Risk management techniques in cloud infrastructures

Pratibha Sharma
Engineering Manager, Airbnb
Seattle, USA

DOI: 10.31364/SCIRJ/v12.i09.2024.P0924994
http://dx.doi.org/10.31364/SCIRJ/v12.i09.2024.P0924994

Abstract: This paper examines risk management methods in the cloud infrastructure, focusing on the identification, assessment and mitigation of risks related to data security and compliance with regulatory requirements. The paper emphasizes the importance of an integrated approach to vulnerability and threat analysis, including automated analysis systems, as well as traditional methodologies, such as STRIDE and FMEA. In the context of modern cloud platforms, special attention is paid to managing configuration vulnerabilities and security risks associated with cloud service providers. The work also examines the importance of selecting and adapting suitable cyber-secure frameworks, such as NIST CSF and ISO 27001, to ensure compliance and minimize risks. In conclusion, it is noted that risk management in the cloud infrastructure requires constant monitoring and adaptation of strategies to changing threats and regulatory requirements.

Keywords: Risk management, cloud infrastructure, data security, cybersecurity frameworks, automated analysis systems, CloudSafe, STRIDE, FMEA, NIST CSF, ISO 27001, configuration vulnerabilities, regulatory requirements.

Introduction

Cloud technologies are rapidly evolving and are widely used in various industries, providing organizations with flexible and scalable resources for data storage and processing. The relevance of this topic is driven by the fact that traditional risk management approaches often prove insufficient in the context of cloud infrastructures. Cloud systems have unique characteristics, such as multi-tenant environments and dependencies on external service providers, which require the adaptation of existing methodologies and the development of new approaches for identifying and assessing risks. With the increasing threat of cyberattacks and stricter regulatory requirements, organizations need to review and improve their risk management strategies.

The purpose of this study is to examine existing risk management methods in cloud infrastructure.

1. Identification and Assessment of Risks in Cloud Infrastructures

Modern cloud platforms represent a specific domain characterized by unique security challenges that organizations must carefully consider. Key threats include data leaks, unauthorized access to resources, credential compromise, insufficiently secured interfaces, and potential system failures. Recognizing these threats and their consequences is an important step toward establishing robust protection for cloud infrastructure.

Vulnerability analysis is a key element in identifying weak points and potential entry points for attackers in cloud systems [1]. To ensure that vulnerability analysis in a cloud environment is as effective as possible, it is recommended to adhere to certain principles, which are reflected in Table 1 below.

Table 1. Principles of Vulnerability Analysis [1]

Principle Name	Principle Description
Asset Identification and Inventory	Conduct a comprehensive analysis of the cloud services, applications, and data storage in use to obtain a complete understanding of the infrastructure.

http://dx.doi.org/10.31364/SCIRJ/v12.i09.2024.P0924994

Use of Specialized Tools	Use software solutions designed to scan vulnerabilities in cloud environments to timely detect potential threats.
Configuration Assessment	Analyze the security settings of the cloud infrastructure, paying attention to access control mechanisms, network parameters, and data encryption.
Prioritization of Identified Vulnerabilities	Determine the criticality of identified vulnerabilities, considering the potential consequences of their exploitation and the likelihood of threat realization.
Remediation of Identified Issues	Develop a rapid response strategy aimed at addressing identified weak points and minimizing the associated risks.

Next, Table 2 will examine the key risks faced by organizations working with cloud computing.

Table 2. Risks Arising When Working with Cloud Infrastructures [2]

Risk Name	Risk Description
Compliance Risks	Companies may face risks related to non-compliance with industry norms and standards such as HIPAA, SOC 2, GLBA, GDPR, and others. These risks arise when cloud service providers do not conduct external audits in accordance with required standards, which can lead to non-compliance with mandatory regulatory requirements. Although leading cloud service providers actively work to obtain certifications for recognized cybersecurity standards, organizations should independently verify the compliance of their processes and systems.
Data Leakage Threats	The risk of data leakage in cloud environments is exacerbated by the shared use of infrastructure between the provider and its clients. Leakage occurs when unauthorized individuals gain access to the company's confidential information. Since organizations' data is stored on cloud providers' servers outside their own premises, attacks on this data can affect all users served by the provider.
Risks Related to Cloud Service Provider Security	Interaction with a cloud service provider poses a risk to companies, as any security breach on the provider's side can directly impact their operations. Most companies rely on cloud solutions provided by various providers. The inability of providers to effectively manage security and risks can cause serious damage to the organization's development. Issues with the provider's reputation, potential bankruptcy, regulatory investigations, or legal proceedings can also negatively impact the provider's clients.
Improper Security Configurations	One of the main causes of data leaks in cloud environments is incorrect security configuration settings. Errors, shortcomings, or gaps in the configuration of the cloud environment can make it vulnerable to threats, leading to significant risks to data security [2].

Due to the rapid pace of societal development, traditional risk assessment methods are often ineffective in the context of cloud systems, which has led researchers to focus significantly on adapting these methodologies for cloud platforms. In this regard, it is proposed to use the concept of reusable threat profiles for threat analysis. This approach is similar to the use of protection profiles in the Common Criteria methodology, which define various threats and associated security aspects [3]. The risk assessment procedure allows for determining the level of threat and the associated risk within the context of an IT system integrated into the SDLC. Identified risks can be mitigated or eliminated by implementing appropriate control measures. After completing the risk assessment, threat modeling is usually conducted.

The first step in risk assessment is to hypothesize a potential attack on the software and analyze the factors motivating the attacker. Parameters such as the value of the data, the security level of the resources used during development, and the software's market presence should be considered. Based on these factors, an acceptable risk level is determined. For example, if a potential data loss could result in a $2,000 loss, but eliminating all potential vulnerabilities would cost $20,000, the company must decide whether such expenses are justified [4]. If the potential attack could damage the company's reputation, leading to significant long-term losses, fixing vulnerabilities might be necessary.

The next step in risk assessment is analyzing the consequences of a successful attack. Various scenarios should be considered, such as theft of critical data, the complexity of carrying out the attack, and the number of users who could be affected.

http://dx.doi.org/10.31364/SCIRJ/v12.i09.2024.P0924994

For example, a denial-of-service attack could impact thousands of users, while the spread of malware could infect a large number of computers. It is also essential to consider the accessibility of the attack target—network or local access, the need for authentication, and other factors.

Risk assessment boils down to determining the likelihood of an attack and the extent of the damage it could cause. Once risks are identified, companies must determine how the attack could be carried out and what it would target.

Threat modeling should be integrated into the early stages of the SDLC, before code is written. This process represents a structured approach to identifying potential threats and prioritizing measures to prevent them, with the goal of protecting critical data. Threat modeling allows security professionals to analyze the necessary protective measures based on the current information system and potential threats.

The effectiveness of threat modeling significantly increases when performed early, allowing potential issues to be identified and addressed in a timely manner, thereby saving resources and reducing the number of threats.

Implementing secure code review procedures during the SDLC phases, especially during implementation, significantly enhances product reliability. This process includes reviewing and validating the code to quickly address vulnerabilities and prevent the development of insecure software. This approach allows developers to be more proactive and respond quickly to potential threats, reducing their occurrence in the final stages of development. There are also several other approaches to security testing, including black-box testing and white-box testing.

Black-box testing involves checking the application's functionality without considering its internal structure, using tools that simulate the actions of an attacker. White-box testing, on the other hand, focuses on analyzing the internal structure of the application, source code, and design documentation. Both approaches complement each other and can be used together to achieve maximum software security.

In addition to manual review, there are automated methods such as static and dynamic testing, which significantly accelerate the process of identifying vulnerabilities and reduce the number of false positives. Implementing these approaches in the development process not only enhances security but also reduces future costs associated with fixing vulnerabilities, ensuring a smoother and more systematic development process [4].

There are four most commonly used risk assessment tools across various types of businesses. All of them are frequently used and easily applicable to different situations, reflected in the picture 1 :

http://dx.doi.org/10.31364/SCIRJ/v12.i09.2024.P0924994

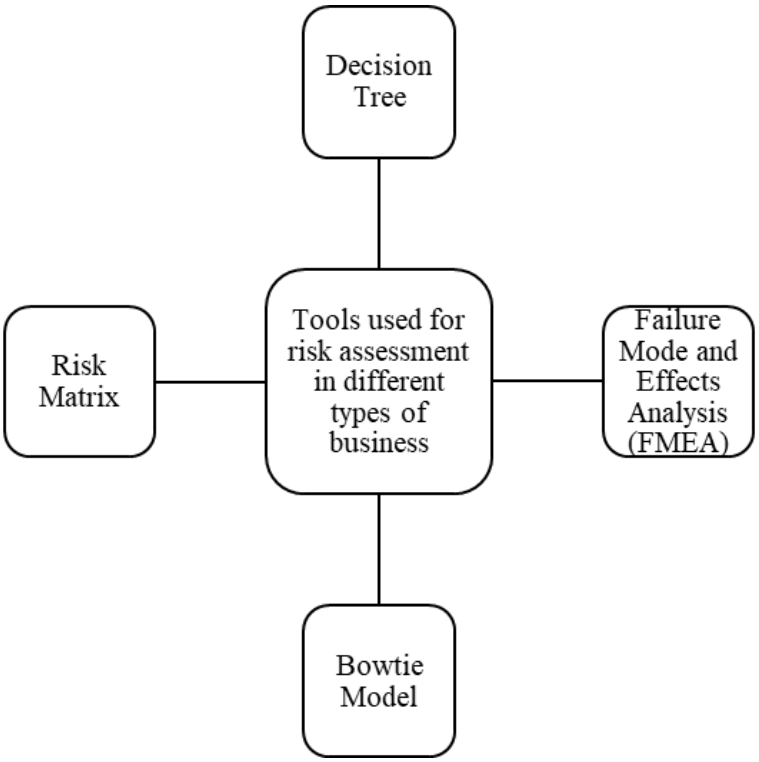

Fig.1. Tools used for risk assessment in different types of business [5].

The risk matrix is presented for clarity in Table 3.

Table 3. Risk Matrix [5]

Probability	Very Likely	Likely	Unlikely	Extremely Unlikely
Consequences Death	High	High	High	Medium
Serious Injuries	High	High	Medium	Medium
Minor Injuries	High	Medium	Medium	Low
Negligible Injuries	Medium	Medium	Low	Low

The risk matrix is a schematic representation of threats, displayed in the form of a table or diagram, which explains its alternative name—the risk diagram. In this format, risks are classified and ranked according to the likelihood of their occurrence and their potential impact on the project or process. The primary goal of using a risk matrix is to identify priority threats that require immediate attention and to develop appropriate measures to eliminate or minimize them. The size and structure of the matrix can vary depending on the project's specifics and the number of risks analyzed [5].

The FMEA methodology, which stands for Failure Mode and Effects Analysis, was developed in the 1940s by the U.S. military to identify potential problems in designs, processes, products, and services. This approach is mainly applied during the design or development stages to identify potential risks and assess their impact. FMEA consists of two key stages:

- Identification of failure modes, i.e., detection of possible malfunctions, problems, or failures.
- Effects analysis, which focuses on studying the impact of these failures on the system or product.

The decision tree method serves as a tool for risk assessment, providing project managers with a framework to evaluate different possible outcomes and their likelihood. Additionally, this tool is often used to calculate the overall cost of a project, product, or service. The decision tree process begins with selecting one element to be evaluated and further branching it into several directions with different goals and scenarios. The result is a diagram resembling a tree with branches, which gave this method its name.

http://dx.doi.org/10.31364/SCIRJ/v12.i09.2024.P0924994

The Bowtie model is designed to demonstrate the cause-and-effect relationships between various sources of risk and their consequences. The left side of the diagram shows the causes of the risk, the right side displays the possible outcomes of its realization, and the central part represents the event where these causes and consequences converge. Visually, this model resembles the shape of a bowtie, with its central part narrow and the sides wide, symbolizing the many causes and effects associated with a single risk [6].

2. Risk Management Based on Standards and Regulatory Compliance

The concept of the "best" cybersecurity framework is contentious, as the ideal framework for your business should be tailored to its specific needs. The selection of an appropriate framework largely depends on the legislation, regulatory requirements, and contractual obligations your organization faces. Generally, there are several key approaches to consider when choosing a suitable cybersecurity framework, including:

- NIST Cybersecurity Framework (NIST CSF);
- ISO 27001/27002;
- NIST SP 800-53 (for moderate or high requirements);
- Secure Controls Framework (SCF) or similar meta-frameworks.

When comparing different cybersecurity frameworks, it is important to consider the number of unique control elements they contain. This directly impacts the extent of coverage that the chosen framework can provide. Fewer control elements make the framework easier to implement, but this may also mean an insufficient level of protection required for the organization. It is important to note that selecting an appropriate framework for managing cybersecurity and privacy is a business decision based on risk analysis, legal requirements, and existing contractual obligations.

When choosing a framework, special attention should be paid to the need to customize it to the specific needs of the company. It is unlikely that one framework will perfectly suit an organization; it may be necessary to adapt it by adding or removing elements, or by combining several frameworks. Customizing frameworks can be likened to trying to fit a square peg into a round hole—it might fit, but it won't be perfect. It is often simpler and less costly to take a more complex and robust framework and remove unnecessary elements from it than to start with a simple one and add new elements [7].

The challenge of choosing a cybersecurity framework also involves understanding how comprehensively the selected framework covers all the necessary control elements. Comprehensive frameworks typically lead to more extensive policies and standards that must be followed, which, in turn, requires more resources to maintain. This creates a dilemma for organizations: how to meet requirements while minimizing the administrative burden. Solving this problem requires an understanding of the organizational culture regarding risks and determining which approach—minimal, moderate, or comprehensive—will be optimal for the company.

Thus, the selection of a cybersecurity framework should be based on a detailed analysis of the business's needs, its strategic goals, and regulatory requirements. It is also important to consider the resource capabilities for implementing and maintaining the chosen framework to ensure its effectiveness in the long term [8].

3. Methods for Risk Mitigation and Control

Regulatory requirements and approaches to risk management continue to evolve. Organizations must continually monitor new trends to maintain regulatory compliance and effectively manage risks. Key directions for future development include:

- Increased emphasis on data protection and cybersecurity: With the growing risks of data breaches and cyberattacks, regulatory requirements are increasingly focusing on data security and information protection. To safeguard confidential data and maintain customer trust, organizations need to adapt their risk management strategies to address these new challenges.

http://dx.doi.org/10.31364/SCIRJ/v12.i09.2024.P0924994

- Adoption of new technologies: Modern technologies such as artificial intelligence, machine learning, and blockchain are fundamentally changing approaches to regulatory compliance and risk management. Utilizing these technologies allows organizations to enhance the efficiency of compliance, automate processes, and improve risk identification and mitigation.

- Unification of regulatory standards at the international level: As business globalization increases, there is a need to harmonize regulatory standards across different countries. This provides organizations with the opportunity to reduce the costs of complying with various regulatory requirements and simplify international operations by aligning their risk management processes with international standards.

- Focus on sustainable development and ESG factors: Environmental, social, and governance (ESG) aspects are becoming increasingly important in the context of regulatory requirements. Organizations that integrate ESG principles into their risk management strategies can not only enhance the sustainability of their operations but also attract investment from socially responsible investors and reduce reputational risks.

Anticipating new trends and leveraging emerging opportunities will allow organizations to prepare for a successful future in risk management and regulatory compliance.

Aligning regulatory requirements with risk management processes plays a crucial role for organizations aiming to manage risks effectively and meet legal and ethical standards. A deep understanding of the regulatory environment, integration of advanced risk management methods, and adherence to best practices enable organizations not only to minimize risks but also to strengthen stakeholder trust.

In the future, organizations must continuously track new trends and opportunities in risk management and regulatory compliance. Adopting these trends and leveraging new opportunities will enable organizations to successfully adapt to the rapidly changing regulatory environment and ensure stable development in the future [9].

Conclusion

In conclusion, risk management in cloud infrastructure is a complex and multifaceted process that requires the integration of modern technologies, such as automated vulnerability analysis systems, with traditional approaches to risk assessment and management. The selection and adaptation of appropriate cybersecurity frameworks are key elements in ensuring robust data protection and regulatory compliance. In a rapidly changing technological and regulatory environment, organizations must continuously improve their risk management strategies to effectively safeguard their assets and minimize potential threats. As a result, successful risk management in cloud infrastructures enhances the resilience and reliability of IT systems and strengthens the trust of customers and partners.

References

1. Securing the Cloud: Assessing Risks and Vulnerabilities in Cloud Environments. [Electronic resource] Access mode: https://cybersuraksa.medium.com/securing-the-cloud-assessing-risks-and-vulnerabilities-in-cloud-environments-9c87b2960528 (accessed 08/15/2024).

2. Risk Management in Cloud Computing. [Electronic resource] Access mode: https://www.scrut.io/post/risk-management-in-cloud-computing (accessed 08/15/2024).

3. Immanuel Kunz, Angelika Schneider, Christian Banse, A Continuous Risk Assessment Methodology for Cloud Infrastructures. [Electronic resource] Access mode: https://www.researchgate.net/publication/361325088_A_Continuous_Risk_Assessment_Methodology_for_Cloud_Infrastructures (accessed 08/15/2024).

4. Alya Hannah Ahmad Kamal, Caryn Chuah Yi Yen, Risk Assessment, Gan Jia Hui, Pang Sze Ling Threat Modeling and Security Testing in SDLC. [Electronic resource] Access mode:

http://dx.doi.org/10.31364/SCIRJ/v12.i09.2024.P0924994

https://www.researchgate.net/publication/347125346_Risk_Assessment_Threat_Modeling_and_Security_Testing_in_SDLC (accessed 08/15/2024).

5. A Quick Introduction to Risk Assessment Tools. [Electronic resource] Access mode: https://safetyculture.com/topics/risk-assessment/risk-assessment-tools/ (accessed 08/15/2024).

6. Risk assessment vs. threat modeling: What's the difference? [Electronic resource] Access mode: https://www.techtarget.com/searchsecurity/tip/Risk-assessment-vs-threat-modeling-Whats-the-difference (accessed 08/15/2024).

7. NIST CSF vs ISO 27001/2 vs NIST 800-53 vs SCF. [Electronic resource] Access mode: https://complianceforge.com/grc/nist-800-53-vs-iso-27002-vs-nist-csf-vs-scf (accessed 08/15/2024).

8. Risk Management in Regulatory Frameworks: Towards a Better Management of Risks. [Electronic resource] Access mode: https://unece.org/DAM/trade/Publications/WP6_ECE_TRADE_390.pdf (accessed 08/15/2024).

9. Aligning Regulatory Standards with Risk Management. [Electronic resource] Access mode: https://fastercapital.com/content/Aligning-Regulatory-Standards-with-Risk-Management.html (accessed 08/15/2024).

http://dx.doi.org/10.31364/SCIRJ/v12.i09.2024.P0924994