Journal of Electronic Research and Application, 2024, Volume 8, Issue 3
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

Research on Network Security Level Protection Measurement Strategy in the Context of Cloud Platforms

Lin Ma*

Zhejiang Testing & Institute for Mechanical and Electrical Products Quality, Hangzhou 310051, China

***Corresponding author:** Lin Ma, malin4050@163.com

Abstract: Platforms facilitate information exchange, streamline resources, and reduce production and management costs for companies. However, some viral information may invade and steal company resources, or lead to information leakage. For this reason, this paper discusses the standards for cybersecurity protection, examines the current state of cybersecurity management and the risks faced by cloud platforms, expands the time and space for training on cloud platforms, and provides recommendations for measuring the level of cybersecurity protection within cloud platforms in order to build a solid foundation for them.

Keywords: Cloud platform; Cyber security; Level protection measurement

Online publication: June 14, 2024

1. Introduction

Regarding national management, national security is partly determined by network security, and it also has an impact on the development of the social economy, if there is a problem with network security, the interests of the masses are difficult to be safeguarded. It is important to create a positive concept of information security, emphasize the security protection of infrastructure, improve the construction of network security information coordination mechanisms, tools, and platforms, strengthen the construction of emergency management capabilities for network security incidents, actively promote the development of the network security industry, and save for a rainy day to prevent incidents from occurring in advance.

2. Network security level protection overview

2.1. Network security level protection process

The work of information security level protection is divided into five stages:

(1) Rating: the first step is to determine the rating of the system before proceeding to the next step.

(2) Filing: After determining the rating of the system, the public security organs will review the materials

submitted by the system, and the public security organs will issue a document called "Filing Certification Materials."

(3) Construction and Rectification: After submission, the existing system will be adjusted according to the relevant information security standards and management norms, including the purchase of appropriate security products and the formulation of appropriate security policies according to the evaluation level.

(4) Level evaluation: After the system is built or repaired, whether the system meets the requirements of the relevant evaluation level must be evaluated by a qualified third-party evaluation organization following the relevant protection level evaluation standards, and after the evaluation is completed, a protection level evaluation report must be prepared.

(5) Supervision and inspection: After the evaluation is completed, the evaluated organization must submit the evaluation report to the public security authorities, and only in this way is the entire evaluation process completed. Next, the public security authorities are responsible for monitoring and inspecting the system during the test period.

2.2. Concept of network security level protection assessment

Cybersecurity level protection assessment is an important step in the cybersecurity workflow, and its workload can be significant. It requires the cooperation of staff involved in server room management, network management, host management, application system management, and security management through face-to-face interviews, on-site equipment inspections, and on-site equipment testing.

2.3. Basic contents of network security level protection assessment

The basic elements of network security level protection assessment include an assessment of the security control room and a system-wide assessment, as shown in **Figure 1**.

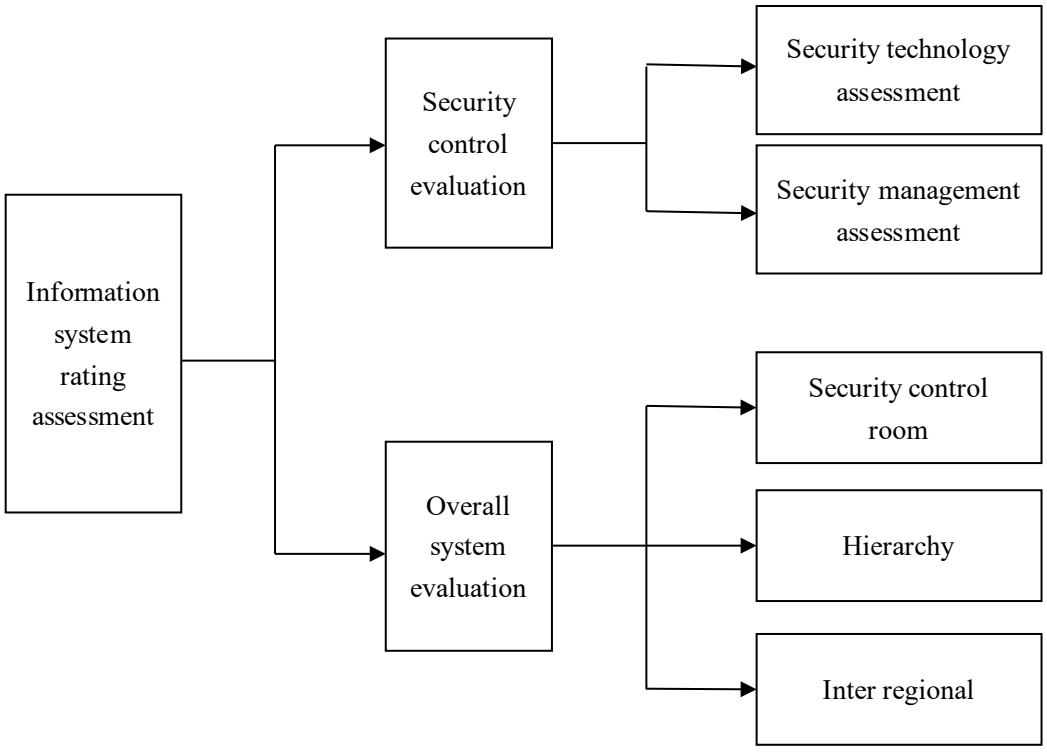

Figure 1. Information system level evaluation content map

Security control evaluation is a measurement of the main configuration and execution of information system equipment. The system-wide evaluation is a comprehensive check of the overall security posture of the system by analyzing the relationship between the topology of the system and the control evaluation based on the security control evaluation. Generally speaking, the success of the overall system evaluation is based on the success of the security control evaluation.

2.4. Network security protection level evaluation workflow

The process of network security protection level evaluation consists of three stages: the first stage is the preparation of the evaluation, the second stage is the on-site implementation of the evaluation, and the third stage is the preparation of the report. The workflow of network security protection level assessment is shown in **Figure 2**.

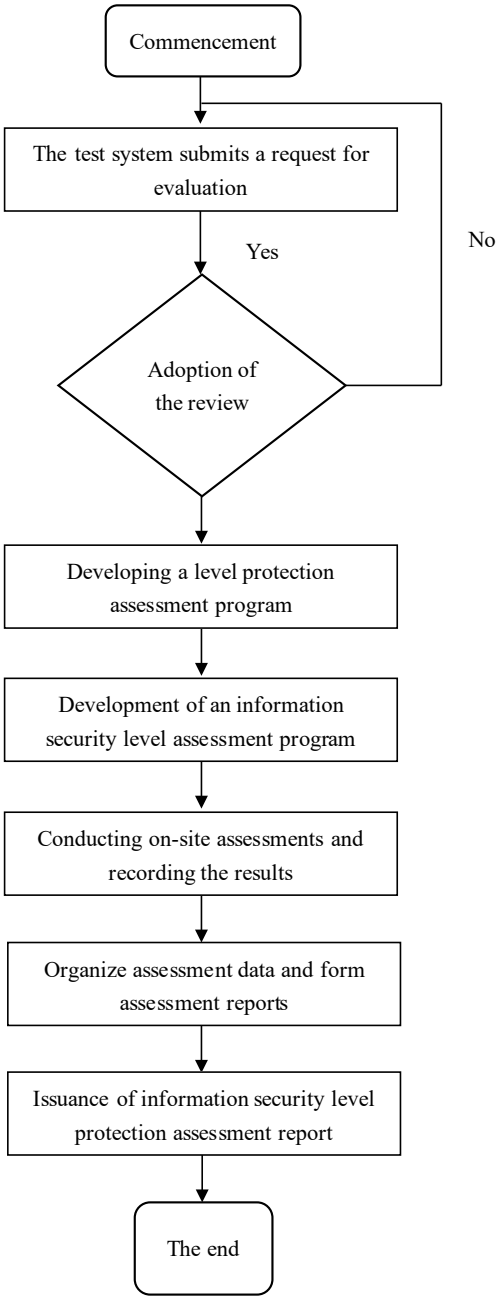

Figure 2. Workflow diagram of the measurement and evaluation

(1) Measurement preparation phase: The preparation phase, i.e., the beginning of the evaluation process, is crucial for proper evaluation. The main goal of this phase is to familiarize with the details of the information system under test. The main objectives of this phase are to familiarize with the details of the information system under test and to prepare the site implementation plan, documentation, and testing tools.

(2) On-site implementation stage: In this stage, the evaluator must arrive at the test unit and carry out the evaluation work on-site. The main work is to complete all the evaluation points according to the classification level of the system, according to the plan, and in accordance with the evaluation specifications for that protection level. At this stage, the evaluation personnel should record the current implementation of the system under test and its security status.

(3) Report writing stage: This stage, like the question stage, is the summarization stage of the level of protection evaluation work. It is a comprehensive evaluation of the security of the system under test. The evaluation in this stage is mainly based on the comparison between the on-site evaluation records and the requirements of the evaluation standards, and then summarizes the differences between the current performance of the system and the corresponding level protection evaluation standards, and puts forward appropriate corrective suggestions, and finally prepares a level evaluation report.

3. Status quo of cloud platform network security management

In security management, problems are dealt with through HA to monitor the network data status and determine the ability of the server to continue to run. vCenter has a limiting effect on the functions of management when it comes to network protection, while the customers in it unfold the division of categories to realize intelligent user management.

4. New requirements for network security level protection

Level Protection 2.0 establishes new standards for level protection measurement and security management methods, security management objectives for big data and cloud platforms, mobile networks, etc. Specific changes in governance standards are reflected in the following aspects:

(1) Changes in equal protection requirements: On the basis of the basic requirements, design requirements, and measurement requirements for network security layer protection for cloud platform environments, certain security protection standards and security reinforcement requirements for new areas such as cloud platforms have been added, and cloud platform-specific layer protection objects and standards have been added.

(2) Changes in grading objectives: Cloud platforms and carrier systems will be evaluated according to their security protection level. The security protection level is determined according to the key contents of the hosted or proposed hosted objects.

(3) Changes in responsibility boundaries: The main challenge in ensuring the level of cybersecurity of cloud platforms is the issue of security responsibility boundaries, where tenants are responsible for the security of tenants and platforms are responsible for the security of platforms.

5. Construction of network security level protection in the cloud platform environment

5.1. Cloud platform functional framework

As shown in **Figure 3**, the cloud platform functional framework is divided into five logical layers.

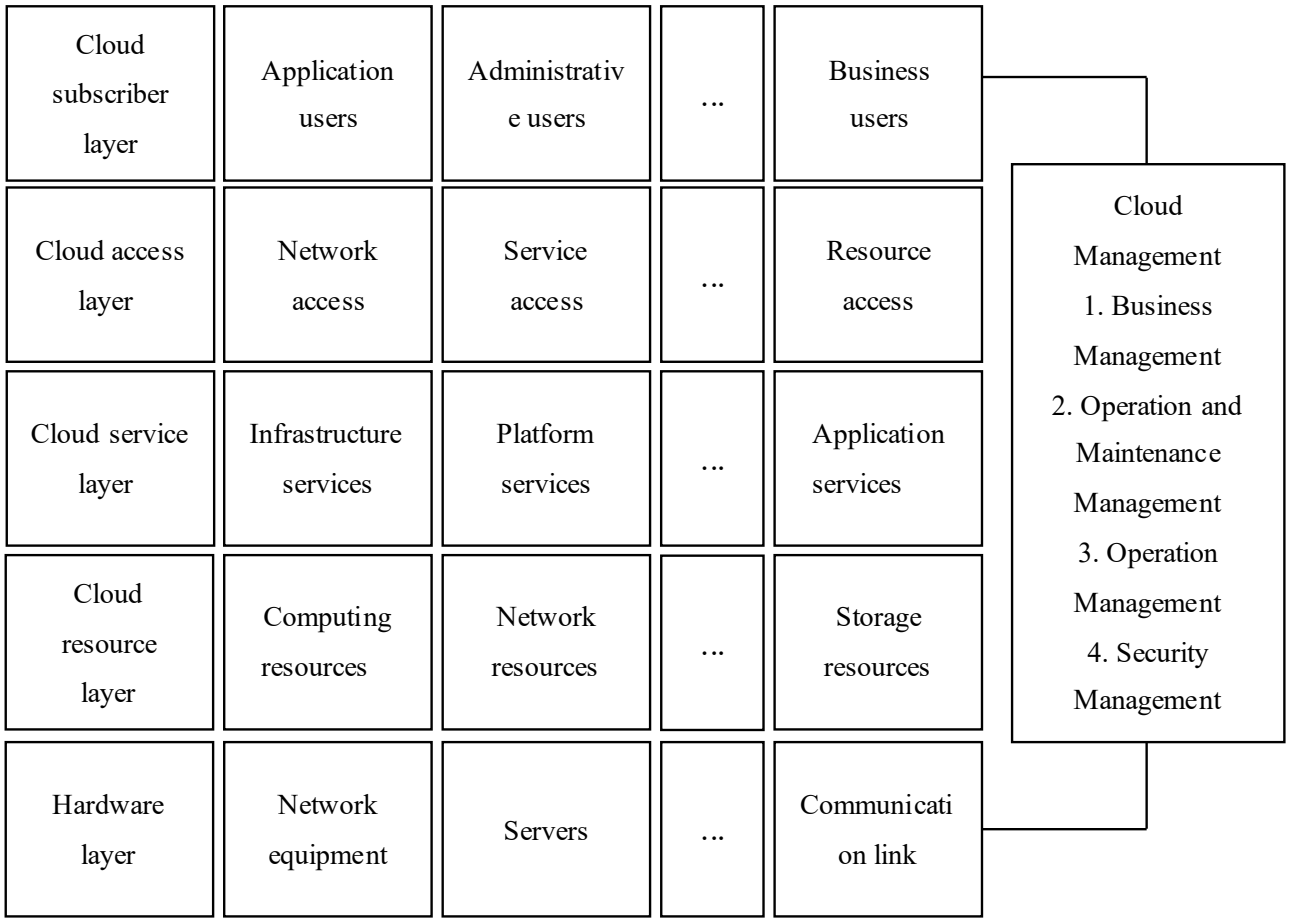

Figure 3. Cloud computing functional framework diagram

5.2. Classification object determination and management task assignment

The cloud platform protection environment is a set of cloud platforms, software, and related components deployed on top of the cloud platform by the cloud service provider. Among them, the cloud service provider has the responsibility to categorize and protect the cloud platform according to the protection level. First, in the IaaS infrastructure as a service model, the cloud service provider is responsible for monitoring VMs and hardware, then the cloud tenant's role is to supervise the operating system, database, middleware, and applications; second, in the PaaS platform-as-a-service model, the cloud service provider's responsibilities include VM monitoring, hardware, operating system, database, and middleware, then the cloud tenant's role is just for applications; Finally, in the SaaS software-as-a-service model, the cloud service provider's responsibilities include VM monitors, hardware, operating systems, databases, middleware, and applications. The cloud tenant is required to provide access to users and maintain user account security.

5.3. Determining security protection objects

Compared with traditional information systems, cloud platforms and cloud systems have all the objectives of enhanced security protection, as shown in **Table 1**.

Table 1. Objects of protection of cloud platform security protection system

Aspects	Functional dimension	Object of protection
Communications and network security	Hardware	Network architecture, network devices, security devices, medium, and physical links
	Cloud resource layer	VM monitors, cloud management platforms, and virtual network/security appliances
	Cloud service layer	Virtual network architecture, virtual proprietary cloud, virtual security appliance
Device and cloud environment security	Hardware facilities	Hosts (physical machines, hosts), terminals, network devices, security devices
	Cloud resource layer	Operating system, database management system, virtual machine monitor, network policy controller, cloud management platform
	Cloud service layer	Virtual machines, database services, middleware, etc.
Application and data security	Application security	Virtual machines, database services, middleware, etc.
	Data security	Business data, authentication data, system data

5.4. Establishment of cloud platform security protection system framework

The cloud security protection technology framework is an important guideline and foundation for the security design of cloud platforms and systems.

(1) Design ideas for cloud security protection technical system

In order to put forward the analysis method of security threats, vulnerabilities, and security protection measures for the defense target, as shown in **Figure 4**.

Through the analysis, about one hundred cases of security risks are identified, including virtual machine escape, cross-virtual machine attack, malicious virtual machine execution network attack, API persistence attack, etc. Then, based on the security protection capabilities to be realized by different tiers of information systems, the security threats to be dealt with by different tiers of cloud platform systems are identified.

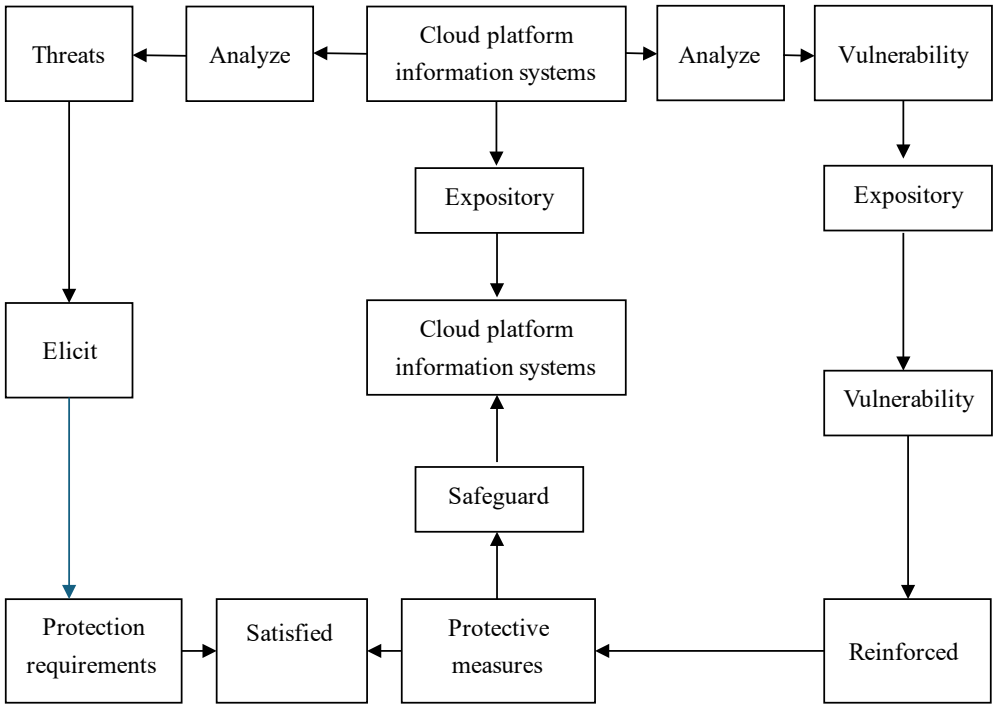

Figure 4. Cloud platform security protection system establishment method

(2) Cloud security protection technology system framework

The functional structure of the cloud platform includes the user layer, the access layer, the resource layer, the service layer, and the management layer. The service model mainly includes IaaS, PaaS, and SaaS, and the cloud service provider or cloud platform has different service models. Cloud service providers or cloud platform service providers and cloud tenants or cloud platform service users have different responsibilities to ensure hierarchical protection according to the vertical protection concept of "one center, three protections."

5.5. Hierarchical security design implementation

The revised cloud platform cascading provisions are consistent with the original standard. However, given that the public cloud platform carries multiple tenants and multiple business systems if the cloud platform fails, the scope of impact is much larger. Therefore, the cloud platform security protection level of the public cloud should be at least level 2.

6. Risks of cloud platform network security management

In the context of level protection 2.0, network security standards are evolving, and the measurement process emphasizes data integrity and privacy, centralized data management, and information protection, but it also faces significant challenges in the actual process of protecting network data.

6.1. Risks faced by network systems

In the context of cloud platforms, the application layer and the hardware layer form a virtual network layer, and the virtual layer faces brand-new hidden risks in its operation. Therefore, cloud platforms also have various risks in the process of implementing information security protection for users.

6.2. Data risk and virus risk

Data integrity protection is a key element of the Cloud Platform 2.0 security level protection, which includes dynamic and static data segregation and residual data handling, and security issues in transmission and storage must be addressed to ensure that data is not compromised or lost.

6.3. Risk of high resource utilization

Virtualization technology changes physical data into logical management data, solves the difficulties between physical frameworks, and allows customers to better use the data provided by physical servers. It is a serious issue when compared with the previous IT architecture where only one application stops when the server fails.

6.4. Virus and malicious code risks

Inside the information center managed by the cloud platform, stable and useful templates are an important part of the selection of virtual machines. Besides, the overall preservation of information in the virtual machine and the continuity of the IP address of the virtual machine provide more opportunities for the spread of viruses.

6.5. Security risks of virtual systems

The most important technology of the cloud platform is virtual reality, and its deployment usually involves the creation of a virtual layer between the application layer and the hardware layer, and the creation of the virtual layer brings new security risks to the system. It is essential to effectively isolate and protect resources between

multiple users within a data center cloud platform.

7. Measuring and evaluating network security level protection under cloud platforms

In order to protect the security level of the network, it is necessary to pay attention to the technical standards in line with the current technical situation and needs, ensure the security and autonomy of the cloud platform, maintain the security of information maintenance and network management, and reasonably use the cyberspace.

7.1. Measuring and evaluating system status and rationally deploying the system

First, before deploying the cloud platform, the business objectives should be measured first. Second, the application environment should be measured, focusing on whether the existing software, hardware, and network terminal environment meet the requirements for virtualization implementation. Thirdly, the technical level should be measured, focusing on whether the technicians have good business skills and can effectively solve the relevant problems that arise in the implementation process.

7.2. Emphasizing data security

The network management process of the cloud platform must also pay attention to data security. Sensitive key encryption technologies such as TrueCrypt and PGP Systems should be selected to ensure that data security risks are managed.

7.3. Focusing on system construction and applying security technology

Security technologies enforce security controls to adequately protect data and information, such as expanding virtual machines and protecting isolated virtual machines. Cloud platform management should use anti-virus software to scan these devices and block virus entry paths, use virtual machines when transferring data from USB drives, etc.

8. Conclusion

The level of network security protection in the cloud platform environment must be based on national security policies and technical standards, and combine the level protection requirements, actual business needs, and technical systems to further standardize and institutionalize security management. At this stage, the rapid development of information technology, cloud platforms, and big data technology are widely used in human life, and the data storage and management of cloud platforms is effective. However, network security on cloud platforms is widely concerned, and the goal of network security management is high. Companies, devices, and individuals are facing positive challenges in choosing high-quality technicians to handle data, eliminate network risks, monitor the functions of virtual machines in time, and establish a stable foundation for security or stability.

Disclosure statement

The authors declare no conflict of interest.

References

[1] Chang J, 2019, Network Security Level Protection Assessment Strategy in the Context of Cloud Platform. Financial Electronic, 2019(6): 2–4.

[2] Yang Y, 2022, Exploration of Security Risk and Construction of Cloud Platform Under the Standard Requirements of Equal Protection 2.0 System. Electronic Components and Information Technology, 6(11): 2–5.

[3] Li X, Yang L, 2020, Research on the Implementation Effect of Network Security Level Protection System-Taking Yichang City, Hubei Province as a Perspective. Three Gorges Forum (Three Gorges Literature-Theory Edition) 2020(04): 100–104.

[4] Guo L, 2020, Court Network Security Management and Response Under Network Security Level Protection 2.0 System. Network Security Technology and Application, 2020(05): 136–137.

[5] Liu H, 2020, Security Area Boundary Based on Network Security Level Protection 2.0. Electronic Technology and Software Engineering, 2020(01): 236–238.

[6] Fu S, 2018, Analysis of Network Security Level Protection Under Cloud Platform Environment. Modern TV Technology, 2018(9): 3–5.