEC 27001, ISO/IEC 27005 /*
Source: *developed by the authors based on ISO/IEC 27001, ISO/IEC 27005*

După evaluarea impactului şi a probabilităţii, pentru fiecare activ/ameninţare, trebuie determinat un scor/o valoare a riscului, utilizată pentru a determina dacă este necesară tratarea suplimentară. De regulă, măsura riscului este determinată ca produs între probabilitate şi impact:

Risc = Probabilitate × Impact

Un exemplu de trecere de la valorile probabilităţii şi a impactului la aprecierea nivelului de risc îl prezentăm în tabelul 3, care se poate urmări adesea. Un asemenea tabel unic este utilizat în întreaga organizaţie, ceea ce simplifică activităţile de evaluare a riscului.

After assessing the impact and probability, a risk score/value must be determined for each asset/threat, used to trigger whether additional treatment is required. Typically, the measure of risk is determined as the product of probability and impact:

Risk = Probability × Impact

An example of moving from probability and impact values to risk level assessment is seen in table 3, that can be often seen. Such a single table is often used across the organization, which simplifies risk assessment activities.

Tabelul 3/ Table 3

Exemplu de matrice de analiză a riscurilor 5×5 (diagramă „cinci pe cinci")/ Example of a 5×5 risk analysis matrix (diagram "five per five")

Nivel de probabilitate/ Probability level	**Nivel de impact/consecință / Level of impact/consequence**				
	1	**2**	**3**	**4**	**5**
5 (Aproape sigur)/ 5 (Almost sure)	Mediu (2)/ Medium (2)	Înalt (3)/ High (3)	Foarte înalt(4)/ Very high (4)	Critic (5)/ Critic (5)	Critic (5)/ Critic (5)
4 (Probabil)/ 4 (Probably)	Mediu (2)/ Medium (2)	Înalt (3)/ High (3)	Foarte înalt(4)/ Very high (4)	Critic (5)/ Critic (5)	Critic (5)/ Critic (5)
3 (Posibil)/ 3 (Possible)	Scăzut (1)/ Low (1)	Mediu (2)/ Medium (2)	Înalt (3)/ High (3)	Foarte înalt (4)/ Very high (4)	Foarte înalt (4)/ Very high (4
2 (Improbabil)/ 2 (Unlikely)	Scăzut (1)/ Low (1)	Scăzut (1)/ Low (1)	Mediu (2)/ Medium (2)	Înalt(3)/ High (3)	Înalt (3)/ High (3)
1 (Rar)/ 1 (Rare)	Scăzut (1)/ Low (1)	Scăzut (1)/ Low (1)	Scăzut (1)/ Low (1)	Mediu (2)/ Medium (2)	Mediu (2)/ Medium (2)
Nivel de risc/ Risk level	**1(Scăzut)/ 1(Insignificant)**	**2(Minor)/ 2(Minor)**	**3(Moderat)/ 3(Moderate)**	**4(Major)/ 4(Major)**	**5(Catastrofal)/ 5(Catastrophic)**

Sursa: *elaborat de autori în baza ISO/IEC 27005 /*
Source: *developed by the authors based on ISO/IEC 27005*

Etapa finală, în procesul de evaluare a riscurilor, constă în elaborarea unui raport de evaluare a riscurilor, cu evidenţierea celor situate peste nivelul acceptabil. Acesta sprijină managementul în luarea deciziilor adecvate privind bugetul, politicile, procedurile de SC. Raportarea se poate face pe *domenii*, *procese şi resurse, eventual amplasate* într-o *unică hartă generalizatoare*. Pentru fiecare ameninţare, raportul ar trebui să descrie vulnerabilităţile corespunzătoare, activele supuse la risc, impactul, probabilitatea apariţiei şi recomandările de control.

3.4. Tratarea riscurilor

După încheierea evaluării şi aprecierii riscului, acestea sunt comparate cu criteriile convenite de tratare a riscului şi se adoptă decizia de tratare a riscurilor în conformitate cu matricea/diagrama de analiză a riscului (tabelul 3). În **zona din dreapta-sus** *(nivel critic (5), sau foarte înalt(4))* sunt riscuri cu probabilitate mare şi impact mare, pentru care trebuie aplicate controale de diminuare a valorii riscului, iar **în zona din stânga-jos** *(nivel scăzut (1))* sunt riscuri cu probabilitate mică şi impact mic, care pot fi ignorate (nu afectează grav afacerea). **Zona de mijloc** *((nivel mediu (2) sau înalt(3))* prezintă

The final stage in the risk assessment process is the elaboration of a risk assessment report, highlighting those that are above the acceptable level. It supports management in making appropriate decisions regarding the budget, policies, CS procedures. Reporting can be done on *areas*, *processes and resources*, *possibly located* in a *single generalized map*. For each threat, the report should describe the corresponding vulnerabilities, risky assets, impact, likelihood of occurrence and control recommendations.

3.4. Risk management

The risk assessment and appreciation are compared, after being completed, with the agreed risk management criteria and the risk management decision is made according to the risk analysis matrix/diagram (table 3). In the **upper right area** *(critical level (5), or very high area (4))* there are the risks with high probability and high impact, for which, check-ups to reduce the value of the risk, must be applied and the **lower left area** *(low level (1))* indicates the risks with low probability and low impact, which can be ignored (does not seriously affect the business). **The middle zone** *(medium (2) or high (3))*

riscuri cu probabilitate medie şi impact mediu, care pot fi/trebuie tratate conform criteriilor politicii de securitate.

Există **patru alternative pentru tratarea riscurilor** [12], realizată în baza criteriilor, care determină situaţiile când riscurile pot fi acceptate şi când nu: reducerea/atenuarea riscului prin aplicarea unor controale suplimentare adecvate; acceptarea riscului în cunoştinţă de cauză; evitarea riscului prin încetarea sau evitarea activităţii care creează riscul; transferul riscurilor asociate către alte părţi. Opţiunile de tratare a riscurilor trebuie să fie selectate în baza rezultatului evaluării riscurilor, a costului preconizat pentru implementarea acestor opţiuni şi a beneficiilor preconizate din aceste opţiuni. Când se pot obţine reduceri mari de riscuri cu cheltuieli relativ mici, astfel de opţiuni ar trebui să fie implementate. Alte opţiuni pentru îmbunătăţiri pot fi neeconomice şi, în asemenea cazuri, trebuie efectuată o analiză de fezabilitate pentru a justifica cheltuielile.

Procesul de tratare a riscurilor rezidă în aplicarea măsurilor *preventive, detective, corective* sau *compensatorii* asupra riscurilor, care se află peste nivelul acceptat, aducându-le la nivelul acceptabil.

Rezultatul gestiunii riscurilor de securitate poate fi transpus în modelul de maturitate a securităţii, identificând, astfel, nivelul de maturitate al SC [15]. Tradiţional, sunt utilizate 5 niveluri de maturitate a SC şi anume: Nonconformitate (1), Conformitate iniţială (2), Conformitate de bază (3), Conformitate acceptabilă (4) şi Conformitate deplină (5), figura 4.

presents medium probability and medium impact risks, which can/should be treated according to the security policy criteria.

There are **four alternatives to risk management** [12], based on criteria, which determine when risks can be accepted and when they cannot: Risk reduction/mitigation by applying appropriate additional controls; Knowing risk acceptance; Avoiding risk by stopping or avoiding the activity that creates the risk; Transfer of associated risks to other parties. Risk treatment options must be selected on the basis of the outcome of the risk assessment, the expected cost of implementing these options and the expected benefits from these options. When large risk decrease can be achieved at relatively low costs, such options should be implemented. Other options for improvement may be uneconomical, and, in such cases, a feasibility analysis must be carried out to justify the expenditures.

The risk treatment process summarizes the application of *preventive*, *detective*, *corrective* or *compensatory* measures on the risks that are above the accepted level, bringing them to the acceptable level.

The result of security risk management can be transposed into the security maturity model thus identifying the maturity level of the CS [15]. Traditionally, 5 levels of CS maturity are used, namely: Nonconformity (1), Initial Conformity (2), Basic Conformity (3), Acceptable Conformity (4) and Full Conformity (5), figure 4.

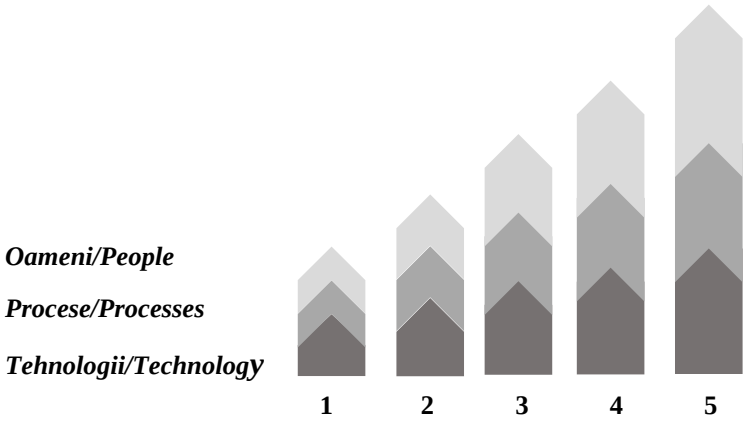

Figura 4. Nivelurile de maturitate ale SMSI/
Figure 4. Maturity levels of ISMS
Sursa: *elaborată de autori/*
Source: *developed by the authors*

După ce riscul a fost tratat, probabilitatea, consecinţa şi valoarea riscului rezidual trebuie reevaluate/calculate din nou. La încheierea pro-

After the risk has been addressed, the probability, consequence and value of the residual risk needs to be reassessed/recalculated. At the end

cesului de selectare a controalelor, obiectivele şi controalele selectate trebuie comparate cu obiectivele de control şi controalele din *Anexa A ISO/IEC 27001:2013* pentru a se asigura că nu au fost omise controalele necesare.

4. Concluzii

Gestiunea SC constituie un proces continuu, care permite organizaţiei să-şi atingă obiectivele de afaceri stabilite. Deşi este un proces destul de complicat, reuşita lui duce la ridicarea nivelului de maturitate atât al SC, cât şi al organizaţiei în întregime.

Securitatea cibernetică, implementată corect în condiţiile telemuncii în masă şi accesului de la distanţă, presupune o nouă abordare, orientată nu doar pe soluţii tehnice-tehnologice, TIC şi sisteme informaţionale tradiţionale, dar şi către securitatea dispozitivelor mobile, de domiciliu cât şi spre consolidarea securităţii IoT, IoB, cloud etc., inclusiv asupra schimbării sistemelor de management, care ar permite controlul şi monitorizarea eficientă a riscurilor cibernetice.

Acest lucru presupune evaluarea şi/sau actualizarea sistematică a riscurilor pentru fiecare tip de activ informaţional. În acest sens, utilizarea standardelor ISO, e.g. [8], [14], [16], [17], [18] şi a publicaţiilor speciale NIST 800-53 [19] şi/sau a modelelor de ameninţări prestabilite poate simplifica procesul de evaluare iniţială sau de actualizare a riscurilor. Însă oricare ar fi cadrul, modelul sau metodologia selectată de abordare a SC/SI, lupta cu complexitatea şi diminuarea influenţei factorului uman impune automatizarea, în cea mai mare măsură posibilă, pentru monitorizarea continuă a controalelor şi a riscurilor securităţii informaţiei.

Automatizarea operaţiilor rutinare se referă la inventarierea activelor, ameninţărilor şi riscurilor cibernetice; evidenţa dispozitivelor mobile şi/sau de domiciliu, cu acces de la distanţă; evidenţa resurselor informaţionale critice/valoroase pentru afacere, măsurarea nivelului de maturitate a SI, pot spori esenţial nivelul SI printr-o postură de securitate mai puternică şi o productivitate operaţională mai mare.

of the control selection process, the selected objectives and controls should be compared with the control objectives and controls in *Annex A ISO/IEC 27001:2013* to ensure that the necessary controls have not been omitted.

4. Conclusions

CS management is an ongoing process that allows the organization to achieve its established business objectives. Although it is a rather complicated process, its success leads to raising the level of maturity of both CS and the organization as a whole.

Cyber security correctly implemented in the conditions of mass teleworking and remote access requires a new approach, focused not only on technical-technological solution, ICT and traditional information system, but also on the security of mobile devices, home and IoT security, IoB, cloud, etc., including changing management systems, which would allow effective control and monitoring of cyber risks.

This involves the systematic assessment and/or updating of risks for each type of information asset. In this respect, the use of ISO standards, e.g. [8], [14], [16], [17], [18] and NIST 800-53 special publications [19] and/or pre-established threat models can simplify the process. initial risk assessment or update. But whatever framework, model or methodology is chosen to approach CS/SI, the fight against the complexity and diminishing influence of the human factor requires automation as much as possible for the continuous monitoring of controls and information security risks.

Automating routine operations regarding the inventory of cyber assets, threats and risks, the record of mobile and/or home devices, with remote access of critical/valuable information resources for business, measuring the level of maturity of CS, can essentially increase the level of CS through a stronger security posture and higher operational productivity.

Bibliografie/ Bibliography:

Surse digitale accesate la data de 26.03.2021/ All digital sources were accessed on 26.03.2021

1. Website Hacking Statistics in 2020. Updated: September 14, 2020 by Agnes Talalaev. Disponibil https://www.webarxsecurity.com/website-hacking-statistics-2018-february/

2. MILKOVICH, Devon. *15 Alarming Cyber Security Facts and Stats*. https://www.cybintsolutions.com/cyber-security-facts-stats/
3. Quarterly Threat Trends. Mid-Year Updated Threat Report, September 2019. https://mypage.webroot.com/rs/557-FSI-195/images/Threat_Report_Mid-Year_Update_Sept_US.pdf
4. Data Breach Investigations Report. https://enterprise.verizon.com/resources/ reports/dbir; Verizon 2020 Payment Security Report Published October 6, 2020. https://enterprise.verizon.com/resources/reports/2020-payment-security-report.pdf/
5. KOSUTIC, D. *9 Steps to Cybersecurity*. Published by: EPPS Services Ltd, Zagreb, 2012, 80 p. http://www.iso27001standard.com/
6. BRAGARU, T., BRICEAG, V., MALCOCI, V., GALAICU V. *Securitatea informației vis-à-vis de securitatea informațională*. Studia Universitatis Moldaviae, 2(122), 2019. Seria „Științe exacte și economice", ISSN 1857-2073, -p. 38-47
7. ISO/IEC 27000:2018. Fifth edition, 2018-02. Information technology. Security techniques. Information security management systems. Overview and vocabulary.
8. ISO/IEC 27032:2012. First edition, 2012-07. Information technology. Security techniques. Guidelines for cybersecurity.
9. 3 things you need to know about prioritizing-vulnerabilities. https://lookbook. tenable.com/predictive-prioritization/ebook-3-things-to-know-about-prioritizing-vulnerabilities
10. Webroot Reports 2019**.** Hook, line and sinker: Why phishing scams work. https://www.webroot.com/in/en/about/press-room/releases/employees-click-phishing-emails-atwork; COVID-19 Clicks - How Phishing Capitalized on a Global Crises Summary. https://rcpmag.com/whitepapers/2020/11/webroot-covid-19-clicks-how-phishing-capitalized-on-a-global-crises-summary.aspx?tc=page0
11. Payment Card Industry Data Security Standard, v3.2.1, May 2018. https://www.pcisecurity standards.org/document_library/
12. ISO/IEC 27005:2018. Information technology. Security techniques. Information security risk management
13. ISO 31000:2018. Risk management – Guidelines
14. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements
15. BRICEAG, V., BRAGARU, T. Evaluarea securității informației organizației în baza unui model de maturitate. *Materialele Conferinței științifico-practice internaționale „Teoria și practica administrării publice"*. Chișinău, AAP, 22 mai 2020, pp.248-252, ISBN 978-9975-3240-9-0
16. ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls
17. ISO/IEC 27017:2015. Information technology. Security techniques. Code of practice for information security controls based on ISO/IEC 27002 for cloud services
18. ISO/IEC 27033:2012-2016. Information Technology. Security techniques. Network security (part 1-6)
19. NIST SP 800. Information technology laboratory. NIST: 21.05.2018. https://www.nist.gov/ itl/nist-special-publication-800-series-general-information/
20. CVE (Common Vulnerabilities and Exposures) https://cve.mitre.org/