Security Control and Management of National Academic Information Resources in Cloud Computing Environments: Postprint

Authors: Wan Li, Hu Changping

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

Abstract

[Purpose/Significance] To construct a security control framework for national academic information resources in cloud computing environments, providing reference for the security assurance of national academic information resources in such contexts. [Method/Process] Drawing upon the organic integration of human, machine, and environment from traditional complex systems security control theory, as well as the human, operations, and technology model from the Information Assurance Technical Framework (IATF), and combining the key domains and governance domains of information security control in cloud computing environments, a security control framework for national academic information resources in cloud computing environments is constructed. [Results/Conclusion] The key areas involved in the security of national academic information resources in cloud computing environments include comprehensive personnel management, control strategies, and security evaluation; the security control framework for national academic information resources in cloud computing environments encompasses both security control measures for national academic information resources in such contexts and the effectiveness measurement of these security control measures.

Full Text

Preamble

ChinaXiv Partner Journal
Volume 63, Issue 7, April 2019

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

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 integration concept 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 for 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**] Key domains involved in national academic information resources security in cloud computing environments include personnel management, control strategies, and security assessment. The framework encompasses both security control measures for national academic information resources in cloud computing environments and effectiveness measurements for these controls.

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

1. Research on Information Security Control in Cloud Computing Environments

Currently, research on security control for academic information resources in cloud computing environments remains scarce. There is a need to construct a framework for national academic information resources security control in cloud computing environments by reviewing domestic and international information security control practices and integrating the characteristics of academic information resources, thereby proposing management and control strategies for safeguarding these resources. Research on information security control in cloud computing environments primarily focuses 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 relatively mature security control system applied across finance, defense, healthcare, and other sectors. NIST defines controls in three major categories: technical, operational, and management, which are further

subdivided into 18 families. NIST SP 800-53r4 details security controls covering policies, oversight, personnel behavior, operations, and information systems. The control families include 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.

ISO/IEC 27003, "Information Technology—Security Techniques—Information Security Management Systems Implementation Guidelines," developed by ISO/IEC JTC1, supports the information security management process to ensure that stakeholders' information assets meet organizationally defined acceptable risk levels. These information security standards provide important references for information security control in cloud computing environments. NIST SP 800-53 indicates that security controls require security classification of information systems, applying relevant baseline control sets from standards.

1.2 Security Control Research for Cloud Business

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. 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. The Cloud Security Alliance (CSA) released a cloud security control matrix to meet industry information security needs, defining security control planning, implementation, assessment, and maintenance based on the lifecycle to guide security control selection across different stages and domains.

Security controls based on different domains approximate best practices and 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, continuously emerging challenges such as new 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. Corresponding security control measures should be formulated for different stages and domains in cloud computing environments to reduce information security risks.

1.3 Security Control Research Under Different Cloud Service Delivery Models

The CSA's Consensus Assessments Initiative Questionnaire (CAIQ) focuses on documenting security controls for IaaS, PaaS, and SaaS products in an industry-recognized manner while ensuring control transparency. The CSA has constructed a cloud service security reference model that maps IaaS, PaaS, and SaaS models to security control and compliance models. The security control model includes application, data information, management, network, trusted computing, computing and storage, and physical layers, describing key aspects of cloud service security controls from a control perspective and providing references for national academic information resources cloud service security controls across different delivery models.

Essentially, security controls are countermeasures or measures for security assurance that prevent, deter, respond to, and react to 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 theories and practices have matured, laying the foundation for information security control in cloud computing environments. Overall, traditional security control exploration provides references for constructing national academic information resources security control systems in cloud computing environments regarding control structure, technology, and measures. Cloud computing security control must build upon traditional IT environment mechanisms while addressing cloud-specific 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 critical security risk issues is necessary.

2. Construction of the Security Control Framework for National Academic Information Resources in Cloud Computing Environments

The construction of national academic information resources cloud services in cloud computing environments faces choices among different cloud service delivery and deployment models, with cloud products already presenting various consumption model combinations and service form changes. Different consumption models and service forms entail significant differences in security risks and control scope and responsibilities. Cloud deployment models for national academic information resources can be categorized as public cloud, private/community cloud, and hybrid cloud. National academic information resources adopt a hybrid cloud deployment model, where infrastructure is shared across multiple clouds requiring cross-cloud scheduling. Accessing both public and private cloud components makes security control more difficult than other deployment models. Security control for national academic information resources in cloud

computing environments is not simply a cloud technology-based solution but requires targeted controls addressing the characteristics and problems of these resources.

Different cloud service delivery model layers entail varying information security assurance responsibilities and scopes between cloud service providers and users. In IaaS mode, providers primarily control security to protect underlying infrastructure and abstraction layers. In PaaS environments, control scope lies between IaaS and SaaS, with providers securing the platform itself while users are responsible for developed cloud applications. In SaaS environments, control scope and measures can be confirmed through Service Level Agreements (SLAs), with content negotiated between users and providers to delineate responsibilities. Comparison across the three models shows that higher service layers correspond to greater provider responsibility and user dependence on provider controls.

Not all security needs are equivalent in cloud computing environments. Based on different security requirements and information systems, 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 resources security assurance in cloud computing environments is a complex systems engineering challenge 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, and environment safety during micro-level information and capability interactions. Drawing upon traditional complex system safety control theory's human-machine-environment organic integration and IATF's people-operation-technology model, combined with cloud computing information security control key domains and governance domains, 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 effectiveness measurements for national academic information resources in cloud computing environments.

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

National academic information resources cloud platform construction requires governmental scientific planning and coordinated organization across relevant

departments at all levels. Implementation must be refined layer by layer through networks and regions, involving numerous stakeholders.

3.1 National-Level Participant Security Management

National academic information resources security in cloud computing environments constitutes an important component of national information security. The construction of these resources aims for sharing and co-construction with relatively centralized resources; 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, losses to the academic field and even national security may result. Therefore, security depends on national macro-level guidance for managing and supervising 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 management can effectively control organizational and geographical obstacles to resource sharing and integration. Planning the overall organizational structure at the national level clarifies resource organization and scheduling for sharing and co-construction, strengthening security assurance through cooperative division of labor and organizational coordination. Establishing supervisory bodies for cloud service construction and issuing relevant standards and laws further regulates cloud service industry and provider behavior.

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 and co-construction under traditional network environments. The Guangdong Provincial Sun Yat-sen Library, as an initiating organization, built a joint reference consultation network involving numerous domestic public libraries to provide reference and document delivery services. Guangdong's reference consultation service, launched in 2001, united commercial academic information resource providers and domestic and international libraries. 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 Inter-System Joint Digital Reference Consultation Steering Committee to standardize and supervise coordination among participating institutions, providing a reference for regional participant management.

Regional-level management requires establishing departments responsible for regional academic information resource security and setting up regional security management groups to organize and manage cloud computing environment construction. This involves formulating sharing and co-construction management norms, clarifying responsibilities of participating institutions, and coordinating division of labor. Regional technical groups provide guidance on technical application issues, develop standard systems including cloud application development standards, metadata standards, and service standards, and solve technical challenges. Resource management groups are responsible for cloud service center resource scheduling, organizing and configuring data from various institutions according to unified workflows, and supervising resource quality and usage. Audit and supervision groups oversee security and auditing during construction, monitoring operations and security incidents, assessing information security, and continuously improving the security system. Expert advisory groups comprising representatives from academic institutions, government agencies, and cloud providers provide 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 security protections. To meet elastic demands of academic institutions, virtual machines supporting cloud functions require recreation and migration, making them vulnerable during migration and necessitating joint participation of network operators, communication service providers, and cloud providers in security protection and control.

Institutions using cloud, communication, and network services form direct buyer-seller relationships through service purchases. During transactions, both parties reach consensus on security issues and establish constraints through contracts. Micro-level management focuses on building trust relationships between academic institutions and service providers. Reliable trust relationships and constraint mechanisms can be established through agreements to ensure cooperation toward predetermined goals. Whether in cloud or network environments, user-provider agreements 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 for trust management in national academic information resources

cloud services.

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

Full-process control strategies focus on security risk management, security baseline construction, security monitoring and emergency response, and compliance auditing.

4.1 Security Risk Management

National academic information resource systems in cloud computing environments still face objective security risks that can be addressed through targeted control measures based on risk assessment. Risk control is a key component that must limit security risks to controllable ranges. The risk management approach involves determining risk domains and factors based on resource distribution, observing and collecting risk factor data, analyzing them with quantitative tools, and formulating security policies and measures based on assessment results to effectively control risks.

The controlled cloud information system comprises networks, personnel, operating environments, and business applications. Due to information security risks, asset vulnerabilities, and security threats, observation and assessment transform security risks into controllable ones, with residual risks cycled through repeated observation and assessment to develop control strategies. This continuous improvement process reduces security risks until all outputs fall within acceptable ranges. Risk assessment includes risk identification, analysis, and evaluation, with analysis covering assets, threats, and vulnerabilities. It involves judging asset categories and values, analyzing threat types and frequencies, assigning vulnerability values, and finally estimating accident probabilities and potential losses based on comprehensive verification of asset values, threat frequencies, and vulnerabilities.

4.2 Security Baseline Construction

The construction of national academic information resources cloud service platforms involves multiple stakeholders. If numerous resource institutions adopt different cloud services, 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 to fully utilize cloud security advantages while controlling risks, highlighting cloud security baseline construction and developing the “FedRAMP Security

Controls" document, which provides references for China's national academic information resources security baseline. Cloud security baseline construction requires expansion beyond traditional security. FedRAMP's baseline transitions from the 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 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.

Baseline construction is a complex systems engineering task. COBIT (Control Objectives for Information and Related Technology) is an IT governance framework enabling managers to establish associations between 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 environments. Baseline establishment must combine cloud security risks and information system lifecycle planning. Academic institutions and cloud providers must apply existing laws, standards, and norms 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 for different business system characteristics. Business systems should be decomposed into modules such as databases, operating systems, and network devices, with security controls refined and baselined according to business layer definitions.

Baseline construction should first distinguish baseline requirements for different security needs, constructing three-level security baselines (high, medium, low) for national academic information resources. For requirements beyond these levels, baselines should be built considering operational environments, characteristics, system functions, threat types, and information types. The role domain of control measures must be clarified—cloud information security baselines should not be more complex but should consider control objectives, operational environments, and technical conditions, emphasizing protection of critical business and operations to enable reasonable control strategy selection.

4.3 Security Monitoring and Emergency Response

Security control requires monitoring the entire information security process, collecting data on security-related activities and practices to seek optimal control solutions, achieving accident warning and emergency response based on secu-

rity predictions. This enables both pre-incident prevention and post-incident 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 is shown in [Figure 4: see original paper].

Security monitoring serves as an important control strategy component, enabling security risk detection. Cloud technologies and academic resource aggregation make national academic information resources attractive targets. Since some attacks are unpredictable, real-time monitoring is an effective countermeasure. Real-time monitoring data collection, analysis, and assessment enable timely control measures, with information security responses preventing attacker damage and minimizing losses. Post-response activities involve timely repair of security vulnerabilities, strengthening the security protection system, and generating reports to reduce recurrence and provide evidence for accountability.

Emergency response is a crucial link in the overall security protection cycle, divided into pre-response, during-response, and post-response phases. Pre-response involves developing response measures under security control strategy guidance, establishing accident handling procedures, and classifying accidents. National academic information resources security accidents primarily involve system failures, data loss and leakage, denial of service, and insecure APIs, requiring tailored emergency plans. During-response involves identifying security issues based on monitoring data and implementing response measures. Post-response involves vulnerability repair, security system reinforcement, and reporting.

Emergency response execution requires personnel involvement to connect relatively independent strategies, protections, monitoring, and responses, implementing information security control solutions. Implementation requires personnel management to improve professional quality and emergency response capabilities to address dynamic changes in security accidents, enabling timely processing and protection to 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 involve internal policy compliance, legal compliance, and external audit coordination, establishing objectives through internal and external processes to clarify compliance with 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 repetitive non-compliant controls inevitably appearing during audits or security incidents. Unified processing of internal and external requirements through compliance efforts can improve efficiency and meet multiple compliance requirements. 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 audits. 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 resources cloud security.

4.5 Security Assessment

Cloud computing system security assessment builds upon traditional information system evaluation. National academic information resources security assessment must reference traditional evaluation processes and methods, which have developed over time into numerous specifications and guidelines. From the U.S. "Trusted Computer System Evaluation Criteria" to the UK's BS7799-1:1999 (ISO/IEC 17799:2000) and the U.S. "Guide for Assessing the Security Controls in Federal Information Systems" (SP 800-53A), these provide 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 for information access control and assurance, making it difficult to extend to new environments. ISO/IEC 17799:2000 provides an information security management system with a plan-do-check-act model for continuous improvement, detailing control measures to guide information security level protection. NIST SP 800-53A provides information system assessment methods, procedures, and recommendations, clarifying evaluation of norms, behaviors, mechanisms, and personnel.

Cloud computing represents a new information system model. The U.S. "Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies" identifies privacy risks in cloud computing and uses relevant standards for risk analysis and assessment. The "Guidelines for Security and Privacy in Public Cloud Computing" analyzes threats and risks in public cloud environments and proposes countermeasures, providing important references for cloud security assessment research. The European Union Agency for Network and In-

formation Security (ENISA) proposed an information security assurance framework detailing cloud platform security indicators. The CSA's Cloud Controls Matrix 3.0 proposes basic security principles for cloud providers to guide overall security risk assessment, providing a control framework spanning 16 domains across industry standards and regulations.

Overall, cloud security assessment has not yet formed a unified system. Organizations have conducted explorations based on traditional information system assessment, focusing primarily on cloud 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 cloud computing challenges including virtualization, data security, application security, physical security, 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 developed a relatively mature hierarchical assessment system from the "Regulations on the Security Protection of Computer Information Systems" to the comprehensive promotion of classified protection, providing a solid foundation for national academic information resources security assessment. Security level assessment is a mature method in information system evaluation, using national standards as the basis and targeting information systems as the evaluation object. Referencing traditional information system security level assessment processes [26-28], this paper constructs a cloud security assessment workflow for national academic information resources [Figure 5: see original paper].

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

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 systems implementation guidelines[EB/OL]. [2018-07-04]. https://wenku.baidu.com/view/53ff26b6dd3a32d737581dd.html.

[3] Winkler V J. Securing the cloud: Cloud computer security techniques and tactics[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+Mat

[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 resources 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 thinking[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 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 the 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/8c79fdfe03d276a2002975331ebf51.html?from=sear

[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 topic and guided the writing.

English Abstract

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

Abstract: [Purpose/significance] This paper aims to construct a security control framework for national academic information resources in cloud

computing environments to provide references for safeguarding these resources. [Method/process] Based on the human-machine-environment organic integration concept 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 for information security control in cloud computing environments, this paper constructs a security control framework for national academic information resources in cloud computing environments. [Result/conclusion] Key domains involved include personnel management, control strategies, and safety assessment. The framework encompasses both security control measures and effectiveness measurements for national academic information resources in cloud computing environments.

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

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