An Approach for Information Security Risk Assessment in Cloud Environments

Livia Maria BRUMĂ
Economic Informatics Doctoral School
The Bucharest University of Economic Studies, Bucharest, Romania
liviabruma@rocketmail.com, brumalivia@gmail.com

Cloud technology has revolutionized the way computational resources are accessed, offering benefits that have led to widespread adoption. The risk of losing important data is one of the reasons why some organizations do not adopt the migration to a public cloud or adopt the partial migration of information that is not critical. The process of risk assessment should be done since the initial stage of a project and become a continuous process. It is an essential process that help management structure to take strategic decision about security mechanisms needed to be implemented to avoid information leaks and about the costs and impact of unexpected events. This paper presents the process of information security risk assessment as well as the importance of knowledge of the associated risks. The paper also proposes a model for determining risk of data security according to their importance for the organization, which provides an overview of vulnerabilities and their real impact on assets. Furthermore, the proposed model helps organizations to choose the right methods to ensure the optimal level of security, in line with operational requirements and critical information.

Keywords: *Cloud computing, Risk assessment, Information security, Security assessment, CVSS metrics.*
DOI: 10.24818/issn14531305/24.4.2020.03

1 Introduction

Cloud technology has revolutionized the way we access computing resources, giving users certain benefits that have led to the widespread adoption of this new technology. Migration to cloud has been adopted by information society, whose citizens can be considered digital citizens - those who use the internet regularly and efficiently [1]. The main advantages of cloud technology can be defined using the NIST (National Institute of Standards and Technology) definition: to allow access as quickly as possible, in a simple way, through the network connection, to a wide range of computing resources, storage and infrastructure with minimum effort for management and maintenance or interaction with service providers [2]. The architecture of cloud consists of diversified technologies, interconnected through the same infrastructure, including networks, databases, operating systems, virtualized equipment etc., which can be vulnerable to cyber-attacks if adequate security controls are not implemented [3]. Unlike traditional IT (Information Technology) technologies, the responsibility for cloud security is shared between the customer and the provider, depending on the SLA (Service Level Agreement. The cloud service provider AWS (Amazon) separates the responsibility for security management as follows: the customer is responsible for security ‘in’ the cloud and the provider for security ‘of’ the cloud [4].

Ensuring an optimal level of data security means protecting the main properties of data: confidentiality, integrity and availability (CIA). The main requirement that organizations must take into consideration when had to choose security controls is to maintain the operational capacity of the services provided. After all, data security is a necessary process to protect the assets used by organizations to achieve their objectives (financial, educational, production), not the main objective. The need for this laborious process of data security emerges from risk analysis, through which potential gaps within the organization can be identified. The process of assessing the security risk of an organization is based on identifying, controlling and minimizing the impact of uncertain events. As the risk cannot be completely eliminated, the objective of the risk management program is to reduce the risk of an event occurring to a residual value accepted by the management of the organizations [5]. Although there are many definitions and mathematical formulas for calculating the value of risk, depending on the analyzed field, this process has a high degree of subjectivity, especially in the case of approaching qualitative values. The risk of an event to be considered a security incident is conditioned by the likelihood that a threat can successfully exploit vulnerabilities in the system.

Although at first sight, the idea of calculating a value to express the risk of an event may seem simple, the number of successful cyber-attacks is increasing, therefore, may be some problems in current methods of calculating risk values or about applied security controls. One of the causes that may underlie risk analysis that do not reflect reality is the perception of the people performing the risk analysis. In some situations, people are tempted to lessen the consequences that may occur as a result of an event, if they are directly interested in using a particular service involved in risk analysis or if they do not have enough information about the possible consequences [6]. It is well known that we should not enter personal data on certain platforms that do not use digital certificates to encrypt traffic, but this does not prevent us from doing so when we are interested in the products or services offered.

The knowledge about vulnerabilities of the systems is a defining step in the risk assessment process. In order to be able to discover and remedy vulnerabilities before they can be exploited by threats, some framework models have been implemented to ensure standardization in their reporting and characterization. Common Vulnerability Scoring System (CVSS) is a model through which vulnerabilities in hardware, software or firmware systems are organized, measured and characterized according to certain metrics that provide information about severity and impact over systems in case they are exploited. [7] Although most CSPs (Cloud Service Provider) have performed a risk analysis, it does not replace, but only complements the organization's internal risk analysis, all the more so as the data is its responsibility.

This paper is organized as follows: ❶ A review of information security risk assessment process, based on different international standard; ❷ proposing a model for determining the risk to data and information security according to their importance for the organization, which provides an overview of their vulnerabilities and real impact; ❸conclusions.

2 The risk management process

The security risk management process is based on identifying, controlling and minimizing the impact of uncertain events. As the risk cannot be completely eliminated, the goal of the risk management program is to reduce the risk of an event occurring to a residual value accepted by management layer. There are many definitions and mathematical formulas for calculating the risk value, both qualitatively and quantitatively, depending on the field in which it is analyzed. A general definition of risk can be stated as the probability of a security incident occurring, conditioned by the probability of a threat occurring and the likelihood that the threat can successfully exploit vulnerabilities in the system.

The risk assessment process requires at least the following elements to be known and analyzed regardless of the field - financial risk, information risk etc.:

(1) A - asset value

(2) T - severity and likelihood of threats;

(3) V - the type and extent of vulnerabilities and likelihood that a threat may exploit them;

(4) I - the possible impact of the damage if an attack is successful.

Thus, risk can be considered as a function of the elements above [5]:

$$\text{RISK} = f\,(A, T, V, I)$$

In order to facilitate the implementation and objectivity of the risk management process, certain international standards and guidelines have been developed to ensure quality, trust and safety for their customers. There are multiple models for performing risk management, such as the standards in the ISO / IEC 27000 family - *Information security management*, the COBIT 5 standard developed by ISACA, special publications NIST SP 800-30 *Rev. 1 Guide for Conducting Risk Assessments* etc. Each one of these standards provides a different process for risk assessment, to help organizations to evaluate the real value of residual risk. In table 1 are presented the stages of the risk management process according to three international standards:

Table 1. Stages in the risk management process [5]

Standard	**ISO/IEC 27005:2011 (E)**	**BS 7799-3:2006**	**NIST SP 800-30**
Stages	Context establishment	Organizational context	
	Risk assessment	Risk assessment	Risk assessment
	Risk treatment	Risk treatment and management decision making	Risk mitigation
	Risk acceptance		
	Risk communication and consultation	Ongoing risk management activities	
	Risk monitoring and review		Evaluation and assessment

As can be seen from Table I, the steps in the risk management process differ depending on the standard used only at the naming level, in fact, the steps contained in the ISO/IEC 27005:2011 (E) standard are addressed in each of the two standards in the table, at different stages. According to the model used, risk management process may comprise several different steps, the most common being based on the following sequence: ❶risk framing ⇨❷ risk assessment ⇨ ❸ risk response ⇨ ❹ risk monitoring [8].

Ideally, after a risk assessment process and the implementation of security mechanisms that use predictive techniques, a system could reach the state of antifragility. According to Nassim Taleb, systems and organizations can be in three states:

- fragile - systems and organizations that can be easily modified or affected by the action of stressors;
- robust - systems and organizations that can cope with adverse conditions;
- antifragile - systems and organizations that improve their resilience with stress.

Thus, if an organization reaches the state of antifragility, it could avoid events such as *Black Swans*, which are *large-scale, unpredictable and irregular events, with massive consequences, unforeseen by a certain observer* [9]. The purpose of a management process aligned with current technologies, must be able to predict future types of threats in order to adapt the organization so that systems are protected by ensuring business continuity and protect critical assets. In this paper, data and information are considered critical assets. The efficiency of a risk management program depends on the level of knowledge about the relational components that influence risk value - assets, impact, threats and vulnerabilities. Determining the risk that certain security breaches will occur is also a challenge due to the fact that the cloud architecture is not standardized, requiring a specific approach for each cloud instance analyzed [10]. To the same extent, with the maximization of security controls that can bring the value of risk as close to zero as possible, operational problems arise, with security controls becoming effective in reducing risk but inefficient in performing tasks and objectives. Figure 1 illustrates the relationship between the concepts used in risk assessment and how they generate implications in risk value:

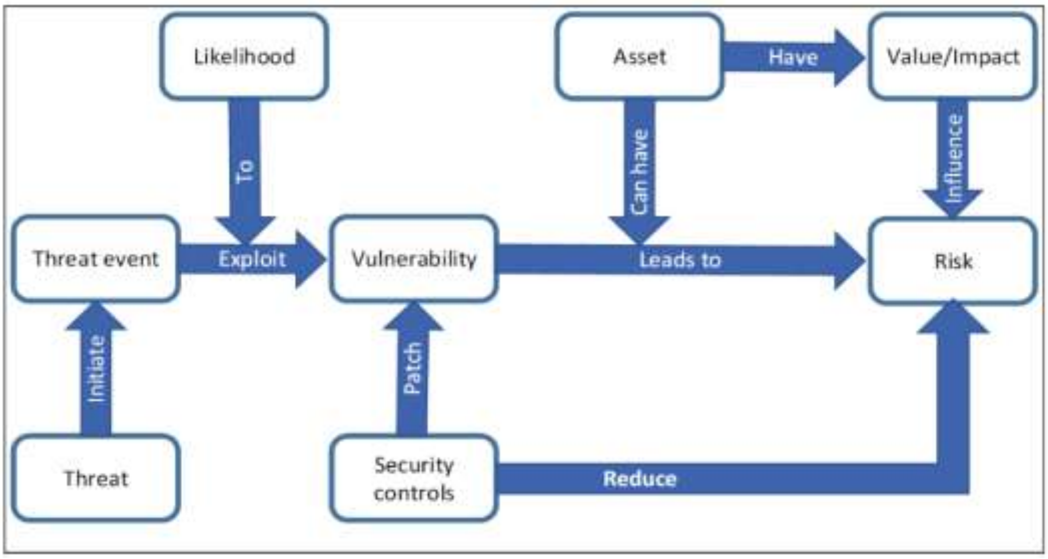

Fig. 1. The relationship between the concepts used in risk assessment

3 Information security risk assessment proposal

The paper proposes a model addressed to the cloud service client (CSC) and involves a detailed risk evaluation based on the elements for which the organization is responsible. Because the shared responsibility model is used, it is necessary to consider the specific cloud elements that are mentioned in the SLA and for which the CSC is responsible for ensuring security. Although CSP may have conducted security assessments and analyzes at the cloud level, an analysis within the CSC that uses the services and knows the degree of confidentiality and importance of certain data, can provide important information in the analysis and evaluation process. Thus, depending on the model chosen by the cloud, IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service), the risk analysis will require the valuation of assets differently, even though central structure is the same.

Figure 2 presents the risk assessment process and the stages in which the CSP should be involved.

Each stage of the risk assessment process is detailed as follows.

A. Context establishment

This stage is a fundamental one, being a stage of defining and planning the risk management within the organization, the residual risk values accepted at the management level as well as the financial impact that the organization can bear to reduce risk. At this stage, basic parameters are defined, which will be the subject of the following stages, risk identification, analysis and mitigation [11]. Also, at this stage, organizations need to consider whether the data that will be migrated to the cloud is subject to certain legislation, so that a certain type of protection is needed for them (personal data, personal identification data, personal information etc.) or if the CSP meets certain international standards that ensure the processing of sensitive data (e.g. ISO / IEC 27018: 2019).

B. Risk evaluation

The second stage involves several sub-stages, which address the main components of risk assessment, identification, analysis and estimation, in the context of data and information security.

B1. System characterization

In order to obtain relevant results for organization's objectives after risk assessment, it is necessary to establish certain assets that will become the core of the risk analysis. For example, a CSC whose main objective is to ensure a level of availability close to 100%, will have a risk analysis that will focus on identifying threats that may jeopardize reaching this threshold. The critical assets of the organization will be the central element around which the risk factors will be analyzed, as the prioritization is the only option in which an accepted residual risk can be obtained at the level of the organization, with a bearable financial cost. Although this task is indisputably of the CSC, certain elements can be found in the SLA signed with the CSP, so that there is a clear delimitation of the tasks and objectives of each entity.

B2. Identifying assets and impact

At this stage, are identified the assets of the organization from the center of the risk analysis, regardless of their nature: tangible assets, such as physical computing equipment and intangible assets, such as information - the main resource in the digital age. The value of the assets directly influences their importance for the organization, implicitly the impact generated by a security event. The analysis of assets provides the needed information to be able to implement the necessary and sufficient protection measures, each of these assets being protected according to its criticality to the organization. For example, we are talking about a waste of resources, economic and functional if we treat all information as if it were restricted or sensitive. Communication with the CSP is essential to be able to evaluate the assets, as there are dependent relationships between the assets managed by the CSC and the CSP. The impact that an event can have on the organization's assets depends on the value of the affected assets.

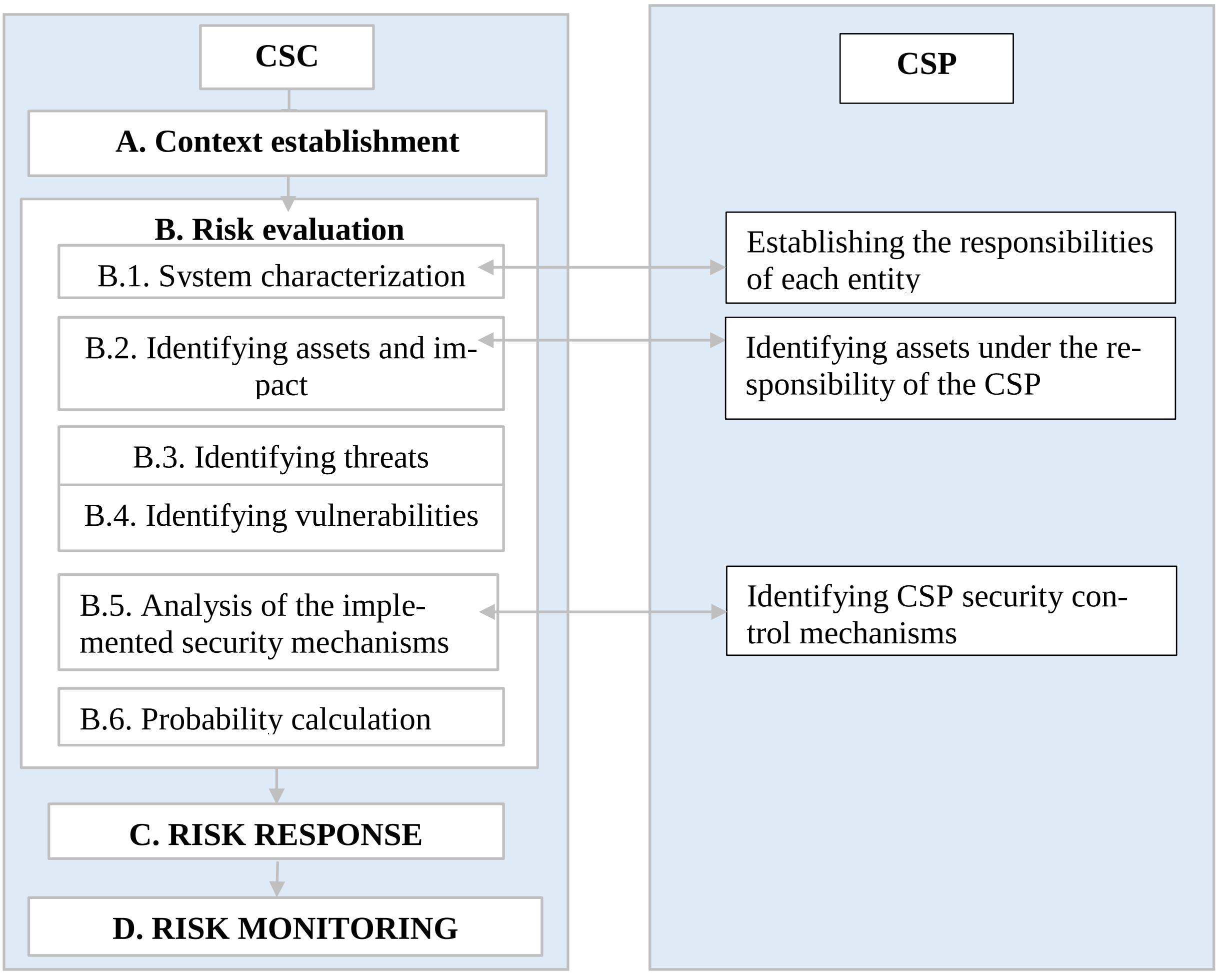
CSC
A. Context establishment
B. Risk evaluation
B.1. System characterization
B.2. Identifying assets and impact
B.3. Identifying threats
B.4. Identifying vulnerabilities
B.5. Analysis of the implemented security mechanisms
B.6. Probability calculation
C. RISK RESPONSE
D. RISK MONITORING
CSP
Establishing the responsibilities of each entity
Identifying assets under the responsibility of the CSP
Identifying CSP security control mechanisms

Fig. 2. The proposed risk assessment process

For the same asset, the loss of different components of the CIA triad has a different impact. For example, losing the integrity of password hashes stored in a database can result in greater losses than losing the availability of the same database for a certain period of time. Thus, determining the impact that certain events can generate on assets is a challenge if this process is not automated, as human errors can occur, intentionally or from the inability to correctly determine the value of the impact.

Detailed knowledge about the critical assets for an organization and the type of provided services is the key component in the process of correctly assigning the impact value. Table 2 shows the most used assets according to certain characteristics.

Table 2. Cloud asset distribution [12]

Responsible	Asset	Primary / Support characteristic	Type
CSP	Datacenter	S	Hardware Asset
	Host/Server	S	Hardware Asset
	Resources	S	Hardware/Software Asset
	Virtual Machine (VM)	S	Software Asset
	Virtual Machine Image (VMI)	P	Information Asset
	Virtual Network	S	Network Asset
	Personal Data of CSC	P	Information Asset
	User Credentials	P	Information Asset
	Data Storage (Files/disk blocks) in the form of SAN/NAS	P	Information Asset
	Services	P	Cloud processes and activities
	Security Logs	P	Information Asset
	Functional Components	P	Cloud processes and activities
	SLA	P	Information Asset
	Cloud Service Management Interface	S	Software Asset
CSC	User/Organization Data	P	Information Asset
	Credentials	P	Information Asset
	Encryption Keys	S	Software Asset
	Functional Components	P	Cloud processes and activities
	Host/Server	S	Hardware Asset
	SLA (Software Level Agreement) (with CSP as well as CTS)	P	Information Asset
	Cloud Service Management Interface	S	Software Asset
	Audit Report	P	Information Asset

The value of assets can be calculated based on their financial value and their importance to the organization. In the case of risk analysis, from the point of view of data and information security, the value of each asset will be calculated according to the data processed, stored or in transit. Thus, each of the parameters authenticity (R_1), integrity (R_2), non-repudiation (R_3), confidentiality (R_4), availability (R_5), and authorization (R_6) will have an assigned value, through which will be obtained the value v (a) of information related to asset.

To find the final value of the assets, the importance of the assets within the infrastructure will also be considered. These can be primary assets or support assets, primary assets having a higher priority in need for security. Thus, depending on the characteristic of being primary or support assets, the value of the assets will be influenced, by multiplying the initial value calculated based on the information parameters, with a factor (x) established by the risk advisor. The value of assets can be determined through a function that considers all the above requirements, as follows:

$$v(a)= f(R_i,x)$$

B3. Identifying threats

Data security threats and events from cloud are in a dynamic process of alignment with the security controls implemented, finding new ways to exploit technical, procedural or human vulnerabilities: unauthorized access to cyber infrastructures, unauthorized modification, deletion or damage of data, cyber espionage, etc. Organizations need to analyze the multiple types of cyber threats (phishing, account hijacking, DoS) and include in the risk response plan those that threaten the security of data and information to prevent causing financial damage, harassment or blackmail. The main actors that generate threats in cyberspace are [13]:

− Cyber terrorists - are focused on disrupting critical services and causing damage to companies, state institutions and critical services in order to harm and destroy them in order to continue their cause;

− Actors sponsored by different nations are known for stealing and filtering intellectual property and sensitive information. The main objective is espionage, theft or any other activity that favors the interests of a particular nation / group of nations;

− Cybercriminals are part of the category of cybercrime whose main purpose is financial gain, through the theft of sensitive and personal data or forcing users to pay certain amounts. Most of the time, after they have taken possession of the money, the data tends to appear on the black market or is sold to the largest bidder;

− Hacktivists - focus on informing citizens by exposing secrets and disrupting certain services / organizations considered to be engaging in unethical or illegal activities. The best-known organization of this kind is WikiLeaks, which publishes non-public documents from information leaks, usually from anonymous sources;

− Malicious people within the organization (insider) are one of the biggest security threats because they possess certain information within the structure and advantages that help them in fulfilling the malicious purpose.

There are numerous studies and reports that analyze the threats and the methods used to attack the cloud, the main threats to data and information security are the following: data breaches, misconfiguration and inadequate change control, account hijacking, insider threat, due diligence, advanced persistent threats (APT). To facilitate the identification of threats in the risk assessment process, it can be used a threat model, that provides a structured picture of vulnerabilities and threats in a cloud system, which can be used to identify possible attacks and establish protection measures against their exploitation [14]. Table 3 presents the STRIDE model, developed by Microsoft, which correlates each possible threat with one of the information characteristics.

Table 3 STRIDE Model

Threat	Spoofing identity (S)	Tampering with data (T)	Repudiation (R)	Information disclosure (I)	Denial of service (D)	Elevation of privilege (E)
Affected Security requirements	Authenticity (R1)	Integrity (R2)	Non-Repudiation (R3)	Confidentiality (R4)	Availability (R5)	Authorization (R6)

The risk advisors will assign values to the security requirements Ri (table 3) according to the needs of the organization. For example, an organization that offers online gaming services, has as its main need the availability of services as well as their authorization, so that the corresponding values are rated higher than confidentiality. At the same time, a banking company needs first and foremost the guarantee of data confidentiality and integrity.

To use these threats in calculating the risk, values were assigned according to the severity of each, in the order of the values given by the CSA (Table 4).

Table 4 Top threats from cloud computing [15]

Threats (T_i)	Value V(j)	Security Responsibility		Stride Model					
		Customer	CSP	S	T	R	I	D	E
Data Breaches (T1)	11	■	■				■		
Misconfiguration and Inadequate Change Control (T2)	10	■			■	■	■	■	
Lack of Cloud Security Architecture and Strategy (T3)	9	■		■	■	■	■	■	■
Insufficient Identity, Credential, Access and Key Management (T4)	8	■		■	■	■	■	■	■
Account Hijacking (T5)	7	■	■	■	■	■	■	■	■
Insider Threat (T6)	6	■		■	■		■		■
Insecure Interfaces and APIs (T7)	5	■	■		■	■	■		■
Weak Control Plane (T8)	4	■			■		■		■
Metastructure and Applistructure Failures (T9)	3	■	■	■	■	■	■	■	■
Limited Cloud Usage Visibility (T10)	2	■	■	■	■	■	■	■	■
Abuse and Nefarious Use of Cloud Services (T11)	1	■	■	■	■	■	■	■	■

For the calculation of the value of threats, the affected security requirements (R1-R6) will also be considered - based on the values assigned by CSC, from table 4, thus, the value of threats to information in the cloud can be calculated based on Vt and Ri:

$$v(T_j)= f(V_j, Ri)$$

B4. Identifying vulnerabilities

The vulnerabilities present in traditional IT systems are also found in cloud architectures, to which are added certain specific vulnerabilities (faulty access control, misconfigured configurations, use of shared resources, supply chain vulnerabilities). There are many databases (owasp.org, mitre.org, vuldb.com) that provide information about the vulnerabilities of operating systems, applications, hardware, etc., their number is growing from year to year. In the Cloud Security Report published by ISC2 in 2019, the main vulnerabilities of the cloud were unauthorized access to resources, insecure interfaces, incorrect configuration of platforms and compromising user accounts. It is important to remember that vulnerabilities in a system that cannot be exploited by threats do represent a risk to the organization, so there is no need to address them.

In order for vulnerabilities to be identified, indexed and analyzed efficiently, the method of setting a value based on the damage they can cause is used, called the Common Vulnerability Scoring System (CVSS) score. For the calculation of these values, certain parameters are used (attack vector, impact on privacy, necessary privileges, etc.) so that each vulnerability will have a CVSS score that can have numerical values contained in [0.10] according to Table 5.

Table 5. CVSS Scores

CVSS Score	0.0	0.1 - 3.9	4.0 - 6.9	7.0 - 8.9	9.0 - 10.0
Rating	None	Low	Medium	High	Critical

The database provided by the National Vulnerability Database, NIST, contains a number of 122,774 vulnerabilities reported between 1999-2020, with a distribution based on scoring according to Figure 3, For the risk calculation, the value used for vulnerabilities v (v) will be the CVSS score indicated in the NIST database.

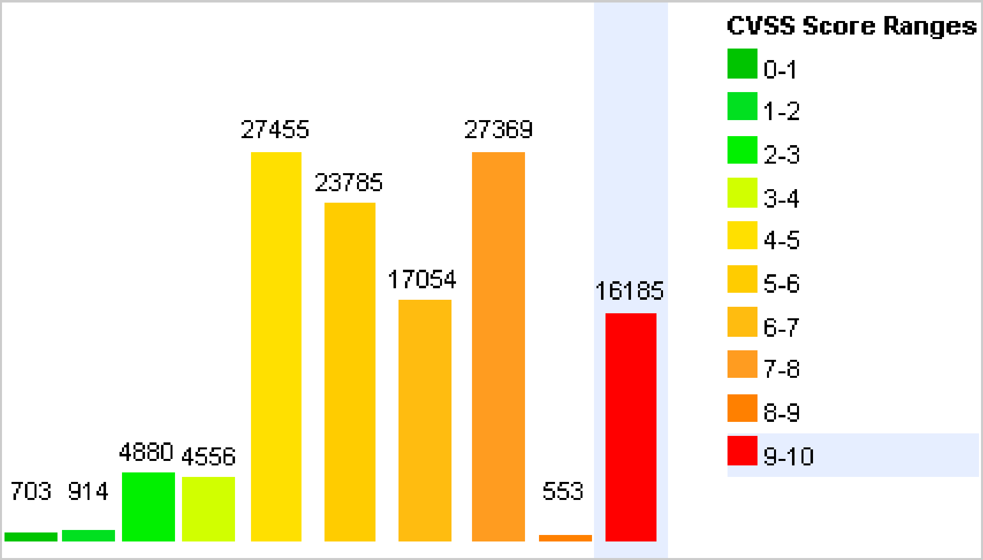

Fig. 3. Vulnerability Distribution by CVSS Scores

B5. Analysis of the implemented security mechanisms

The security controls applied in response to risk have the role of diminishing the probability that incidents will occur. Depending when they are applied, there may be preventive, detection and corrective controls, and depending on the area in which they are applied, there may be three types of security controls [16]:

- Administrative - actions, policies and procedures involved in selecting, developing, implementing and maintaining the security of security measures;
- Physical – used for protecting computer systems, buildings and equipment from unauthorized intrusions and against natural disasters;
- Technical - technical solutions (equipment, security templates), security policies and procedures for the control and protection of information are used.

For the protection of cloud, CSA (Cloud Security Alliance) has published a guide with essential security measures, in 133 domain and addressed to various cloud architectures (SaaS, PaaS, IaaS) in accordance with various international standards for information protection.

The stage of establishing appropriate protection mechanisms is a defining stage, as the financial costs for the implementation of certain devices/services can influence the choice of appropriate equipment. Also, although the purpose of a risk analysis process is to obtain a residual risk as close to zero, operational requirements must prevail, security mechanisms having the role of protecting the key components of information: confidentiality, integrity, availability, authenticity and non-repudiation.

B6. Probability calculation

Determining the value of probability that an incident to take place is an essential step, as it directly influences the value of the risk and all the activities that succeed in this stage. The use of quantitative values provides a higher degree of objectivity to the risk analysis compared to qualitative values, instead a more difficult process is used.

The main problem with probability assignment is that values are considered according to known events. In some cases, the lack of evidence that certain events took place is confused with the lack of evidence that they existed (if no spy has been caught in the last 50 years it does not mean that they did not exist or that the risk does not exist). The probability of an event occurring can be expressed using both percentages and qualitative units. Table 6 presents a series of values for the probability to occur an event that may generate security risks:

Table 6. Distribution of probability values [17]

Qualitative value	Semi-quantitative value		Description
Very High	96-100	10	The error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year.
High	80-95	8	It is very likely that an error, accident or act of nature will occur; or occurs between 10-100 times a year.
Moderate	12-79	5	An error, an accident, or an act of nature may occur; or occurs 1-10 times a year.
Low	5-20	2	An error, accident or act of a nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.
Very Low	0-4	0	It is very unlikely that an error, accident or act of a nature will occur; or occurs less than once every 10 years.

If no security mechanism is implemented, the probability of exploiting a vulnerability can be considered the value of *exploit code maturity* from CVSS parameters [7] . If at the previous stage of the analysis, certain mechanisms meant to protect the assets were identified, the probability value will decrease. Thereby, the value of *exploit code maturity* will be decrease depending on the implemented mechanisms.

Risks can be quantified using the intuition of experts or through specialized tools and methods (Monte Carlo Analysis or Simulation, Decision tree, etc.). There are two methods by which an organization's risk can be assessed: ❶ quantitative assessment and ❷ by qualitative assessment [18]:

❶ this type of assessment assigns concrete values to each risk factor:

– Single Loss Expectancy (SLE) – assesses the loss if an asset is being compromised due to a risk. SLE can be calculated if the value of the asset (AV) and the loss interval (EF) caused by the exploitation of a vulnerability are known, EF having values in the range [0,1]:

$$SLE = AV * EF$$

– Annual Loss Expectancy (ALE) – evaluates the possible loss for an asset over a year. ALE can be calculated using the annual occurrence rate (ARO) and SLE:

$$ALE = ARO*SLE$$

Quantitative assessment is a complex process that can be difficult to be implemented but has the advantage to provide information about risks and asset by financial impact and value and the security level can be better determined based on the CIA elements. [19]

❷ Unlike quantitative assessment, qualitative risk analysis uses relative values associated with risk, such as high, medium and low. Compared to the quantitative method, the qualitative method is more subjective and should be used only when a quantitative analysis is not possible. One of the methods used for this type of analysis is by developing a risk matrix, but the main problem with this matrix is that although they seem to provide an objective risk value, in fact, they only provide certain values that do not always reflect the real situation.

After going through the steps of establishing the value of the information security risk, the management structure of an organization must decide how to deal with the risk issue.

C. Risk response

The elaboration of the risk response consists in determining the ways to reduce or eliminate: threats; the probability of occurrence of the risk, impact, based on the results obtained in the previous stage of risk assessment. Depending on the risk response strategy chosen, certain risks may be [20]: avoided by stopping risk-causing activities, reduced to an acceptable level of residual risk, transferred to an insurance company or accepted - organizations assume losses incurred as a result of an event, without taking any action to prevent it from occurring.

D. Risk monitoring

The last stage of the risk management process aims to monitor the risks to verify that the organization complies with the assessment and implementation of risk response measures and to determine changes in the values of the impact generated by a particular event. [21]

4 Conclusions

Data and information security are one of the main challenges in all technology reference areas, and the cloud computing environment is no exception to this rule. Although there are many methods of data security, cyber security incidents and data loss occur frequently, so innovative and automated methods are needed to minimize the loss and occurrence of security breaches. An information security risk assessment process is required to take place to choose the appropriate security controls to protect the most important asset in today's society: information. The proposed model for risk information and data security assessment provides an overview of vulnerabilities, threat and real impact of security incidents over critical assets - data and information. Also, performing a risk analysis without consulting the CSP will not lead to conclusive results that can provide an overview of informational risks of organizations. At the same time, is highlighted the need for the correct assignment of information properties (CIA, non-repudiation, authorization and authenticity), in future, usage of advanced con-textual detection mechanisms will lead to avoiding human subjectivity.

References

[1] K. Mossberger, C. J. Tolbert and R. S. McNeal, Digital Citizenship - The Internet, Society, and Participation, Massachusetts London, England: The MIT Press Cambridge, 2008

[2] P. Mell and T. Grance, The NIST Definition of Cloud Computing, 2011

[3] L. M. Brumă, Data Security Methods in Cloud Computing, Informatica Economică, vol. 24, nr. 1, pp. 48-60, 2020.

[4] Shared Responsibility Model, AWS Amazon, https://aws.amazon.com/compliance/shared-responsibility-model/, April 2020

[5] S. K. Katsikas, „Risk Management," in Computer and Information Security Handbook, 2009, pp. 605-625.

[6] A. Loske, „IT Security Risk Management in the Context of Cloud Computing," 2015

[7] Common Vulnerability Scoring System SIG, https://www.first.org/cvss/, October 2020

[8] NIST, Managing Information Security Risk Organization, Mission, and Information System View, Gaithersburg, 2011

[9] N. N. Taleb, Antifragile, Random House Trade Paperbacks, 2014.

[10] S. Corbin, The Importance of Application Delivery Standardization in the Cloud, https://www.cloudtp.com/doppler/the-importance-of-application-delivery-standardization-in-the-cloud/, April 2020

[11] C. L. Smith and D. J. Brooks, Security Risk Management, in Security Science, Butterworth-Heinemann, 2013, pp. 51-80

[12] S. Basu, A. Sengupta and C. Mazumdar, A Quantitative Methodology for Cloud Security Risk Assessment, 7th International Conference on Cloud Computing and Services Science, 2017

[13] https://www.redlegg.com/blog/cyber-threat-actor-types, October 2020

[14] A. Gholami și E. Laure, Advanced Cloud Privacy Threat Modeling, Computer Science & Information Technology, 2016

[15] L. M. Brumă, Security Vulnerabilities in Cloud based E-learning, 16th International Scientific Conference "eLearning and Software for Education" DOI: 10.12753/2066-026X-20-024, Bucharest, 2020, pp. 190-197

[16] D. Walkowski, „ f5," F5 Networks, Inc, https://www.f5.com/labs/articles/education/what-are-security-controls, September 2020

[17] Nikolićand, B.; Ružić-Dimitrijević, L., Comparative Analysis of Tw o Risk Assessment Methods in Information System, Proceedings of Informing Science & IT Education Conference, 2013

[18] CompTIA, CompTIA Security+, GTS Learning, 2018.

[19] E. Stroie, Advantages and Disadvantages of Quantitative and Qualitative Information Risk Approaches, Chinese Business Review, vol. 10, nr. 12, pp. 1106-1110, 2011.

[20] https://www.greycampus.com/opencampus/project-management-professional/plan-risk-responses

[21] M. Metheny, „Risk management,” in Federal Cloud Computing (Second Edition), Syngress, 2017, pp. 185-210.

Livia Maria BRUMĂ has graduated the Faculty of Military Electronic and Information Systems of the Military Technical Academy „Ferdinand I” from Bucharest in 2016. She holds a Master Degree in Electronics applied in robotics for security and defense. At present, she works in cyber security domain and she is involved as a Ph.D. student in the Economic Informatics Doctoral School from the Bucharest University of Economic Studies.