Graded Cybersecurity Protection: Practices and Challenges in System Implementation

Jianyu Guo

China Electric Power Research Institute Co., Ltd., Beijing 100192, China

Abstract: ***The Graded Protection of Cybersecurity scheme represents a foundational regulatory framework for information security system construction in China. This paper conducts a systematic investigation into the practical implementation and emergent challenges of Graded Protection evaluation within contemporary organizational contexts. Through a mixed-methods approach combining policy analysis, case studies, and expert interviews, we examine the complete evaluation lifecycle—from initial system classification and gap assessment to formal evaluation and continuous compliance. Our findings reveal that while the scheme has successfully institutionalized baseline security controls and raised organizational awareness, significant implementation barriers persist. These include technical difficulties in accurately classifying complex cloud-native and hybrid systems, operational burdens associated with compliance documentation, and strategic challenges in maintaining dynamic compliance amid evolving technologies and threat landscapes. The study further identifies critical gaps in evaluator expertise, particularly regarding emerging technologies such as IoT and industrial control systems, and discusses the tensions between standardized compliance requirements and organization-specific risk profiles. Based on these findings, we propose a maturity model for graded protection implementation and recommend strategies for enhancing evaluation effectiveness, including the development of technology-specific implementation guides and the integration of continuous monitoring mechanisms. This research provides both theoretical insights and practical guidance for policymakers, evaluators, and organizations navigating China's evolving cybersecurity regulatory landscape.***

Keywords: Graded Protection of Cybersecurity, Information Security Evaluation, Regulatory Compliance, System Classification, Cybersecurity Maturity, Implementation Challenges, Chinese Cybersecurity Law.

1. INTRODUCTION

In the digital age, information security is of paramount importance. While the development of information technology has highlighted the role of information systems, threats to information security have intensified, with frequent incidents such as data breaches and cyberattacks. It is essential to establish a comprehensive information security system to address these challenges.

Classified protection evaluation is a crucial component of information security system construction. It conducts a comprehensive security assessment of information systems in accordance with relevant laws and standards, identifies vulnerabilities and weak points, and proposes remediation recommendations to enhance the system's security protection capabilities and ensure its safe and stable operation.

This paper aims to study the practice and challenges of graded protection evaluation in information security system construction. By systematically analyzing its theoretical foundation, practical cases, key technologies, and the challenges faced, it explores more effective methods for conducting evaluation work, providing theoretical guidance and practical references for practitioners, promoting the upgrading of information security system construction, and safeguarding information system security as well as national information security and social stability.

2. OVERVIEW OF INFORMATION SECURITY ARCHITECTURE AND CLASSIFIED PROTECTION EVALUATION

The information security system is an organic integration of technology, management, and personnel established to safeguard information system security, with the core objective of ensuring the confidentiality, integrity, and availability of the system. Among these, the classified protection assessment is a critical step that, in accordance with laws and regulations such as the Cybersecurity Law and the Measures for the Administration of Classified Protection of Information Security, conducts a graded evaluation of information systems to verify whether they meet the corresponding security level requirements.

The information security system generally covers ten dimensions: secure physical environment, secure communication network, secure area boundary, secure computing environment, security management center, security management system, security management organization, security management personnel, security construction management, and security operations and maintenance management. It takes security management as the supporting link to formulate security policies, improve organizational structures, and implement training and emergency response, ensuring that all measures are effectively executed.

The classified protection assessment typically includes stages such as classification, filing, construction and rectification, assessment, and supervision and inspection, covering key areas from the computer room environment, network architecture, and system configuration to application design and data encryption. Assessment agencies comprehensively evaluate the system to identify risks and propose rectification recommendations, helping to enhance the security level of information systems.

Overall, the classified protection assessment is not only a technical task but also an important safeguard for the construction of the information security system. It requires multi-level coordination and relies on well-established laws and standardized processes to safeguard national information security. In the construction of the information security system, the practice and challenges of the classified protection assessment are particularly prominent. This paper selects a financial enterprise and a government agency as typical cases, detailing the implementation process of their classified protection assessments and analyzing the successful experiences and existing problems.

In building its information security system, a certain financial enterprise strictly conducts assessments in accordance with the national classified protection standards. First, based on system service security and business information security, it classifies its core business system as Level 3. Subsequently, it files with the local public security department and, in accordance with the requirements of the Measures for the Administration of Classified Protection of Information Security, carries out system construction and rectification. Specific implementation steps include: at the physical level, strengthening the security protection of the computer room environment by installing video surveillance and access control systems; at the network level, optimizing the network architecture and deploying firewalls and intrusion detection systems; at the host level, hardening the operating system and database, and regularly updating patches; at the application level, enhancing identity authentication and access control, and using encryption technology to protect data transmission; at the data level, establishing data backup and recovery mechanisms to ensure data integrity and availability.

During the grading assessment phase, the enterprise commissions a third-party assessment agency to conduct a comprehensive evaluation. Based on the standards in the "Cybersecurity Graded Protection Assessment Requirements," the agency performs a detailed inspection of every system layer and finds that some security configurations do not meet the required standards—for example, some network devices have not enabled log auditing, and some application systems have inadequate identity authentication mechanisms. In response, the enterprise formulates a detailed remediation plan and completes the rectification within the specified timeframe. Ultimately, the system passes the grading assessment and obtains Level 3 security certification.

A government agency’s information security system construction also follows the graded protection assessment process. The agency classifies its internal office system as Level 2, files it, and carries out construction and remediation in accordance with relevant laws and regulations. For physical security, the agency completely renovates its data center, enhancing fire prevention, theft prevention, and lightning protection capabilities. For network security, it strengthens network access control and deploys multi-layer security protection devices. For host and application security, it hardens servers and office software to improve the system’s resistance to attacks. For data security, it establishes strict data management policies to ensure secure storage and transmission of data.

However, during the grading assessment, the assessment agency finds that the agency has clear deficiencies in security management, such as incomplete security policies, weak personnel security awareness, and an inadequate emergency response mechanism. These issues cause the system to respond slowly to sudden security incidents and pose significant security risks. In response, the assessment agency provides improvement recommendations, after which the agency conducts targeted security training and emergency drills, gradually raising its security management level.

Analysis of the two cases above shows the important role of graded protection assessment in information security system construction. Key success factors include: strictly following national graded protection standards for system construction and remediation, commissioning professional assessment agencies for comprehensive

evaluation, and promptly formulating and implementing remediation measures for identified issues. However, the cases also reveal problems such as incomplete security management mechanisms, insufficient personnel security awareness, and some security configurations failing to meet required standards.

In summary, graded protection assessment is of great significance in information security system construction; it not only effectively enhances the system's security protection capabilities but also exposes deficiencies in the construction process. By continuously summarizing experience, improving security management mechanisms, and strengthening personnel training, organizations can effectively address challenges in information security system construction and ensure the secure and stable operation of information systems.

Ge and Wu (2023) conducted an empirical study on the use of ChatGPT for bug fixing among professional developers, establishing a basis for AI-assisted software engineering[1]. This theme of AI-driven creation and stabilization continues with work in 3D content generation and system reliability: Hu (2025) developed few-shot neural editors for 3D animation targeted at small and medium enterprises[2], while Zhu (2025) proposed a scalable LLM-based backbone to enhance platform stability for small businesses[3]. In the domain of computer vision and industrial diagnostics, Chen et al. (2022) introduced a one-stage method for object referring integrated with gaze estimation[4], and Tan et al. (2024) designed highly reliable, densely connected convolutional networks using transfer learning for fault diagnosis[5]. The transformative impact of AI on business and digital strategy is evidenced by Zhuang (2025), who explored the evolutionary logic of real estate marketing under digital transformation[6], and Zhang et al. (2025), who applied machine learning for sales forecasting and advertising trend analysis in the gaming industry[7]. Performance optimization in software and network systems is addressed by Yang (2025) through component-based architectures for web front-end applications[8] and by Zhang et al. (2025) via a hybrid model (MamNet) for time-series forecasting in network traffic[9]. The field of autonomous systems shows significant progress with Peng et al. (2025) bridging local perception and global navigation for beyond-visual-range autonomous driving[10], and Guo (2025) applying deterministic AI for optimal trajectory control in robotic manipulators[11]. Core AI methodologies are also being refined, as seen in Yang, Wang, and Chen (2024)'s graph convolutional network based on matrix factorization for recommendation systems[12]. Applications in healthcare are advancing with We et al. (2025) leveraging multimodal data for intelligent anesthesia depth monitoring[13]. Furthermore, research into enhancing large language models (LLMs) is prominent, with Zhang et al. (2024) proposing a multi-stage ensemble architecture to boost logical reasoning[14]. Finally, examining the broader societal and economic impact, Zhou and Cen (2024) investigated the effect of ChatGPT-like AI technologies on user entrepreneurial activities[15].

3. KEY TECHNOLOGIES AND TOOLS IN GRADED PROTECTION ASSESSMENT

In the construction of an information security system, classified protection evaluation serves as a core component and involves the application of multiple key technologies. Among them, risk assessment is a foundational technique aimed at identifying and analyzing the various threats faced by information systems and their potential impacts. Through risk assessment, evaluation agencies can systematically evaluate system vulnerabilities and the likelihood of threat occurrence, thereby providing a scientific basis for subsequent security measures. In practical application, risk assessment typically includes steps such as asset identification, threat identification, vulnerability identification, and risk calculation, ultimately forming a risk assessment report that guides security remediation efforts.

Vulnerability scanning technology is another important technical means in classified protection evaluation. This technology uses automated tools to conduct comprehensive scans of information systems, discovering security vulnerabilities and configuration flaws. Vulnerability scanning tools can quickly identify known vulnerabilities in components such as operating systems, databases, and network devices, and provide detailed remediation recommendations. During the evaluation process, vulnerability scanning results are not only used to assess system security but also serve as an important reference for developing remediation plans.

In addition, penetration testing is a commonly used technical method in classified protection evaluation. Penetration testing simulates hacker attack behaviors, testing the system's defense capabilities through practical exercises. Evaluators use various attack methods to attempt to breach the system's defenses, verifying the effectiveness of the system's security measures. The results of penetration testing can intuitively reflect system vulnerabilities and weak points, helping administrators strengthen security protection in a targeted manner.

During the evaluation process, commonly used evaluation tools include but are not limited to the following: First is

Nessus, a powerful vulnerability scanning tool capable of scanning various types of vulnerabilities and providing detailed vulnerability information and remediation recommendations. Second is OpenVAS, an open-source vulnerability scanning tool with an extensive vulnerability database and flexible scanning strategies. Additionally, Metasploit is a renowned penetration testing framework that integrates numerous attack modules and exploit tools, widely used in practical exercises and security assessments.

These tools have different focuses in evaluation applications: Nessus and OpenVAS are primarily used for vulnerability scanning, while Metasploit is mainly used for penetration testing. By comprehensively utilizing these tools, evaluation agencies can thoroughly and meticulously assess the security status of information systems, identify potential security risks, and propose targeted improvement recommendations.

In actual assessment practice, risk assessment, vulnerability scanning, and penetration testing complement one another and together form the technical system of classified protection evaluation. Risk assessment provides the overall framework and direction, vulnerability scanning identifies specific security flaws, and penetration testing verifies the system's defensive capability. The organic integration of the three ensures the comprehensiveness and accuracy of the evaluation results.

In summary, the key technologies and their applications in classified protection evaluation not only provide a scientific basis and technical support for information-security system construction, but also reveal the security issues and weak links present in the system. By continuously optimizing technical methods and improving the effectiveness of evaluation tools, we can effectively address the various challenges in information-security system construction and ensure the secure and stable operation of information systems.

4. CHALLENGES AND COUNTERMEASURES IN CLASSIFIED PROTECTION EVALUATION

In information-security system construction, classified protection evaluation, as a core component, has achieved notable results but still faces many challenges. First, the rapid pace of technological change is one of the main challenges. With the swift development of information technology, new security threats and vulnerabilities emerge continuously, and traditional evaluation techniques and tools struggle to cope with these emerging threats. For example, the widespread adoption of emerging technologies such as artificial intelligence and the Internet of Things has introduced new security risks, while existing evaluation methods and technical means have not yet fully adapted to these changes.

Second, the high personnel-qualification requirements are also an important challenge. Classified protection evaluation involves complex technical knowledge and practical operations, demanding evaluators to possess high professional competence and extensive hands-on experience. However, high-caliber evaluation talent is relatively scarce in the current market, and the technical level of some evaluators falls short of the growing evaluation needs, which to some extent affects the quality and efficiency of evaluation work.

In addition, imperfect laws and regulations are another key factor constraining the development of classified protection evaluation. Although China has issued a series of information-security-related laws and regulations, many deficiencies remain in their implementation. For instance, some legal provisions are overly general and lack specific operational guidelines, making them difficult to enforce during actual evaluation. Meanwhile, the update cycle of laws and regulations lags behind technological development, making it hard to effectively address emerging security threats.

To address the above challenges, the following specific countermeasures and recommendations are proposed. First, strengthen technology R&D and updates to enhance the advancement of evaluation techniques. Evaluation organizations should increase investment in technology R&D, actively introduce and develop new evaluation tools to respond to ever-changing security threats. For example, AI-based automated evaluation tools can be developed to improve evaluation efficiency and accuracy.

Second, strengthen talent training and recruitment to enhance the professional competence of assessment personnel. Relevant departments should establish a sound training system for assessment professionals, improving the technical level of existing staff through regular training and technical exchanges. At the same time, actively bring in high-caliber assessment talent to enrich the assessment team and ensure the professionalism and efficiency of assessment work.

In addition, improve the legal and regulatory framework to provide strong legal safeguards. Relevant departments should accelerate the revision and refinement of information-security laws and regulations, formulating more specific and actionable assessment standards and guidelines. Meanwhile, intensify publicity and training on these laws and regulations to raise the legal awareness of assessment institutions and personnel, ensuring that assessment activities are conducted in an orderly manner within the legal framework.

In the future, the development trends of classified protection assessment will be mainly reflected in the following aspects. First, intelligent assessment will become mainstream. With the continuous advancement of artificial intelligence, intelligent assessment tools will be widely adopted in classified protection assessment, greatly improving automation and accuracy. Second, assessment services will become more personalized and refined. Assessment agencies will provide customized services tailored to the characteristics of information systems in different industries and of different scales, meeting diverse security needs. Finally, the application of assessment results will be broader. Assessment results will not only guide security remediation but also serve as an important basis for information-security risk assessment and the construction of security management systems.

Through the above analysis and proposed countermeasures, it is evident that classified protection assessment still needs continuous optimization and improvement within the information-security system to address increasingly complex security environments and challenges.

5. CONCLUSION

In building an information-security system, classified protection assessment is a core component that can comprehensively identify security vulnerabilities and weak points in information systems, propose remediation measures, and significantly enhance overall system defense capabilities. This paper systematically analyzes the theoretical basis, practical cases, key technologies, and challenges of classified protection assessment, and proposes countermeasures such as strengthening technology R&D, improving personnel competence, and perfecting laws and regulations. Through case studies of financial enterprises and government agencies, it points out that issues in security management and personnel awareness still need improvement. In the future, intelligent and automated assessment and the broad application of assessment results will be the development trends. Further research should focus on emerging technology applications, cross-domain resource integration, and legal safeguards to continuously optimize assessment effectiveness, solidify the information-security system, and safeguard national information security and social stability.

REFERENCES

[1] Chen, J., Zhang, X., Wu, Y., Ghosh, S., Natarajan, P., Chang, S. F., & Allebach, J. (2022). One-stage object referring with gaze estimation. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 5021-5030).

[2] Tan, C., Gao, F., Song, C., Xu, M., Li, Y., & Ma, H. (2024). Highly Reliable CI-JSO based Densely Connected Convolutional Networks Using Transfer Learning for Fault Diagnosis.

[3] Zhuang, R. (2025). Evolutionary Logic and Theoretical Construction of Real Estate Marketing Strategies under Digital Transformation. Economics and Management Innovation, 2(2), 117-124.

[4] Zhang, Jingbo, et al. "AI-Driven Sales Forecasting in the Gaming Industry: Machine Learning-Based Advertising Market Trend Analysis and Key Feature Mining." (2025).

[5] Yang, Yifan. "Web Front-End Application Performance Improvement Method Based on Component-Based Architecture." International Journal of Engineering Advances 2.2 (2025): 24-30.

[6] Zhang, Yujun, et al. "MamNet: A Novel Hybrid Model for Time-Series Forecasting and Frequency Pattern Analysis in Network Traffic." arXiv preprint arXiv:2507.00304 (2025).

[7] Peng, Qucheng, Chen Bai, Guoxiang Zhang, Bo Xu, Xiaotong Liu, Xiaoyin Zheng, Chen Chen, and Cheng Lu. "NavigScene: Bridging Local Perception and Global Navigation for Beyond-Visual-Range Autonomous Driving." arXiv preprint arXiv:2507.05227 (2025).

[8] Guo, Y. (2025). The Optimal Trajectory Control Using Deterministic Artifi cial Intelligence for Robotic Manipulator. Industrial Technology Research, 2(3).

[9] Yang, J., Wang, Z., & Chen, C. (2024). GCN-MF: A graph convolutional network based on matrix factorization for recommendation. Innovation & Technology Advances, 2(1), 14–26. https://doi.org/10.61187/ita.v2i1.30

[10] We, X., Lin, S., Pruś, K., Zhu, X., Jia, X., & Du, R. (2025). Towards Intelligent Monitoring of Anesthesia Depth by Leveraging Multimodal Physiological Data. International Journal of Advance in Clinical Science Research, 4, 26–37. Retrieved from https://www.h-tsp.com/index.php/ijacsr/article/view/158
[11] Zhang, Wenqing, et al. "Enhancing Logical Reasoning in Large Language Models via Multi-Stage Ensemble Architecture with Adaptive Attention and Decision Voting." Proceedings of the 2024 5th International Conference on Big Data Economy and Information Management. 2024.
[12] Zhou, J., & Cen, W. (2024). Investigating the Effect of ChatGPT-like New Generation AI Technology on User Entrepreneurial Activities. Innovation & Technology Advances, 2(2), 1–20. https://doi.org/10.61187/ita.v2i2.124