Research on Decision Support Service Models and Strategies for University Libraries: Postprint

Authors: Zhang Xu, Zhang Xiangxian, Lu Heng

Date: 2023-07-26T00:00:00+00:00

Abstract

[Purpose/Significance] To address the practical challenge that decision support services in university libraries are still in their nascent stage and lack systematic theoretical guidance for service enhancement, this study constructs a decision support service model for university libraries to provide a reference framework for development strategies.

[Method/Process] Employing grounded theory methodology, six university libraries were selected, and 40 respondents comprising both decision support service personnel and decision-making users were identified for in-depth interviews. Drawing upon resource-based theory and decision process theory respectively, the study systematically examined the resource foundations of university library decision support services and related elements such as user needs, and subsequently analyzed the typical structural relationships among these elements.

[Results/Conclusion] From the three dimensions of resources, services, and demands, a university library decision support service model encompassing 21 categories and 9 core categories was constructed. Based on this model, service strategies were proposed, including emphasizing the construction of heterogeneous resources, providing multi-level decision support services, and taking basic resource needs as the entry point.

Full Text

Preamble

Security Control and Management of National Academic Information Resources in Cloud Computing Environment

Wan Li[1], Hu Changping[2]
[1]School of Journalism & Communication, Nanchang University, Nanchang 330031
[2]School of Information Management, Wuhan University, Wuhan 430072

Abstract

[**Purpose/Significance**] This study constructs a security control framework for national academic information resources in cloud computing environments to provide references for safeguarding these resources. [**Method/Process**] Drawing upon the human-machine-environment organic unity from traditional complex system safety control theory and the people-operation-technology model from the Information Assurance Technical Framework (IATF), combined with key domains and governance domains of information security control in cloud computing environments, this paper builds a security control framework for national academic information resources in cloud computing environments. [**Result/Conclusion**] The key domains involved in national academic information resource security in cloud computing environments include personnel management, control strategy, and security assessment. The framework encompasses both security control measures for national academic information resources in cloud computing environments and effectiveness measurements of these controls.

Keywords: academic information resources; security control; security management; information resource security
Classification Number: G250
DOI: 10.13266/j.issn.0252-3116.2019.07.001

1. Introduction

Currently, research on security control of academic information resources in cloud computing environments remains scarce. There is a need to construct a framework for national academic information resource security control in cloud computing environments by reviewing information security control practices both domestically and internationally, and by incorporating the characteristics of academic information resources. This framework will inform management and control strategies for safeguarding national academic information resources in cloud computing environments. Research on information security control in cloud computing environments has primarily focused on the following aspects:

1.1 Information Security Control Standards and Classification

The National Institute of Standards and Technology (NIST) classifies information security controls by first determining the impact level of information systems and then applying baseline security control sets from relevant standards. NIST's Special Publication 800 series addresses hot topics in computer security and has become a primary standard guiding information security construction in the United States, with applications in finance, defense, healthcare, and other domains, forming a relatively mature security control system [1]. NIST defines controls that can be categorized into three major types: technical, operational, and management, which are further subdivided into 18 families. NIST SP 800-53r4 specifies detailed security controls involving policies, oversight, personnel conduct, operations, and information systems. The security control families in-

clude access control, awareness and training, audit and accountability, security assessment and authorization, contingency planning, incident response, personnel security, risk assessment, and system and information integrity [3-4].

ISO/IEC 27003, developed by the ISO/IEC JTC1 technical committee, provides implementation guidelines for information security management systems, aiming to support the information security management process and ensure that stakeholder information assets meet organizationally defined acceptable risk levels [2]. These information security standards serve as important references for information security control in cloud computing environments.

1.2 Cloud Business Security Control Research

ISO/IEC 27017, "Information Technology—Security Techniques—Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services," provides cloud service providers with development directions for secure cloud services and serves as a standard document for accepted protection controls, proposing control models to address cloud service risks [5-6]. The U.S. government's Federal Risk and Authorization Management Program (FedRAMP) defines cloud computing security control requirements, primarily covering vulnerability scanning, conflict monitoring, and logging [7]. The Cloud Security Alliance (CSA) has released a cloud security control matrix to meet cloud industry information security needs. Based on the lifecycle, this matrix defines security control planning, implementation, assessment, and maintenance to guide security control selection at different stages and in different domains [8].

Security controls based on different domains represent best practices for effective cloud security assurance. However, more complex controls are not necessarily better; the optimization goal is to adopt simple yet effective measures. Therefore, reasonable and cost-effective security controls should be implemented. Furthermore, new challenges such as emerging vulnerabilities and attacks require continuous security improvement, disclosure of new vulnerabilities, and remediation. Security controls and procedures must be continuously reviewed and improved to support mission changes and respond to evolving threats [8]. Corresponding security control measures should be formulated for different stages and domains in cloud computing environments to reduce information security risks.

1.3 Security Controls for Different Cloud Service Delivery Models

The CSA's Consensus Assessments Initiative Questionnaire (CAIQ) focuses on providing an industry-accepted approach to documenting security controls for IaaS, PaaS, and SaaS products while ensuring transparency [9]. The CSA has also constructed a cloud service security reference model that maps IaaS, PaaS, and SaaS models to security control and compliance models, covering application, data information, management, network, trusted computing, computing and storage, and physical layers. This provides a reference for national aca-

demic information resource cloud service security control from the perspective of different cloud service delivery models [10].

In essence, security controls are countermeasures or measures for security assurance that prevent, deter, respond to, and recover from security risks. Control classification is diverse and requires tailored solutions based on different control objects, typically involving technical, management, and operational categories. Traditional security control has formed mature theories and practices, laying the foundation for information security control in cloud computing environments. Overall, traditional security control exploration provides a basis for research on national academic information resource security control in cloud computing environments, offering references for framework construction, technologies, and measures. Cloud computing security control must build upon traditional IT environment mechanisms while addressing cloud-specific information security risks and proposing control recommendations around key cloud security domains to provide secure cloud services. Since simply transplanting traditional network security technical measures is insufficient, research on cloud-specific key security risk issues is necessary.

2. Framework Construction for National Academic Information Resource Security Control in Cloud Computing Environments

National academic information resource cloud service construction in cloud computing environments faces choices among different cloud service delivery and deployment models. Current cloud products have already exhibited various consumption model combinations and service form changes. Different consumption models and service forms entail significant differences in security risks and the scope and responsibilities of security controls [11]. Cloud deployment models for national academic information resources can be categorized as public cloud, private/community cloud, and hybrid cloud. The hybrid cloud deployment model is adopted, where infrastructure is shared between two or more clouds, requiring cross-cloud scheduling during resource sharing. Accessing both public and private cloud components makes security control more difficult than in other deployment models.

National academic information resource security control in cloud computing environments is not a simple cloud technology-based solution but requires targeted controls addressing the characteristics and problems of national academic information resources in cloud environments. At different cloud service delivery model layers, cloud service providers and users bear different information security assurance responsibilities and scopes. In IaaS mode, cloud service providers primarily implement security controls to protect underlying infrastructure and abstraction layers. In PaaS environments, security control scope falls between IaaS and SaaS, with providers securing the platform itself while users are responsible for their developed cloud applications. In SaaS environments, security

control scope and measures can be confirmed through Service Level Agreements (SLAs), with content negotiated between users and providers to delineate respective security control responsibilities. Comparison of the three delivery models reveals that higher-level cloud services entail greater provider responsibility and increased user dependence on provider controls.

Not all security requirements are equivalent in cloud computing environments. Based on different security needs and information systems, security control priorities vary. For the public cloud portion of national academic information resources, confidentiality controls emphasize integrity and availability, while for the private cloud portion, they emphasize confidentiality and feasibility. Therefore, security controls can be prioritized and baselined according to different deployment models.

National academic information resource security assurance in cloud computing environments is a complex systems engineering endeavor with intricate hierarchical structures and information and capability interactions. Complex system functional intrinsic safety lies in achieving structural intrinsic safety, maintaining system structure and boundary stability, and ensuring human-machine-environment safety during micro-level information and capability interactions. Drawing on traditional complex system safety control theory's human-machine-environment organic unity and IATF's people-operation-technology model, combined with key and governance domains of information security control in cloud computing environments, this paper constructs a security control framework for national academic information resources in cloud computing environments [Figure 1: see original paper] [10,12-14]. The framework highlights critical aspects including personnel management, risk management, security baseline construction, emergency response, compliance auditing, and information security assessment. It encompasses both security control measures and their effectiveness measurements.

3. Personnel Management for National Academic Information Resources in Cloud Computing Environments

National academic information resource cloud platform construction requires scientific planning by government information agencies and coordinated organization among relevant departments at various levels. Implementation must be refined layer by layer through networks and regions. The construction involves numerous stakeholders.

3.1 National-Level Participant Security Management

National academic information resource security in cloud computing environments constitutes an important component of national information security. The construction of national academic information resources faces shared resource pools, and once the cloud platform is compromised, numerous academic information resource service institutions are threatened. If attackers exploit

cloud platform vulnerabilities to steal, modify, or delete academic information resources stored in the cloud, losses will extend beyond the academic domain to potentially threaten national security. Therefore, security depends on national macro-level guidance for managing and supervising national academic information resource cloud services.

China attaches great importance to information security assurance, having established the National Informatization Leading Group to strengthen informatization construction and maintain national information security. Implementation is managed through the National Information Service Management Coordination Committee, which coordinates division of labor among academic information resource service institutions involved in cloud services, clarifies responsibilities, and formulates cooperation policies.

National-level security management can effectively control organizational obstacles to national academic information resource sharing and geographical obstacles to cross-regional resource integration. Planning the overall organizational structure at the national level clarifies resource organization and scheduling for sharing, strengthening security assurance through cooperative division of labor and organizational coordination. Additionally, establishing supervisory bodies for cloud service construction and issuing relevant standards and laws can further regulate cloud service industry and provider behaviors.

3.2 Regional-Level Participant Security Management

Regional-level management involves the meso level, following national guidelines to construct regional academic information resource cloud service centers, formulate detailed regional security management policies, coordinate division of labor among different institutions, and strengthen management of cloud service providers and the industry. China has accumulated experience in academic information resource sharing under traditional network environments. For example, as an initiating organization, Guangdong Provincial Sun Yat-sen Library built a joint reference consultation network involving numerous domestic public libraries, providing reference consultation and document delivery services [15]. Guangdong's reference consultation service, launched in 2001, united commercial academic information resource providers and libraries both domestic and international. In 2003, it built its own online reference consultation platform, gradually achieving resource sharing and user service openness. During construction, Guangdong provided necessary policy and management support for provincial resource sharing, establishing the Guangdong Provincial Cross-System Joint Digital Reference Consultation Steering Committee to oversee standard system construction, with relevant government departments responsible for supervision and coordination [16].

Regional-level participant management requires establishing regional academic information resource security management departments and setting up regional security management teams to organize and manage cloud computing environ-

ment construction. This involves developing sharing management specifications, clarifying responsibilities of participating institutions, and coordinating division of labor. Regional cloud service technical teams provide guidance on technical application problems, develop standard systems (e.g., cloud application development standards, metadata standards, service standards), and solve technical challenges. Resource management teams are responsible for cloud service center resource scheduling, unified work specifications, data organization and configuration, and quality and usage supervision. Audit and supervision teams oversee security monitoring and auditing during construction, evaluating management specifications and control strategies to continuously improve the security system. Expert guidance teams comprising representatives from academic institutions, government departments, and cloud service providers offer recommendations to enhance security controls. The regional-level participant security management architecture is shown in [Figure 2: see original paper].

3.3 Micro-Level Participant Security Management

Micro-level participants primarily include academic information resource service institutions, cloud service providers, network operators, communication service providers, and other supply chain service providers [Figure 3: see original paper]. Network operators provide network connectivity and certain network security protections. To meet elastic demands of academic institutions, virtual machines supporting cloud service functions require recreation and migration, making them relatively vulnerable during migration and necessitating joint participation of network operators, communication service providers, and cloud service providers in security protection and control.

All services used by academic information resource institutions—cloud computing, communication, network—are purchased through service providers, forming direct buyer-seller relationships. During transactions, both parties reach consensus on security issues and are bound by contractual agreements. The focus of micro-level participant management lies in building trust relationships between academic institutions and service providers. During cloud service construction, reliable trust relationships and constraint mechanisms can be established to bind responsibilities and obligations, promoting cooperation toward predetermined goals. Whether in cloud or network environments, agreements between users and service providers are effective management methods. Service Level Agreements (SLAs), negotiated between providers and users, define obligations and responsibilities to achieve continuous service objectives and represent an important means of trust management for national academic information resource cloud services.

4. Full-Process Control Strategies for National Academic Information Resource Security in Cloud Computing Environments

Full-process control strategies for national academic information resource security in cloud computing environments focus on security risk management, security baseline construction, security monitoring and emergency response, and security compliance auditing.

4.1 Security Risk Management

National academic information resource systems in cloud computing environments still face objective information system security risks. Targeted control measures can be adopted through security risk assessment. Risk control constitutes a key component of security control, requiring that cloud service information system security risks be limited to controllable ranges to enhance security assurance. The risk management approach involves identifying risk domains and factors based on resource distribution, observing and collecting risk factor data, analyzing it using quantitative tools, and formulating security policies and measures based on risk assessment to effectively control risks [18].

A controlled cloud information system comprises networks, personnel, operating environments, and business applications. Due to information security risks, asset vulnerabilities, and security threats in cloud computing environments, security risks must be observed and assessed to transform them into controllable risks. Residual risks undergo further cycles of observation and assessment to develop security control strategies, which are continuously improved to reduce risks until all output risks fall within acceptable ranges. Risk assessment generally includes risk identification, analysis, and evaluation. Risk analysis encompasses assets, threats, and vulnerabilities. Asset categories and values are first determined, followed by analysis of threat types and frequencies, vulnerability level assignment, and finally, comprehensive verification to estimate accident probabilities and potential losses.

4.2 Security Baseline Construction

The construction of national academic information resource cloud service platforms involves multiple stakeholders. If numerous resource institutions adopt cloud services from different providers, they must address complex network structures and diverse server types. Therefore, maintenance cannot rely solely on traditional information system approaches while ignoring cloud-specific characteristics and requirements. Security assurance must establish relevant baseline specifications for implementing controls.

The U.S. FedRAMP program conducts cloud security management research, emphasizing cloud security baseline construction and developing the "FedRAMP Cloud Security Controls," which provides references for China's national aca-

demic information resource security baseline construction [19]. Cloud security baseline construction requires expansion beyond traditional security. FedRAMP's baseline transitions from traditional NIST SP 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations" to cloud-adapted security controls.

Referencing NIST SP 800-53r4 and FedRAMP 2.0, baseline construction should include at least 17 security control families: access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, and system and information integrity. NIST SP 800-53r4 expands access control and system/services acquisition to cover cloud computing and supply chain security requirements [4,20].

Baseline construction is a complex systems engineering task. COBIT (Control Objectives for Information and Related Technology) is an IT governance framework that enables managers to establish associations among information security control objectives, technologies, and risks, providing clear strategic and practical guidance. COBIT can serve as a foundation for baseline development, having been mapped to many information security standards with components directly applicable or adaptable to cloud computing environments. Baseline establishment must combine cloud security risks and information system lifecycle planning. Academic institutions and cloud service providers must apply existing laws, standards, and specifications to develop and select controls, considering cloud service system security, business process security, and cloud environment security. The baseline should be business-system-oriented, with different protections based on business system characteristics. Business systems should be decomposed into modules (e.g., databases, operating systems, network devices) for refined security control baseline development.

Baseline construction must first distinguish baseline requirements corresponding to different security needs, establishing three-level baselines (high, medium, low) based on security requirements. For requirements beyond these levels, factors such as operating environment, operational characteristics, system functions, threat types, and information types should be considered. The scope of control measures must be clarified—cloud information security baselines should not be overly complex but should consider control objectives, operating environments, and technical conditions, emphasizing protection of critical business operations and operations.

4.3 Security Monitoring and Emergency Response

Full-process security monitoring seeks optimal control solutions through data collection on security-related activities and practices, enabling accident predic-

tion, early warning, and emergency response based on security forecasts. This achieves both pre-accident prevention and post-accident control.

Security monitoring collects, analyzes, and reports security event data from cloud information systems and service processes, involving user, application, and system activities. Collected security-related data is aggregated to provide quantitative references for security event assessment and maintain events within reasonable ranges. The monitoring and feedback process [21] is shown in [Figure 4: see original paper].

Security monitoring serves as a crucial component of control strategies, enabling security risk detection. Cloud technologies and academic resource aggregation make national academic information resources attractive targets. Since some attacks cannot be anticipated, real-time monitoring is an effective countermeasure. Real-time monitoring data collection, analysis, and evaluation enable timely controls, while response measures prevent attacker damage and minimize losses. Post-response activities involve timely repair of security vulnerabilities, reinforcement of the security protection system, and report generation to reduce recurrence and provide evidence for accountability.

Emergency response is a vital link in the overall security protection cycle, divided into pre-response, during-response, and post-response phases. Pre-response involves developing security response measures under the guidance of security control strategies, establishing accident handling procedures, and classifying accident types. National academic information resource security accidents primarily involve system failures, data loss and leakage, denial of service, and insecure APIs. Contingency plans must be developed for different accident types. During-response involves identifying security issues based on monitoring data and implementing response measures. Post-response involves vulnerability repair and system reinforcement.

Emergency response execution requires personnel involvement to connect relatively independent strategies, protection, monitoring, and response, implementing information security control solutions. Implementation requires personnel management to enhance professional competence and emergency response capabilities to address dynamic changes in security accidents, enable timely processing and protection, and compensate for model and measure deficiencies.

4.4 Security Compliance Auditing

Compliance auditing plays an important role in traditional outsourcing relationships. In cloud computing environments, cloud service providers and academic institutions face challenges in establishing and monitoring continuous compliance of information security controls. Compliance and auditing primarily involve internal policy compliance, legal compliance, and external audit coordination, establishing objectives through internal and external processes to clarify compliance with user contracts, laws, regulations, and standards, and whether strategies, procedures, and processes are effectively implemented.

Cloud service providers must comply with diverse IT process control requirements, including internal and external demands. Numerous compliance requirements form complex relationships, with inevitable repetitive non-compliant controls appearing during audits or security events. Compliance efforts can unify these requirements to improve efficiency and meet multiple compliance demands. In the long term, individual compliance efforts will be replaced by overall IT process compliance.

Compliance must be organically integrated with operational risk and internal controls. KPMG proposes a three-lines-of-defense mechanism: the first line involves risk identification, assessment, and monitoring through compliance management and internal controls; the second line optimizes combinations of compliance management, internal controls, and risk mitigation; the third line integrates methods, processes, and standards used in internal auditing [22]. Cloud service providers and academic institutions can adopt the Governance, Risk, and Compliance (GRC) concept to design continuous, formal compliance procedures for national academic information resource cloud security construction.

4.5 Security Assessment

Cloud computing information system security assessment builds upon traditional information system security evaluation. National academic information resource security assessment in cloud computing environments must 借鉴 traditional processes and methods. Traditional assessment has developed long-term, forming a series of norms and guidelines, from the U.S. "Trusted Computer System Evaluation Criteria" [23] to the UK's BS7799-1:1999 (ISO/IEC 17799:2000) [24] and NIST SP 800-53A [25], all providing references for cloud computing security assessment.

The "Trusted Computer System Evaluation Criteria" classifies security protection capabilities into seven levels, providing standards for computer security assessment. However, published earlier, it focuses on technical requirements and information access control, making it difficult to extend to new environments. ISO/IEC 17799:2000 provides an information security management system, proposing a continuous improvement model through plan-do-check-act processes and enumerating control measures to guide information security level protection. NIST SP 800-53A provides guidelines for assessing security controls in federal information systems.

Overall, cloud security assessment has not yet formed a unified system. Organizations have conducted explorations based on traditional assessment, focusing primarily on cloud service provider security capability requirements and cloud platform security standards. Applying cloud computing to national academic information resource storage and services requires continuous security assessment to reduce adoption risks and improve overall protection capabilities. Assessment must overcome challenges brought by cloud computing technologies, including virtualization, data security, application security, physical secu-

rity, multi-tenancy, system security, and network security. Unlike traditional assessment environments, cloud assessment must be conducted in large-scale, heterogeneous technology, mixed physical and virtual, and multi-tenant shared environments.

China has promulgated the "Regulations on the Security Protection of Computer Information Systems" and comprehensively promoted level protection. Traditional information system security assessment standards have developed over a long period, forming a relatively mature level assessment system that provides a good foundation for cloud assessment work. Security level assessment is a mature method in the information system security assessment field, with the state promulgating relevant standards as assessment bases for information systems. Referencing traditional level assessment processes [26-28], this paper constructs a cloud security assessment workflow for national academic information resources, shown in [Figure 5: see original paper].

The assessment process is divided into four phases: preparation, plan development, on-site assessment, and results analysis/reporting. The preparation phase initiates the project, establishes assessment teams, and collects data on the current state of national academic information resource cloud information systems. The plan development phase determines assessment content and develops assessment plans. The on-site assessment phase implements the plan and records results. The results analysis phase analyzes and summarizes findings, generates assessment reports, and provides feedback. Throughout the process, multi-stakeholder collaboration and communication among participants in national academic information resource cloud services are required to ensure assessment effectiveness.

5. Conclusion

Drawing upon the human-machine-environment organic unity from traditional complex system safety control theory and the people-operation-technology model from the Information Assurance Technical Framework, combined with key and governance domains of information security control in cloud computing environments, this paper constructs a security control framework for national academic information resources in cloud computing environments. The framework identifies key domains including personnel management, control strategy, and security assessment, encompassing both security control measures and their effectiveness measurements. The paper analyzes these key domains and proposes optimization measures to provide references for organizing and implementing national academic information resource security assurance in cloud computing environments.

References

[1] Wang Huili, Yang Chen, Zhang Mingtian, et al. Research on SP800 series information security standards [J]. Information Technology & Standardization,

2011(5): 65-69.

[2] ISO/IEC-27003(CN) Information Technology—Security Techniques—Information Security Management System Implementation Guidelines [EB/OL]. [2018-07-04]. https://wenku.baidu.com/view/53ff26b6dd3a32d737581dd.html.

[3] Winkler J. Cloud Security: Architecture, Strategy, Standards and Operations [M]. Translated by Liu Gezhou, et al. Beijing: China Machine Press, 2012.

[4] Security and Privacy Controls for Federal Information Systems and Organizations [EB/OL]. [2018-07-04]. http://go.thalesesecurity.com/rs/480-LWA-970/images/NIST-Special-Publication-800-53-Revision-4.pdf.

[5] ISO/IEC 27017:2015 Information Technology—Security Techniques—Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services [EB/OL]. [2018-07-17]. https://www.iso.org/standard/43757.html.

[6] ISO/IEC 27017 Extending ISO/IEC 27001 into the Cloud [EB/OL]. [2018-07-17]. https://www.bsigroup.com/Documents/iso-27017/resources/ISO-27017-overview.pdf.

[7] FedRAMP. Security Assessment Framework [EB/OL]. [2018-07-17]. https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/01/FedRAMP-Security-Assessment-Framework-v2-1.pdf.

[8] CSA CCM V3.0.1 [EB/OL]. [2018-07-17]. https://cloudsecurityalliance.org/search/?s=Cloud+Controls+Ma

[9] CAIQ (Consensus Assessments Initiative Questionnaire) [EB/OL]. [2018-10-21]. https://searchcloudsecurity.techtarget.com/definition/CAIQ-Consensus-Assessments-Initiative-Questionnaire.

[10] Security Guidance for Critical Areas of Focus in Cloud Computing v3.0 [EB/OL]. [2018-07-17]. https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.

[11] Hu Changping, Lü Meijiao. Research status and problems of national academic information resource security assurance organization in cloud environments [J]. Information Studies: Theory & Application, 2017, 40(11): 10-16.

[12] Wang Ying, Wang Song. Risk Transmission and Control of Complex Systems [M]. Beijing: National Defense Industry Press, 2015.

[13] Yu Wenjin, Li Jianjun. Network security design and construction based on IATF [J]. Information Security and Communications Privacy, 2010(1): 122-125.

[14] Cloud Security Control Matrix CCM Chinese-English Version [EB/OL]. [2018-06-29]. https://max.book118.com/html/2018/0303/155631961.shtm.

[15] Zhao Yanlong. Functional characteristics of the UCDRS system and its application in library joint reference consultation service networks [J]. Digital Library Forum, 2006(7): 66-68.

[16] Hu Junrong. Constructing a cross-system joint digital reference consultation service network platform [J]. Library and Information Service, 2006, 50(5): 83-87.

[17] Chen Chi, Yu Jing, et al. Cloud Computing Security System [M]. Beijing: Science Press, 2014.

[18] Wang Zhenxue. Information System Security Risk Estimation and Control Theory [M]. Beijing: Science Press, 2011.

[19] Zhao Zhangjie, Liu Haifeng. Analysis of U.S. federal government cloud computing security strategy [J]. Information Network Security, 2013(2): 1-4.

[20] Zhou Yachao, Zuo Xiaodong. Cloud baseline under cybersecurity review system [J]. Information Security and Communications Privacy, 2014(8): 42-44.

[21] Li Tianfeng, Yao Xin, Wang Jinsong. Research on large-scale network anomalous traffic real-time cloud monitoring platform [J]. Information Network Security, 2014(9): 1-5.

[22] KPMG Banking Operational Risk Seminar. Organic integration of operational risk management with internal control and compliance management [EB/OL]. [2018-06-29]. https://wenku.baidu.com/view/8c790dfe03d276a20029753e0912a2167c98.html?from=s

[23] Trusted Computer System Evaluation Criteria [EB/OL]. [2018-06-29]. https://en.wikipedia.org/wiki/Trusted_{{{Computer}}*{{System}}}*{{{Evaluation}}_{{Criteria}}}.

[24] BS7799-1:1999 Information Security Management [EB/OL]. [2018-06-29]. http://doc.mbalib.com/view/8448db6df953cf0870802975331ebf51.html.

[25] NIST Special Publication 800-53A, Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations [EB/OL]. [2018-06-29]. https://www.nist.gov/itl/nist-cloud-computing-related-publications.

[26] Information Security Technology—Guidelines for Information System Security Level Protection Assessment Process [EB/OL]. [2018-06-29]. http://tds.antiy.com/biaozhun/6/index.html.

[27] Xiao Guoyu. Practice of information system level protection assessment [J]. Information Network Security, 2011, 36(7): 86-88.

[28] Yang Lei, Guo Zhibo. Level assessment of information security level protection [J]. Journal of Chinese People's Public Security University (Science and Technology), 2007, 13(1): 50-53.

Author Contributions

Wan Li: Drafted and revised the manuscript.
Hu Changping: Proposed the research topic and guided the writing.

Security Control and Management of National Academic Information Resources in Cloud Computing Environment

Wan Li[1], Hu Changping[2]
[1]School of Journalism & Communication, Nanchang University, Nanchang 330031
[2]School of Information Management, Wuhan University, Wuhan 430072

Abstract: [Purpose/significance] To provide references for national academic information resources security in cloud computing environments, this paper aims to construct a security control framework for national academic resources in cloud computing environments. [Method/process] Based on Human-Machine-Environment organic unity in conventional complex system safety control theory and Information Assurance Technical Framework that combines "the people, the operation, the technology," this paper integrates the key domain and governance domain in information security guarantee to construct the above security control framework. [Result/conclusion] Under the cloud computing environment, the key domains in national academic information resources security include personnel management, control strategy, and safety assessment. The framework contains not only the national academic information resources security strategy, but also effectiveness measurements of it.

Keywords: academic information resources; security control; security management; information resources security

Note: Figure translations are in progress. See original paper for figures.