Computing and Informatics, Vol. 41, 2022, 1186–1206, doi: 10.31577/cai_2022_5_1186

RISK ASSESSMENT METHOD OF CLOUD ENVIRONMENT

Martin Zbořil

Prague University of Economics and Business
Faculty of Informatics and Statistics
W. Churchill Sq. 1938/4
130 67 Prague, Czech Republic
e-mail: zbom01@vse.cz

Abstract. Cloud technology usage in nowadays companies constantly grows every year. Moreover, the COVID-19 situation caused even a higher acceleration of cloud adoption. A higher portion of deployed cloud services, however, means also a higher number of exploitable attack vectors. For that reason, risk assessment of the cloud environment plays a significant role for the companies. The target of this paper is to present a risk assessment method specialized in the cloud environment that supports companies with the identification and assessments of the cloud risks. The method itself is based on ISO/IEC 27005 standard and addresses a list of predefined cloud risks. Besides, the paper also presents the risk score calculation definition. The risk assessment method is then applied to an accounting company in a form of a case study. As a result, 24 risks are identified and assessed within the case study where each risk included also exemplary countermeasures. Further, this paper includes a description of the selected cloud risks.

Keywords: Cloud computing, cloud services, security, risk assessment, method, case study

Mathematics Subject Classification 2010: 94A99

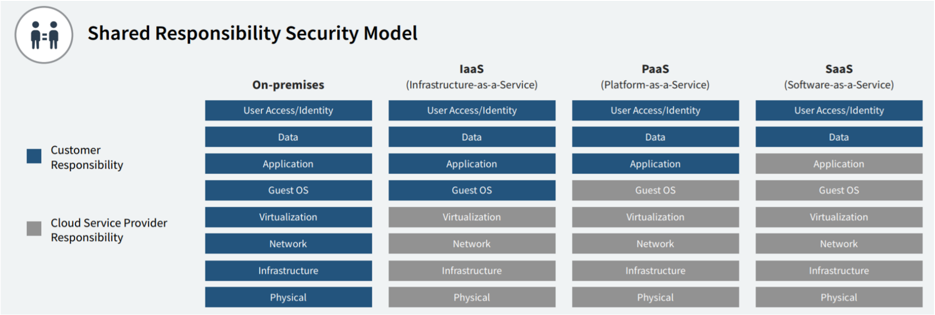
1 INTRODUCTION

Cloud computing technology is leveraged by a vast number of nowadays companies or at least the word "cloud" resonates in their IT strategies and planning. The

COVID-19 situation, where the number of people working from the "home-office" has significantly increased and a small portion of companies have even offered the "work from everywhere" concept to their employees, has shown the importance of cloud computing technology. The technology helped companies to ensure that cloud resources are still fully available for the employees even remotely. The adoption of a cloud solution, however, brings certain security risks that the companies need to take into consideration and manage.

Before talking about the security side of cloud computing, it is important to define what involves this technology. The definition from NIST agency is considered as one of the most respected definition where the cloud computing is defined as: *"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (. . .) that can be rapidly provisioned and released with minimal management effort or service provider interaction."* [1]

NIST further listed five main characteristics that each service needs to fulfill to consider it as a cloud service. Among these characteristics belong *On-demand self-service*, *Broad network access*, *Resource pooling*, *Rapid elasticity* and *Measured service*. The publication further describes two fundamental models: service and deployment model. The service model refers to the scope of provisioned components and consists of Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). The service model and what responsibilities lay on the customer's side and provider's are shown in Figure 1. The second one, the deployment model, deals with the approach how the services are provided to the clients. All the characteristics and both models are described in [1].



Shared Responsibility Security Model

■ Customer Responsibility

□ Cloud Service Provider Responsibility

On-premises	IaaS (Infrastructure-as-a-Service)	PaaS (Platform-as-a-Service)	SaaS (Software-as-a-Service)
■ User Access/Identity	■ User Access/Identity	■ User Access/Identity	■ User Access/Identity
■ Data	■ Data	■ Data	■ Data
■ Application	■ Application	■ Application	□ Application
■ Guest OS	■ Guest OS	□ Guest OS	□ Guest OS
■ Virtualization	□ Virtualization	□ Virtualization	□ Virtualization
■ Network	□ Network	□ Network	□ Network
■ Infrastructure	□ Infrastructure	□ Infrastructure	□ Infrastructure
■ Physical	□ Physical	□ Physical	□ Physical

Figure 1. Cloud service model and distribution of responsibilities [2]

Cloud services bring specific security issues that the organizations which adopted the services into their IT environment need to be aware of. The importance of appropriate handling of the cloud security specifics has been growing constantly since the number of organizations that are adopting the cloud services increases every year, as it is evident from many reports. The examples of such reports are

State of Cloud Security 2018 [3], *Cloud Security Report 2018* [4], *Cloud Adoption and Risk Report 2019* [5], *2020 State of the Cloud Report* [6], *Cloud Security Report 2020* [7].

In the case that organizations manage the cloud services in the same way as the security of the traditional on-premise infrastructure, they might confront many severe issues and threats that have the potential to influence the whole business. For that reason, organizations should not underestimate the governing of cloud service security, mainly in relation to their IT environment. The first step that organizations should perform is an analysis of their current IT environment to find the main relevant security gaps/issues. A usual method for this purpose is a risk assessment.

The risk assessment is one part of the whole risk management. This approach is very important for the entire business as it helps to identify the risks that exist in organizations, prioritize them and mitigate them to an acceptable level. The organizations that decided not to manage (inc. identification) their risks are in danger that some of the risks might be exploited and might greatly influence the stability of the organizations [8].

The definition of risk management is defined as: *"Risk management includes the company-wide measurement and supervision of all business risks"* [9]. The International Organization for Standardization issued a detailed standard that focuses on risk management; the particular standard is *ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management* [10]. This standard provides a managerial guideline to risk management and the overview of the defined risk management process is presented in Figure 2.

The risk management process according to the standard ISO/IEC 27005 is divided into six main components. In the first context establishment phase, a risk analyst finds an external and internal context to the risk management, that includes e.g. risk management purpose, scope and boundaries, organization's risk appetite, risk evaluation, and acceptance criteria [10].

The second risk assessment phase is divided into three subphases: risk identification, risk analysis, and risk evaluation. The risk identification determines the possible sources of a potential loss or any other harmful consequence. A risk analyst needs to identify assets, threats, vulnerabilities, existing controls, and potential consequences. The risk analysis phase then requires a determination of the analysis methodology (qualitative, quantitative) and involves assessment of the incident likelihood and determination of the risk level. The risk evaluation phase then focuses on the comparison between the determined risk level against risk evaluation and acceptance criteria [10].

Within the risk treatment phase, the countermeasures and controls are designed for identified risks. In the end, the identified risks along with their severity and designed mitigation actions are presented to the stakeholders. Then, it needs to be decided in cooperation with the stakeholders what risks will be handled and how. The most frequent risk treatment approaches are risk reduction, risk retention (acceptance), risk avoidance, and risk-sharing [10].

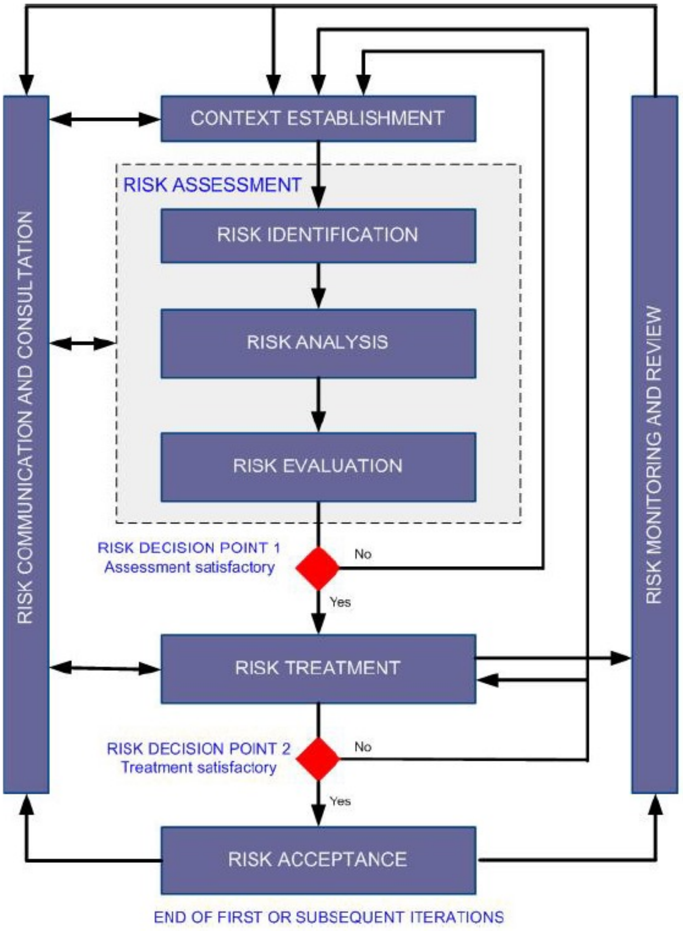


Figure 2. Risk management process based on ISO/IEC 27005 based on [10]

The risk acceptance phase focuses on a formal acceptance and recording of the risks and responsibilities for the decision. Risk communication and consultation is a continuous activity and assures that the entire process of risk management, including the interim results, are correctly communicated and consulted with the stakeholders. Another continuous activity, Risk monitoring, and review, then focus on complete monitoring of the entire process [10].

For the purposes of the risk management that covers the cloud environment, the specifics of the cloud technology in comparison to a traditional environment always need to be considered at the side of cloud service customers (CSC). This important fact was highlighted in [11] where also examples of the specifics relevant for the risk management were presented:

- The owner of the SaaS may not be the same as the owner of the infrastructure where the SaaS runs on.
- Data are not stored at the CSC. Their location is often unidentifiable.
- CSC does not have full control over the service, including its security.
- Resources of cloud service may be scaled up/down, in/out in a short time.
- CSC has a broad access to the cloud service through the internet.

1.1 Literature Review

The risks factors that are associated with the cloud computing relationship were the subject of the research that is described in [12]. The research was placed in the environment of Swedish public organizations. The authors conducted survey research as well as interviews with five experienced IT decision-makers. As the main risk related to cloud computing was identified the security. The additional risks involved e.g. measurement problems, a small number of providers or competencies.

Security concerns and threats of cloud services have been discovered and discussed in many publications. An overview of current cloud computing risks and remedies was gathered in a form of a survey and presented in [13]. This publication also involved a listing of cloud objects that the protection should focus on. Another publication [14] focused on a detailed description of selected cloud risks. Among them were e.g. VM-based malware, botnet hosting, rogue clouds, regulation, or attacks targeting a multi-tenant environment. Identification of risks and threats that affect the decision process of organizations whether to adopt the cloud services or not are the subjects of the publication [15]. Besides, an insight into the organization's perceiving of cloud adoption, and cloud technology, in general, is another part of this publication.

The security issues in the cloud environment were surveyed and presented in [16]. The authors confirmed within their research that security is considered as the top issue within the decision-making process whether to migrate the resources into cloud computing or not. The entire security of cloud solutions is impacted mainly by their two significant characteristics – multitenancy and virtualization. The authors further focused their research on particular security issues related to different types of the cloud service model – Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS).

Many articles are further dedicated to cloud security threats. Cloud threats and attacks aiming at the cloud services are discussed in the publication [17]. Moreover, the authors also provided an overview of the mitigation actions that help to protect the environment, among which are e.g. protecting data in transit, using proper encryption techniques, regular backups, implementation of strong key generation, storage, and management. A further set of threats specific to the cloud environment was presented in [18]. Examples of the discussed threats were vendor lock-in and browser security issues. Many other publications that focus on cloud security threats have been published and discuss similar threats; examples of such publications are [19, 20, 21].

The security of cloud computing solutions is related to the controlling mechanisms that check how the cloud solution is securely implemented and configured. The authors of [22] established a new approach on how to ensure sufficient transparency during the audit of cloud providers. The tool also considers requirements that might be established by the cloud customers towards the cloud providers.

One of the most respected sources of risks identified in the cloud environment is [23] that was issued by the *European Network and Information Security Agency (ENISA)*. This publication includes also identified benefits and catalogs for vulnerabilities and assets relevant to the cloud environment. Security Guidance for Critical Areas of Focus in Cloud Computing [24] defines 14 domains across cloud security; their examples are data security, application security, identity, and access management, virtualization, and compliance. The Cloud Security Alliance organization further published Cloud Control Matrix [25] tool that offers controls linked with the mentioned domains. Moreover, Cloud Security Alliance also developed *Consensus Assessments Initiative Questionnaire* [26] that supports the controls from Cloud Control Matrix with detailed questions.

Many publications focus directly on risk assessment in the cloud environment. Article [27] compares five methods for risk assessment where all the assessment methods leverage the quantitative approach. The methods involve *SecAgreement: A Security Risk Assessment Model, The Mean Failure Cost (MFC), The Mean Failure Cost External (MFCext) and the Mean Failure Cost Internal (MFCint), The MFC Extension model (MFCE), Multi-dimensional Mean Failure Cost Model (M2FC).* The authors of the paper introduced each method and briefly described the main areas where the methods differ. One of the method was previously described in [28]. The authors of the publication provided readers with cybersecurity metrics especially developed for the cloud computing environment. Their model is established on the generic HTC (Hybrid Threat Classification) model and MFC (Mean Failure Cost) function.

Another interesting perspective on how to look on the risk management was presented in [29] where the authors described a risk assessment method for cloud computing that is based on game theory. The authors named the method CRAMM and it is based on the presumption that an attacker and a defender are the players involved into the game. The authors further defined many rules such as that *"Every attack is considered as successful unless there is a security measure for it,"* [29]. The method involves analysis of attacker's strategy dangerous on the asset value and relevant risks. This method might be considered rather as experimental than to be leveraged in enterprises.

The authors of [30] presented a risk assessment method that involves SLA (Service Level Agreement) negotiation, SLA fulfilling, certifications/standards compliance, location information, business resilience, and other criteria that are mostly related to cloud service operation. This shows that the methodology greatly involves measuring of the quality of the cloud service and so performance monitoring is relevant for that; therefore, the establish risk assessment method described in this paper requires active connection to the cloud environment to work properly.

Risk assessment within the environment of cloud providers is a subject of [31]. The authors dedicated their research to establishing a risk assessment framework that would help cloud service providers to assess their own IT infrastructure. As a result, the authors developed Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model that is based on the quantitative risk assessment. For complete performing of the assessment, the supplier security posture assessment and supply chain mappings are necessary. The authors further compared the results of quantitative risk assessments with the results that would be achieved with well-known methods such as CRAMM, ISO 27005, NIST 800-30, OCTAVE Allegro, etc.

The authors of [32] established another risk assessment framework dedicated purely to cloud resources. The perspective of this framework is not in covering the entire IT environment of an organization, but a single application deployed within the cloud. More precisely, the framework targets the design phase of the application since the appropriate design ensures secure and effective operation of the application. The authors incorporated also different types of cyber (cloud) attacks scenarios that might negatively impact the applications.

Research related to risks and cloud computing was conducted also for specialized areas. One of such examples is risk assessment over artificial intelligence-power mobile cloud applications [33]. The authors, however, focused not only on security risks but also on other types such as risks emerging from operating over 5G and 6G. The research involved also the problematics of Android security mechanisms.

1.2 Contribution

This paper focuses on one significant issue in organizations and that is disregarding cloud security specifics when managing the organizations' IT security. The risks might be in a form of insufficient controls, wrong security settings, compliance issues, or others. Moreover, the importance of the correct management of cloud services security is getting even more significant with the mentioned increasing trend of cloud services usage.

The main objective of this paper is to present a developed method of risk assessment over the security of the cloud environment that would help its users and organizations to identify the cloud risks. The current risk assessment frameworks that are designed especially for the cloud environment focus rather on the cloud provider's side. The method described in this paper, however, aims the side of the cloud customer. The literature review also showed that many of the articles provide only an overview of the relevant risks without establishing a complex approach to how to deal with the risk assessment in the cloud environment. This paper offers a risk management method that leverages the predefined cloud risks that were gathered through many relevant sources and risks identified during the security assessment of the organization where 170 security controls are applied and that is described further in Section 2. Such a method is especially useful for companies that do not have sufficient expertise and experience with cloud services and principles.

The established method, furthermore, is based on the internationally respected standard ISO/IEC 27005 and thus, it significantly increases the credibility of the designed method as it is associated with a very high probability to be accepted by potential regulators or some other parties performing IT audit over the cloud customer's environment.

The contribution of this paper also involves a description of the particular application of the cloud risk assessment method on one organization.

2 METHODOLOGY

The author of this paper initiated the research with a detailed analysis of the theoretical background related to cloud computing and risk management; among the selected examples belong *The NIST Definition of Cloud* [1] or *ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management* [10]. Then, the author followed with a literature review of publications with a focus on the ones that relate to cloud security and risk management in the cloud environment. As a result, the author performed a synthesis of the outputs that arose from the theoretical background and the literature review. These results served for the design of the risk assessment method for the cloud environment that is described in detail in Section 2.1.

The designed risk assessment framework was then applied and verified through a case study. The presented case study includes a detailed calculation of risk scores and a description of the selected risks. The established risk assessment method was utilized in praxis at a real organization. The IT infrastructure and identified risks were exactly the ones that are published in this paper. Nevertheless, the description of the company is anonymized as was requested by the company itself. The organization along with its IT infrastructure is described in Section 3.1 and the results of the case study are presented in Section 3.2.

2.1 Risk Assessment Method

The proposed risk management method is based on the risk management process defined by the ISO/IEC 27005 standard [10] and is presented in Figure 2.

The designed risk management method incorporated all phases of the standard ISO/IEC 27005 that were already described in the Introduction. Further, the designed process added:

Cloud security assessment – The cloud risk assessment method is contained in the entire Cloud Security Governance Framework that is designed and established by the author of this paper as a topic (result) of his Ph.D. thesis. The framework has not been yet published as a whole and therefore, cannot be

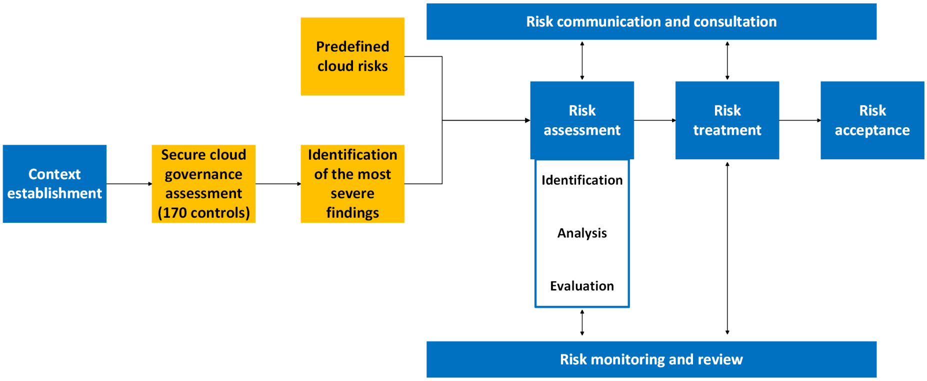

Risk communication and consultation
Predefined cloud risks
Risk assessment
Risk treatment
Risk acceptance
Context establishment
Secure cloud governance assessment (170 controls)
Identification of the most severe findings
Identification
Analysis
Evaluation
Risk monitoring and review

Figure 3. Developed risk management processed based on the ISO/IEC 27005 standard [10]

referenced. The framework consists of 170 controls that aim to the cloud environment of the organizations. Multiple frameworks exist for the cloud environment, however, they are mostly focused on the cloud service providers' side; e.g. Cloud Computing Compliance Controls Catalog (C5) developed by Bundesamt für Sicherheit in der Informationstechnik, Cloud Capability Matrix (CCM) developed by Cloud Security Alliance. For that reason, the author developed a framework that focuses on the cloud service customers' side. The controls from the framework were established based on the detailed analysis of ten artifacts (frameworks/standards/regulations), qualitative research (in-depth interviews with four cloud security specialists), and the author's vast experience in the field of cloud security.

Identification of the most severe findings – analyses of the security assessment results where the most severe findings that need to be remediated are transformed into risks.

Predefined cloud risks – list of predefined cloud risks that are presented below.

This risk assessment method offers its users a list of predefined risks that simplifies the identification phase. In total, the list contains 36 cloud risks divided into four domains: policy and organizational, technical operation, technical system, legal. The predefined risks are presented in Table 1. The risks were identified based on [23, 24, 34].

The scoring methodology was based on the exemplary scoring present in the ISO/IEC 27005 where the score level (SL) uses asset value, vulnerability severity, and the probability of threat occurrence:

$$SL = \text{Asset} \times \text{Vulnerabilities} \times \text{Threat}.$$

Domain	**Identified Risks**
Policy and organizational	R.P1 Vendor lock-in, R.P2 Technology lock-in, R.P3 Loss of governance, R.P4 Internal compliance challenges, R.P5 External compliance issues, R.P6 Cloud service termination/failure, R.P7 Cloud provider acquisition, R.P8 Failure of supply chain, R.P9 Insufficient performance and availability of services, R.P10 Problem of unique specification of service provider, R.P11 Service provider limiting information disclosure, R.P12 Difference between work important matter of use company and cloud service provider specification, R.P13 Insufficient fulfilling service level agreement, R.P14 Loss of business reputation due to co-tenant activities, R.P15 Intellectual property theft
Technical operation	R.TO1 Resource exhaustion (under/over provisioning), R.TO2 Cloud provider malicious insider, R.TO3 Intercepted data in transit, R.TO4 Data leakage on up/download, R.TO5 Conflicts between customer hardening procedures and cloud environment, R.TO6 Impact of when data of other cloud customers are seized, R.TO7 Incomplete/disrupted backups, R.T08 Unavailable service, R.T09 Unauthorized access, R.T10 Loss of control
Technical system	R.TS1 Isolation failure, R.TS2 Management plane compromised, R.TS3 Insecure data deletion, R.TS4 DDoS, R.TS5 Economic DoS, R.TS6 Insufficient security of encryption keys, R.TS7 Malicious probes or scans, R.TS8 Service engine compromised, R.TS9 Insufficient interoperability with local systems, R.TS10 Incomplete/insecure data deletion, R.TS11 Insecure/inappropriate handling of data by service provider, R.TS12 Insufficient logs, R.TS13 Unavailability of backups, R.TS14 Misconfigured cloud services, R.TS15 Insecure communication
Legal	R.L1 Subpoena, e-discovery, R.L2 Jurisdiction changes, R.L3 Insufficient data protection, R.L4 Licensing issues, R.L5 Contract breaches

Table 1. Predefined risks for risk assessment of a cloud environment

In comparison to the standard, the author of this risk management method adjusted the asset, vulnerability, and threat values to provide larger granularity. The possible values of each of these components are:

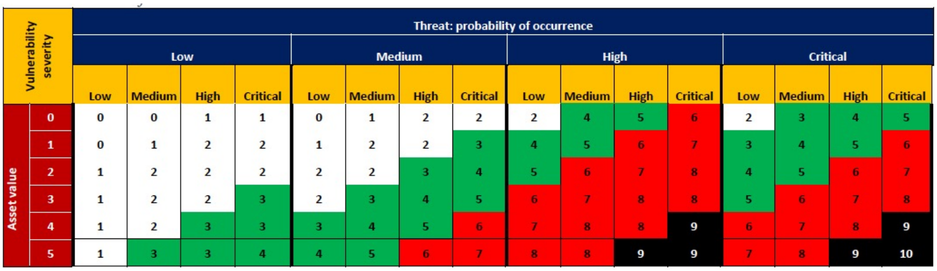
- Asset value $\in \{0, 1, 2, 3, 4, 5\}$, where 0 is the lowest and 5 is the highest.
- Vulnerability severity $\in \{\text{Low}, \text{Medium}, \text{High}, \text{Critical}\}$.
- Probability of threat occurrence $\in \{\text{Low}, \text{Medium}, \text{High}, \text{Critical}\}$.

The score level of risk is then calculated according to Figure 4.

The score might have the values:

$$SL \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

The lowest value 0 presents the risk with the lowest impact, and contrariwise, the highest value 10 is linked with the risks with the highest impact. The final risk severity is determined as:



Vulnerability severity		Threat: probability of occurrence															
		Low				Medium				High				Critical			
		Low	Medium	High	Critical	Low	Medium	High	Critical	Low	Medium	High	Critical	Low	Medium	High	Critical
Asset value	0	0	0	1	1	0	1	2	2	2	4	5	6	2	3	4	5
	1	0	1	2	2	1	2	2	3	4	5	6	7	3	4	5	6
	2	1	2	2	2	2	2	3	4	5	6	7	8	4	5	6	7
	3	1	2	2	3	2	3	4	5	6	7	8	8	5	6	7	8
	4	1	2	3	3	3	4	5	6	7	8	8	9	6	7	8	9
	5	1	3	3	4	4	5	6	7	8	8	9	9	7	8	9	10

Figure 4. Calculation of risk score

- Low – score level $\in \{0, 1, 2\}$,
- Medium – score level $\in \{3, 4, 5\}$,
- High – score level $\in \{6, 7, 8\}$,
- Critical – score level $\in \{9, 10\}$.

According to the calculated risk severity, the risk treatment approach is recommended to each identified risk. Risk avoidance is omitted in these recommendations since this action is the most dependent on the unique situation of the company. The recommended actions are determined as follows:

- Low risk – Risk retention,
- Medium risk – Risk retention, reduction, sharing,
- High risk – Risk reduction, sharing,
- Critical risk – Risk reduction.

3 RESULTS

This main chapter is divided into two sections. Section 3.1 contains a description of the company that is used within the case study. The following Section 3.2 describes selected risks and a list of all identifed risks. Each risk is also linked with the calculated score and the recommended treatment.

3.1 Case Study – Company Environment

This paper operates with an accounting company in which the IT environment consists of both on-premise and cloud components. The organization's environment besides traditional on-premise assets contains also multiple cloud services deployed as Software-as-a-Service and Infrastructure-as-a-Service. This cooperation of the on-premise and cloud environments is a common set-up in organizations. The ratio and criticality of the components that run in each environment depend only on the appetite and needs of the particular organizations. The decision of whether to implement cloud services and what part of their infrastructure put to the cloud must be carefully considered. Organizations need to take into consideration all benefits and drawbacks of both approaches (e.g. general higher savings with cloud services, storing organizations' critical data at cloud provider).

The company (hereafter also referred to as "subject") that is assessed in this case study offers accounting and tax services to its clients. In total, the company has around 50 employees where approximately half of them work from home-office and half of them work from the company's office. The employees also often go to clients where they need to remotely connect to the internal systems.

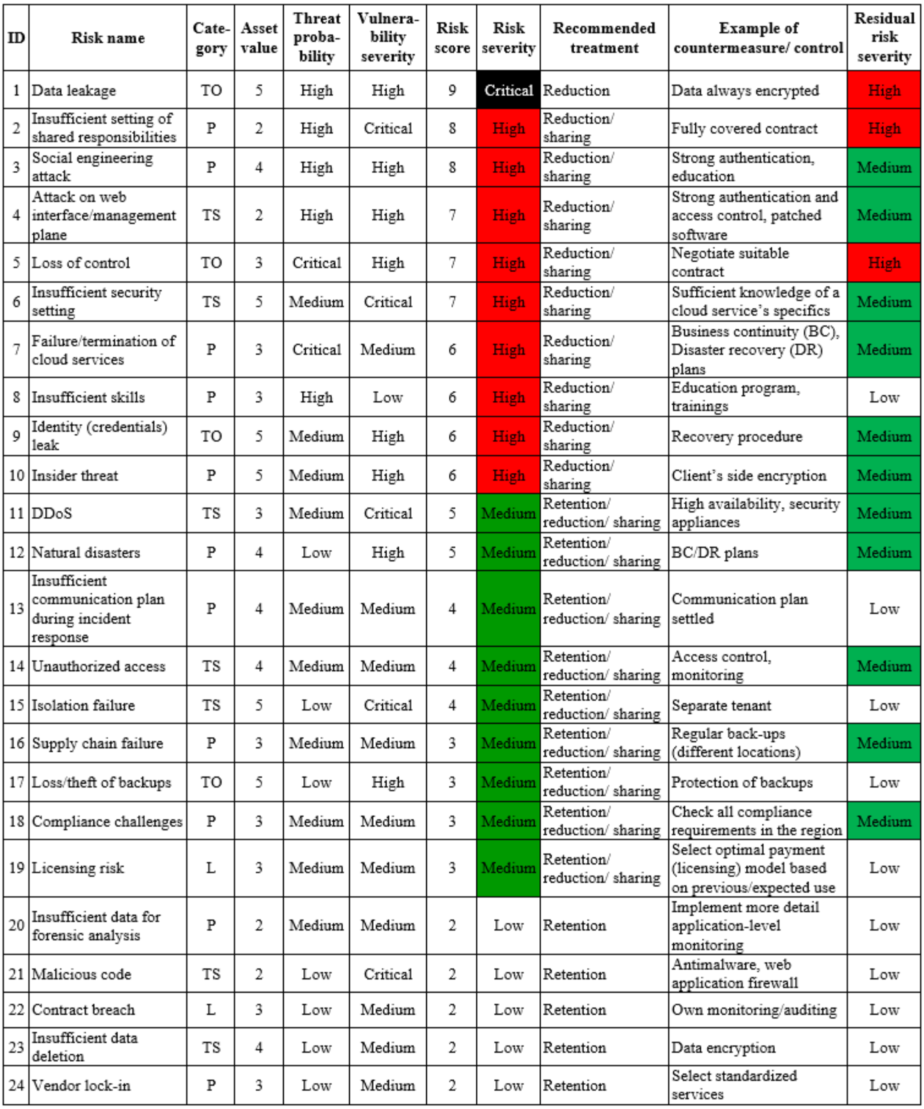
The company has implemented both traditional on-premise systems and cloud services. The on-premise systems cover mainly accounting and tax applications, Windows Office applications and infrastructure assets (servers, networks, databases, etc.) including their management tools (e.g. network assets). The cloud services present mainly Google Apps platform that includes e.g. an email client and storage (Google Drive) where employees may store and share files. Further, the cloud services are used also for CRM (Customer Relationship Management) applications; this particular application is delivered by a local start-up company. Lately, the company started to use also the security tool (McAfee ePO) which includes a web platform for management and analysis. The company further uses users within Google Cloud Platform for testing purposes (testing environment for simulating the local infrastructure). All the cloud services are provided as Software-as-a-Service solutions except for the testing environment that is Infrastructure-as-a-Service.

Based on the interviews with the company representatives, 9 assets related to cloud risks were identified as significant. The company does not use any asset value evaluation scale. For that reason, the asset value was assessed according to the scale from the used risk assessment method (values from 0 to 5). As a result, customer data, customer trust, HR data and service delivery belong among the primary assets. The supportive assets include IT assets, credentials, cloud services management interface/API and user directory.

3.2 Case Study – Risk Assessment

During the risk assessment, overall 24 risks related to cloud services were identified. The risks are composed of 1 critical, 9 high, 9 medium and 5 low risks. The following paragraphs include a detailed description of all the critical and high risks, plus two selected medium risks. The whole list of risks along with the score calculation and severity is contained in Figure 5.

The analysed company decided that countermeasures and controls need not be designed for risks with Low severity. The decision was done upon the recommendation based on the risk method. The reason is that these risks have the minimum potential for influencing the company so they might be accepted. For the rest of the risks, particular actions are designed to mitigate the risks. The examples of these countermeasures and controls are listed also in Figure 5. This figure includes the residual risk severity after applying the mitigation actions.



ID	Risk name	Cate-gory	Asset value	Threat proba-bility	Vulnera-bility severity	Risk score	Risk severity	Recommended treatment	Example of countermeasure/ control	Residual risk severity
1	Data leakage	TO	5	High	High	9	Critical	Reduction	Data always encrypted	High
2	Insufficient setting of shared responsibilities	P	2	High	Critical	8	High	Reduction/ sharing	Fully covered contract	High
3	Social engineering attack	P	4	High	High	8	High	Reduction/ sharing	Strong authentication, education	Medium
4	Attack on web interface/management plane	TS	2	High	High	7	High	Reduction/ sharing	Strong authentication and access control, patched software	Medium
5	Loss of control	TO	3	Critical	High	7	High	Reduction/ sharing	Negotiate suitable contract	High
6	Insufficient security setting	TS	5	Medium	Critical	7	High	Reduction/ sharing	Sufficient knowledge of a cloud service's specifics	Medium
7	Failure/termination of cloud services	P	3	Critical	Medium	6	High	Reduction/ sharing	Business continuity (BC), Disaster recovery (DR) plans	Medium
8	Insufficient skills	P	3	High	Low	6	High	Reduction/ sharing	Education program, trainings	Low
9	Identity (credentials) leak	TO	5	Medium	High	6	High	Reduction/ sharing	Recovery procedure	Medium
10	Insider threat	P	5	Medium	High	6	High	Reduction/ sharing	Client's side encryption	Medium
11	DDoS	TS	3	Medium	Critical	5	Medium	Retention/ reduction/ sharing	High availability, security appliances	Medium
12	Natural disasters	P	4	Low	High	5	Medium	Retention/ reduction/ sharing	BC/DR plans	Medium
13	Insufficient communication plan during incident response	P	4	Medium	Medium	4	Medium	Retention/ reduction/ sharing	Communication plan settled	Low
14	Unauthorized access	TS	4	Medium	Medium	4	Medium	Retention/ reduction/ sharing	Access control, monitoring	Medium
15	Isolation failure	TS	5	Low	Critical	4	Medium	Retention/ reduction/ sharing	Separate tenant	Low
16	Supply chain failure	P	3	Medium	Medium	3	Medium	Retention/ reduction/ sharing	Regular back-ups (different locations)	Medium
17	Loss/theft of backups	TO	5	Low	High	3	Medium	Retention/ reduction/ sharing	Protection of backups	Low
18	Compliance challenges	P	3	Medium	Medium	3	Medium	Retention/ reduction/ sharing	Check all compliance requirements in the region	Medium
19	Licensing risk	L	3	Medium	Medium	3	Medium	Retention/ reduction/ sharing	Select optimal payment (licensing) model based on previous/expected use	Low
20	Insufficient data for forensic analysis	P	2	Medium	Medium	2	Low	Retention	Implement more detail application-level monitoring	Low
21	Malicious code	TS	2	Low	Critical	2	Low	Retention	Antimalware, web application firewall	Low
22	Contract breach	L	3	Low	Medium	2	Low	Retention	Own monitoring/auditing	Low
23	Insufficient data deletion	TS	4	Low	Medium	2	Low	Retention	Data encryption	Low
24	Vendor lock-in	P	3	Low	Medium	2	Low	Retention	Select standardized services	Low

Figure 5. Risk register of identified risks related to cloud services

The table also provides information regarding categorization of each risk. Precisely, the the category is represented by its abbreviation in a separate column. The possible categories correspond to Table 1: Policy and organizational (P), Technical operation (TO), Technical system (TS) and Legal (L).

Data leakage. The Google Apps environment is not configured according to the security best practices. The identified source of the discrepancy is that when the environment was deployed, the company's administrators had not required skills and experience with Google Apps. Another source is insufficient maturity of internal processes and policies related to the usage of Google Apps by employees as there is not defined currently, what are the responsibilities of employees and what is restricted from. As a result, employees may share data through Gmail and Google Drive without any process or technical restrictions. Further, the company has no data protection mechanism, such as DLP (Data Loss Prevention).

Insufficient setting of shared responsibilities. The accounting company does not have clearly defined responsibilities with the cloud providers. Their contracts are on too much general level. Regarding the Google cloud services, it is obvious that the negotiation with such a huge provider has merely no chance to adjust the contract to the accounting company's requirements. A similar situation is with the McAfee ePO security tool. However, the contract should be relatively easily negotiated with the provider of the CRM system as it is a local start-up.

The issues are mainly the blank spots in the contract, and in the management of the services, where it is not clearly defined who is responsible for certain activities, whether it is the cloud provider or the accounting company. Examples of such insufficiencies are responsibilities in case of incidents, forensic activities, data loss, logging configuration and other areas.

Social engineering attack. Social engineering attacks, especially in the form of phishing, are popular among hackers due to their relatively high level of success. The victims usually receive emails that seem like legitimate ones but in reality, the victims are forced to perform some malicious actions such as login into a counterfeit website and thus sending the credentials to the hackers or downloading files that contain malicious malware. The Google Apps platform provides clients with protection measures that identify and block such malicious emails. The measures are represented e.g. by blocking certain types of files, enabling DMARC policies or automatic blocking of malicious links and files. These measures are not, however, configured within the environment of the accounting company and thus the employees face an increased risk of successful phishing attacks.

Attack on web interface/management plane. Since the cloud services are accessible through internet, they might be usually accessible by anybody in the default setup. Through the web interface/management plane, organizations control the entire cloud infrastructure including virtual machines, databases, network appliances, etc. Therefore, such remote access to the resources presents an increased risk.

The accounting company has not configured access restrictions to the management planes of Google Apps nor the testing Google Cloud Platform. Within the current setup, the management planes are accessible all around the world. The company should consider implementing the restrictions, to enforce the access only from e.g. the company network.

Loss of control. Adoption of cloud services unavoidably transpose a certain level of control from organizations to cloud service providers. Such sharing of responsibilities was described within the service model and shown in Figure 1. The shared responsibility principle means that the cloud service provider fully controls the underlying infrastructure and the cloud service customer for everything built on the top of the provided resources. The consequence is that when organizations wants to be compliant with certain security requirements or standards/regulations, compliant need to be both parts – the environment controlled by the provider and the environment controlled by the customer. This is relevant for all organizations that leverage cloud services. In the case of the accounting company, the risk is highlighted even more at the local startup that operates the CRM system.

Insufficient security setting. Appropriate configuration of the resource is the fundamental step in protection of the IT infrastructure, especially when cloud services are accessible from public internet. During the assessment it was identified that many services are configured insecurely. This might be caused by insufficient knowledge of the administrators or by intended disregarding of security good practices. The deeper analysis showed that the accounting company does not have configuration baselines which would define how exactly the services should be configured. The required configuration might be also controlled or enforced in some cloud services, such as Google Cloud Platform.

Failure/termination of cloud services. Within the cloud model, organizations leverage services that are operated by cloud service providers. This fact also means that organizations in the role of cloud service customers are highly dependent on the providers and that they cannot prevent any failure or termination of the cloud service. The failure might be caused e.g. by hardware issues in data centers, wrongly developed update or insufficient performance of the infrastructure. The provider might also decide to completely terminate the service due to e.g. financial problems.

The accounting company should ensure a proper solution for business continuity. This might involve e.g. keeping backup in the on-premise environment or implementing redundant solution.

Insufficient skills. During the risk assessment, a significant risk in a form of insufficient cloud technology knowledge of administrators was identified. The lack of environmental knowledge results in the insecure configuration of the services.

In the case of the company, this was especially true at the configuration of the Google Apps and Google Cloud Platform. The administrators were not trained and had minimum time to educate themselves for these platforms. At Google Apps, the lack of knowledge/insecure configuration may lead e.g. to sharing data with unauthorized external users, insufficient data protection, missing incident detection mechanisms, not applied email rules. At Google Cloud Platform, among the examples of the impacts might be mentioned public accessibility to the virtual network, not configured logging, unencrypted services and not updated resources.

The McAfee ePO service is an intuitive tool but only for its fundamental operation. The tool offers a large portfolio of advanced capabilities where, however, the administrators need to gain new skills. Then, mainly the incident response activity capabilities might be onboarded into the incident response process.

Identity (credentials) leak. The protection of employees' credentials is crucially important for all organizations. The protection of identities is especially ensured by technical measures and by the secure behavior of employees. The technical measures involve protection against phishing attacks, services that check public databases of leaked accounts, behavioral analysis of users' activities and many others. It was already highlighted that the accounting company misses a sufficient implementation of anti-phishing protection. Plus, during the review it was identified that the employees are not sufficiently educated for secure password management.

Insider threat. The provider of the CRM application is a new and small start-up company. For that reason, the company does not presumably have highly formalized processes, directives and security requirements. A relatively low level of control mechanisms over system administrators and developers was set on the provider's side. The majority of administrators' and developers' outputs are controlled at least through "peer review". This risk might have an impact on confidentiality, integrity and availability of all data in the cloud services. Besides, the risk might indirectly influence the trust of clients if data about the client leaks through the cloud service. One possible solution that the company might take is to send encrypted data into the cloud and do not trust that the provider's security controls are sufficient.

Insufficient communication plan during incident response. Incidents in the cloud environment touch not only the accounting company (cloud customer) but have relevance also to the cloud provider. One of the reasons is that the accounting company does not have all administration operations under its control and needs to interact with the cloud providers to perform some of the actions or gain access to some logs. The company has not established any communication plan with the cloud providers for incident response. The result might be the incident is not remediated when it occurs since the administrators are not able to access required logs and cannot perform remediation actions, and simultaneously the cloud provider is not obliged to perform any action as they are not negotiated.

Supply chain failure. The CRM application is dependent on another external service that is hosted in an unknown data centre. The CRM provider has to rely on its SLA that is agreed between this provider and the provider of the external service. As a result, the subject has no possibility of how it may influence cloud service delivery. The outage of the data centre might have a great impact on the availability of the CRM application. Besides, inconvenient actions of data centre administrators might influence the security of customers' data. The provider of the data centre has not delivered any certification or another statement declaring the service level. Although this provider states that the service recovery is done up to 24 hours, no formalized evidence or testing is provided. The main recommendation for the subject is to perform regular back-ups of all data and store them in a different location.

4 DISCUSSION

The correct configuration of cloud services should never be underestimated and disregarded in the management of IT infrastructure. Otherwise, many security risks might occur and be exploited in organizations. Within the case study, data leakage, insufficient setting of shared responsibilities, social engineering attack, and data protection were identified as the most severe risks in the environment of the accounting company. As it is obvious, such risks might influence companies in many areas, from the availability of its systems to the loss of data.

To eliminate the risks, protect the company's environment and ensure an effective operation of the company's assets, it is important to remediate risks in both technical and process areas. Even though the technical risks might be remediated, if the processes in the company are not established correctly, the unmanaged/unrestricted activities of the employees will lead the cloud resources into an incorrect state. Nevertheless, all exploited risks bring a financial loss to companies where the only questions are in what form the financial loss comes and what is the amount of it.

For companies that plan to adopt cloud services or have already implemented them, it is always cheaper and more effective to mitigate the risks in the early phases even though it requires more resources and additional work than to leave the mitigation to the later phases. Mitigation of the risks is an important step, however, without proper identification of them, the mitigation is not effective.

The presented method offers a solution that facilitates its users with the identification of cloud risks. With the usage of the predefined risks and detailed controls that are present in the security assessment tool, all the risks related to the cloud environment should be identified.

5 CONCLUSION

The main objective of this paper was to present a developed risk assessment method for the cloud environment. The method was applied in the form of a case study based on an accounting company with both cloud and on-premise infrastructure. In total, 24 security risks were identified in the case study. At each risk, the asset value, threat probability, vulnerability and total risk score/severity were defined. Besides, recommended treatment and examples of relevant countermeasures/controls that support mitigation of the risks have been specified. Future research in the domain of cloud security might focus multiple criteria decision making to help select the appropriate cloud service model for an observed company. Besides, another option includes the focus strictly on the cloud adoption phase.

Acknowledgement

The paper was written with the support of the specific project IG409031 "The role of internal audit in the context of COVID-19 and increased information security risks" granted by the Prague University of Economics and Business, the Faculty of Informatics and Statistics.

REFERENCES

[1] Mell, P.—Grance, T.: The NIST Definition of Cloud Computing. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2011, doi: 10.6028/NIST.SP.800-145.

[2] Davidson, M. A.—Jensen, G.—Buffomante, T.—Ahmed, L.—Jensen, B.—Cahill, D.: Oracle and KMPG Cloud Threat Report 2019: Defining Edge Intelligence: Closing Visibility Gaps with a Layered Defense Strategy. Oracle and KPMG, 2019, https://www.oracle.com/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf.

[3] Patel, V.—Casey, N.—Chronis, P.—Kaur, G.—LaRosa, V.—Panico, M.—Ruffalo, M.—Zacharias, J.: State of Cloud Security 2018. Cloud Security Alliance, 2018, https://downloads.cloudsecurityalliance.org/assets/research/geab/GEAB-State-of-the-Cloud-2018.pdf.

[4] 2018 Cloud Security Report. Crowd Research Partners, 2018, https://crowdresearchpartners.com/wp-content/uploads/2018-Cloud-Security-Report.pdf.

[5] Cloud Adoption and Risk Report 2019. McAfee, 2018, https://mscdss.ds.unipi.gr/wp-content/uploads/2018/10/Cloud-Adoption-Risk-Report-2019.pdf.

[6] 2020 State of the Cloud Report. Flexera, 2020, https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020.

[7] Cloud Security Report 2020. Cybersecurity Insiders, 2020, `https://www.cybersecurity-insiders.com/wp-content/uploads/2020/08/2020-Cloud-Security-Report-ISC2.pdf`.

[8] Calder, A.—Watkins, S. G.: Information Security Risk Management for ISO 27001/ISO 27002. 3rd Edition. IT Governance Publishing, 2019, doi: 10.2307/j.ctvndv9kx.

[9] Wolke, T.: Risk Management. De Gruyter Oldenbourg, 2017.

[10] ISO/IEC 27005:2018 Information Technology – Security Techniques – Information Security Risk Management. ISO/IEC, 2018, `https://www.iso.org/standard/75281.html`.

[11] Zbořil, M.: Security Risk Management - Cloud Environment. In: Doucek, P., Chroust, G., Oškrdal, V. (Eds.): Strategic Modeling in Management, Economy and Society (IDIMT-2018). Trauner Verlag Universität, Linz, Austria, Schriftenreihe Informatik, Vol. 47, 2018, pp. 367–374.

[12] Hodosi, G.—Haider, A.—Rusu, L.: Risk Factors in Cloud Computing Relationships: A Study in Public Organizations in Sweden. Procedia Computer Science, Vol. 181, 2021, pp. 1179–1186, doi: 10.1016/j.procs.2021.01.315.

[13] Garg, A.—Rathi, R.: A Survey on Cloud Computing Risks and Remedies. International Journal of Computer Applications, Vol. 178, 2019, No. 29, pp. 35–37, doi: 10.5120/ijca2019919139.

[14] Singh, E. G.—Parminderpal: Cloud Computing Risks and Benefits. International Journal of Advanced Research in Computer Science, Vol. 8, 2017, No. 4, pp. 256–259.

[15] Kajiyama, T.—Jennex, M.—Addo, T.: To Cloud or Not to Cloud: How Risks and Threats Are Affecting Cloud Adoption Decisions. Information and Computer Security, Vol. 25, 2017, No. 5, pp. 634–659, doi: 10.1108/ICS-07-2016-0051.

[16] Khoda Parast, F.—Sindhav, C.—Nikam, S.—Izadi Yekta, H.—Kent, K. B.—Hakak, S.: Cloud Computing Security: A Survey of Service-Based Models. Computers and Security, Vol. 114, 2022, Art. No. 102580, doi: 10.1016/j.cose.2021.102580.

[17] Amara, N.—Zhiqui, H.—Ali, A.: Cloud Computing Security Threats and Attacks with Their Mitigation Techniques. 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), IEEE, 2017, pp. 244–251, doi: 10.1109/CyberC.2017.37.

[18] Alshammari, A.—Alhaidari, S.—Alharbi, A.—Zohdy, M.: Security Threats and Challenges in Cloud Computing. 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), IEEE, 2017, pp. 46–51, doi: 10.1109/CSCloud.2017.59.

[19] Singh, A.—Chatterjee, K.: Cloud Security Issues and Challenges: A Survey. Journal of Network and Computer Applications, Vol. 79, 2017, pp. 88–115, doi: 10.1016/j.jnca.2016.11.027.

[20] Coppolino, L.—D'Antonio, S.—Mazzeo, G.—Romano, L.: Cloud Security: Emerging Threats and Current Solutions. Computers and Electrical Engineering, Vol. 59, 2017, pp. 126–140, doi: 10.1016/j.compeleceng.2016.03.004.

[21] Barnwal, A.—Pugla, S.—Jangade, R.: Various Security Threats and Their Solutions in Cloud Computing. 2017 International Conference on Computing, Communication and Automation (ICCCA), IEEE, 2017, pp. 758–764, doi: 10.1109/CCAA.2017.8229923.

[22] Ismail, U. M.—Islam, S.: A Unified Framework for Cloud Security Transparency and Audit. Journal of Information Security and Applications, Vol. 54, 2020, Art. No. 102594, doi: 10.1016/j.jisa.2020.102594.

[23] Catteddu, D.—Hogben, G.: Cloud Computing: Benefits, Risks and Recommendations for Information Security. European Network and Information Security Agency (ENISA), 2009, `https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment`.

[24] Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. Cloud Security Alliance, 2017, `https://cloudsecurityalliance.org/artifacts/security-guidance-v4`.

[25] Cloud Control Matrix. Cloud Security Alliance, `https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix/#overview`.

[26] Consensus Assessments Initiative Questionnaire. Cloud Security Alliance, 2017, `https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-0-1/`.

[27] Jouini, M.—Ben Arfa Rabai, L.: Comparative Study of Information Security Risk Assessment Models for Cloud Computing Systems. Procedia Computer Science, Vol. 83, 2016, pp. 1084–1089, doi: 10.1016/j.procs.2016.04.227.

[28] Jouini, M.—Ben Arfa Rabai, L.: Mean Failure Cost Extension Model Towards Security Threats Assessment: A Cloud Computing Case Study. Journal of Computers, Vol. 10, 2015, No. 3, pp. 184–194, doi: 10.17706/jcp.10.3.184-194.

[29] Furuncu, E.—Sogukpinar, I.: Scalable Risk Assessment Method for Cloud Computing Using Game Theory (CCRAM). Computer Standards and Interfaces, Vol. 38, 2015, pp. 44–50, doi: 10.1016/j.csi.2014.08.007.

[30] Djemame, K.—Armstrong, D.—Guitart, J.—Macias, M.: A Risk Assessment Framework for Cloud Computing. IEEE Transactions on Cloud Computing, Vol. 4, 2016, No. 3, pp. 265–278, doi: 10.1109/TCC.2014.2344653.

[31] Akinrolabu, O.—Nurse, J. R.—Martin, A.—New, S.: Cyber Risk Assessment in Cloud Provider Environments: Current Models and Future Needs. Computers and Security, Vol. 87, 2019, Art. No. 101600, doi: 10.1016/j.cose.2019.101600.

[32] Sen, A.—Madria, S.: Application Design Phase Risk Assessment Framework Using Cloud Security Domains. Journal of Information Security and Applications, Vol. 55, 2020, Art. No. 102617, doi: 10.1016/j.jisa.2020.102617.

[33] Elahi, H.—Wang, G.—Xu, Y.—Castiglione, A.—Yan, Q.—Shehzad, M. N.: On the Characterization and Risk Assessment of AI-Powered Mobile Cloud Applications. Computer Standards and Interfaces, Vol. 78, 2021, Art. No. 103538, doi: 10.1016/j.csi.2021.103538.

[34] Weil, T.: Standards for Cloud Risk Assessments – What's Missing? IT Professional, Vol. 22, 2020, No. 6, pp. 16–23, doi: 10.1109/MITP.2019.2949361.

Martin Zbořil works at the Department of System Analysis, Faculty of Informatics and Statistics, University of Economics, Prague, in 2022, he obtained his Ph.D. there. His field of research is the cyber security with the main focus on cloud security. He has published many articles within this area where he provided the results of the research aimed at cloud security specifications, risks, providers selection and other relevant topics. He works also as IT security specialist in PricewaterhouseCoopers (PwC) where he focuses also on cloud security and where he leads the Cyber Resilience team. He has received multiple certificates within the cloud area: CCSP (Certified Cloud Security Professional), PCSM (Professional Cloud Security Manager), CCSK (Certificate of Cloud Security Knowledge), Microsoft Azure/M365 certificates (AZ-900, AZ-500, MS-500) and Amazon Web Service certificates (AWS Security Specialty, AWS Solutions Architect Associate, AWS Cloud Practitioner).