Check for updates

Article

Journal of Librarianship and Information Science
2019, Vol. 51(1) 78–94
© The Author(s) 2016
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0961000616668572
journals.sagepub.com/home/lis

Factor identification and computation in the assessment of information security risks for digital libraries

Shuiqing Huang, Zhengbiao Han and Bo Yang
Nanjing Agricultural University, China

Ni Ren
Nanjing Agricultural University, Jiangsu Academy of Agricultural Sciences, China

Abstract

This study proposes an objective methodology for identifying and computing the factors relevant to the assessment of information security risks for digital libraries that is also compliant with the ISO 27000 and the GB/T 20984 standards. By introducing a fuzzy comprehensive assessment method and an expert investigation method to the dimensions of assets and threats, this study proposes a model for computing the value of assets and the severity of threats. In the dimension of vulnerabilities, a vulnerability computation model based on the multi-channel weighted average method is proposed. By considering the digital library of a typical public library in China as the object of assessment, this study acquires assessment data by using a combination of a questionnaire survey, an on-site survey and vulnerability scanning. Research findings consisted of the following: (1) the digital library identified a total of 3111 information security risk items; (2) according to the assessment results attained using a combination of the factor identification and computational methodologies proposed here in conjunction with the multiplicative method specified in GB/T 20984, the high-risk (or higher risk) items accounted for 0.9% of all risky items, which is consistent with the status quo in information security risks faced by digital libraries. The analysis showed that the proposed methodology is more scientific than the currently prevailing direct value assignment method.

Keywords

Asset, digital library, ISO27000, risk assessment, threat, vulnerability

Introduction

Digital libraries allow users to efficiently access resources of digitized information through network facilities and a variety of retrieval channels. Digital libraries play an increasingly important role in the daily lives of people and provide increasingly diverse contents and services (Frias-Martinez et al., 2006). Digital libraries are highly reliant on professional technologies, including computer technologies, network technologies and data communication technologies. Therefore, digital libraries are confronted with far more severe security risks than traditional libraries. An information security event may affect the operation and services of an entire digital library. In recent years, China's information security survey of digital library has indicated that information security incidents had occurred in all 30 of its digital libraries (Huang, 2011). Of these, one such incident had occurred in six libraries, two information security incidents had occurred in 10 libraries, whereas three or more incidents had occurred in the remainder. In

Corresponding author:
Zhengbiao Han, Research Center for Correlation of Domain Knowledge, College of Information Science and Technology, Nanjing Agricultural University, Nanjing, China.
Email: zbh1985@njau.edu.cn

this backdrop, a number of researchers have expressed concern for the information security of digital libraries. Related research initially focused on such security technologies as access control, and authentication and digital signature, to improve the information security status of digital libraries (Adam et al., 2002; Fox and ElSherbiny, 2011; Saeednia, 2000).

However, the cause of information security incidents in digital libraries may originate in management events, such as information security rules and regulations that are not up to standard. Merely relying on technology is insufficient to solve the problem of information security in digital libraries. Therefore, some researchers have moved beyond a focus on handling security risk technically to a stage where equal importance is accorded to technology and management. Information security in digital libraries has multiple dimensions, including infrastructure, digital content, users, standards and legal issues. In order to ensure information security assessment methods that are scientific and feasible, digital libraries should build an information security management system to cope with unexpected information security events via risk assessment, preventive mechanisms and active intervention, in compliance with the principle and thought of related information security standards (Anday et al., 2012; Thompson, 2013). In recognition of its security efforts, OCLC has met ISO 27001 security standards and has received registrations (ISO/IEC, 2013: 1–2). The OCLC's ISO 27001 information security management system is aligned with ISO 9001:2000 certified quality processes (OCLC, 2015). Both the international standard ISO 27000 and the Chinese standard GB/T 20984 for information security management provide certain methods for computing ultimate risk values by using a combination of factors including assets, threats and vulnerabilities. However, digital libraries are confronted with a great variety of assets, threats and vulnerabilities that are important to the operation of these libraries to varying degrees, and hence may have varying degrees of influence on information security for digital libraries. Therefore, the assessment of information security risks for digital libraries should delve into the methods used to identify and compute the relevant assets, threats and vulnerabilities. Considering that the objects of assessment have a diversity of attributes, this study introduces a fuzzy comprehensive assessment method to identify and compute such factors. The research findings can presumably not only optimize the methodology of the assessment of information security risks for digital libraries, but also offer a systematic guide to security risk control for digital libraries, thus improving information security management of digital libraries.

Literature review

The methodology for the assessment of information security risks refers to the means and methods of analysis used for the assessment of information security risks, and will affect each step of assessment as well as its final result. In comparison with the numerous studies on such themes as paper-based information security for traditional libraries (Ajegbomogun, 2004; Holt, 2007), information system security (Balas, 2005) and information security for digital libraries (Fox, 2006; Kuzma, 2010), the research on the methodology of assessment of information security risks for digital libraries remains in its incipience, and can be classified into three types.

The first type of researches relates to the security assessment model for library information systems. On the basis of the instrument of assessment for information security systems proposed by Hagen et al. (2008), Ismail and Zainab (2013) acquired a reliable assessment scale for the security status of library information systems by adopting the questionnaire survey method and using the information system personnel of 50 libraries as the object of the survey. The assessment scale contained five dimensions – technological security basis, information security policy, program and control, management tools and methods, and innovation consciousness. The research results showed that libraries continued to attach importance to technologies but ignored management; in particular, organizational control was deficient in security policies and user training. However, the research focused on security in library information systems; hence, the assessment scale cannot simply be applied to the assessment of information security risks for digital libraries. The assessment of information security risks for digital libraries involves a variety of factors, and an excessive number of survey questions may cause the respondents to lose patience. Therefore, it is infeasible to use the method to gather survey data for the assessment of information security risks for digital libraries.

The second type of research relates to the assessment of information security for digital libraries in accordance with the related norms and standards. This aspect has become the mainstream in the assessment of information security risks for digital libraries. The IT Baseline Protection Manual (ITBPM) is an information security protection norm prepared by experts under the leadership of the Federal Office for Information Security in Germany. The ITBPM provides a reference standard for implementing IT security management, analyzing threats to information assets, and supervising system security mechanisms (German Federal Office for Information Security, 2000: 1–2). Based on the ITPBM standard, Zeng (2012) built a model called "Asset-Threat-Security Measure" to assess and analyze information security risks for college libraries. Via systematic literature review, Anday et al. (2012) concluded that the ISO 27000 standard was the most suitable standard for the management of information security risks for digital libraries. The principles set forth in the ISO 27000 are independent

of specific assessment methods, because of which ISO 27000 does not expressly stipulate the assessment methods that should be applied in any given situation. Appendix E of ISO 27005 offers three assessment methods (the risk value matrix method, the threat grading method and the two-valued risk method) with examples (ISO/IEC, 2011: 52–54). The GB/T 20984 assigns five-grade values to assets, threats, vulnerabilities, and risk grades. Appendix A – Computation Methods for Risks – lists two risk assessment modes: the matrix method and the multiplicative method (AQSIQ (China National Standardization Management Committee), 2007: 18–21. See Appendix to this paper). Huang and Ren (2014) analyzed the applicability of the assessment methods (the risk value matrix method, the practical risk matrix method (an improvement over the risk value matrix method) and the multiplicative method) specified by ISO 27005 and GB/T 20984 to the assessment of information security risks for digital libraries. Han et al. (2016) conducted a case study on the assessment of information security risks for a public digital library in China by using the multiplicative method specified in GB/T 20984. The case study showed that the multiplicative method was more suitable for the assessment of information security risks for digital libraries in China. This type of research focuses on methods of computing risk values in the assessment of information security risks, and the direct value assignment method is used to compute the values of assessment factors. Risk assessment involves a great diversity of factors, and thus is an important issue in identifying and computing various factors.

The third type of research relates to the quantitative assessment of information security risks for traditional libraries or digital libraries based on a specific mathematical model or method. Zhu et al. (2009) used the grey analytic hierarchy process to determine the index system for risk assessment and weight values of different indices and compute the various risk values for digital libraries. Li (2011) used the fault tree analysis method to assess information security risks to libraries. The fault tree analysis method is commonly used in system security engineering and can help build an organic connection between the faults of a system and the faults of system components using symbols. Li et al. (2015) built a dynamic risk assessment model for digital library information systems and applied multi-agent technology to the dynamic risk assessment of the information security of digital libraries. This type of research focuses on the application of quantitative mathematical methods in the assessment of information security risks to digital libraries. Because no related standard is available for reference, such research possesses a certain innovativeness, but is deficient in normativeness and universality, and defective in operability.

The assessment of information security risks to digital libraries usually involves three factors: assets, threats and vulnerabilities. The identification and computation of such factors form an important part of the assessment model for information security risks, and the value assignment methods of such factors directly determine the objectivity and accuracy of the assessment results. Fuzzy comprehensive assessment was proposed by Zadeh (an expert in the US in automatic control) in 1965 (Shao, 2009). This method can give a reasonable overall assessment for a thing that possesses a diversity of attributes, or whose overall quality is affected by a diversity of factors. The factors involved in the assessment of information security risks to digital libraries include a diversity of attributes, and are affected by a diversity of factors (for example, the asset value of a digital library is jointly determined by confidentiality, integrity and availability, and may be affected by the business operation of the digital library). Relying on the ISO 27000 and GB/T 20984 standards, this paper applies fuzzy comprehensive assessment to the identification and computation of assets and threats involved in the assessment of information security risks to digital libraries, and assesses information security risks to a public library in China using the practical matrix method and the multiplicative method to compute various risk values with a view to verifying the feasibility of the fuzzy comprehensive assessment method. Finally, this study determines a suite of normative, objective, and operable methods to assess information security risks to digital libraries.

Methodology

Both the international standard ISO 27000 and the Chinese standard GB/T 20984 state concern regarding the four risk factors of assets, threats, vulnerabilities and existing control measures. In risk assessment, vulnerabilities and existing control measures cannot be separated from each other. In both the ISO 27000 and the GB/T 20984, existing control measures are thus not considered separately, but in conjunction with the identification and computation of vulnerabilities. Therefore, the risk factors for information security in digital libraries consist of assets, threats and vulnerabilities. The relationship between risk value (R) and risk factors can be formularized as $R = R(A,T,V)$, where A stands for asset value, T represents threat severity and V stands for degree of vulnerability.

Identification and computation model for asset value

Assets refer to the things or resources that are in the possession of or under the control of a digital library, and can yield social and economic benefits for the digital library (i.e. they are valuable to the digital library). Asset value is

jointly determined by three attributes: confidentiality, integrity and availability. Meanwhile, the importance of confidentiality, integrity and availability to asset value varies from asset to asset. Asset value is jointly determined by the values of the three attributes and the degree of the importance of each to assets. Based on the principle of multi-factor fuzzy comprehensive assessment, the construction of the computation model for asset value can be described as follows:

1. Create a factor set (U): $U = \{u_1, u_2, u_3\}$, where, u_1 stands for the confidentiality of assets, u_2 stands for the integrity of assets, and u_3 stands for the availability of assets.
2. Create an assessment set (V). Five grades of values are assigned to confidentiality, integrity, and availability—$V = \{1, 2, 3, 4, 5\}$—where 1 to 5 represent, respectively, the five assessment grades (very low, low, medium, high, very high). For details of the value assignment standard, refer to Han et al. (2016).
3. Compute the single-factor assessment matrix (R_i). The mapping matrices of the three attributes in the assessment set V can be obtained according to the survey results of value assignments to the three attributes,

$$R_i = \{r_{i1}, r_{i2}, r_{i3}, r_{i4}, r_{i5}\},\ \sum_{j=1}^{5} r_{ij} = 1 \cap r_{ij} \geqslant 0 \ (\text{i} = 1, 2, 3) \quad (1)$$

r_{ij} (i = 1, 2, 3; j = 1, 2, 3, 4, 5) stands for the degree of belongingness of u_i to v_j. r_{ij} can be calculated according to the proportion of each asset value factor in each asset value index. Values are assigned to r_{ij} as follows: (1) the number of questionnaires on value assignment for confidentiality, integrity and the availability of an asset is e; (2) there are k types of survey objects (for example, management, technology, service, and so on), and the weights of value assignment to the survey objects differ from one another; (3) the weight of the ath type of survey objects (a = 1, 2, …, k) is w_a, and $\sum_{a=1}^{k} w_a = 1$; then, $r_{ij} = \dfrac{\sum_{t=1}^{e} N \times W}{\sum_{t=1}^{e} W}$.

If v_j is assigned to factor u_i of the tth survey object, N is 1; otherwise, N is 0. If the tth survey object belongs to the ath type, $W = w_a$.

4. Create a comprehensive assessment matrix (R). By combining the three single-factor assessment matrices, the comprehensive assessment matrix from the factor set to the assessment set is attained, that is, $R = \left(r_{ij}\right)_{3\times 5}$.
5. Create a weight set (W). Weight set (W) is the set of degrees of importance of the three attributes to asset value, that is, $W = \{w_1, w_2, w_3\}$, and $w_1 + w_2 + w_3 = 1$, where, w_1, w_2, w_3, respectively, stand for the degrees of importance of confidentiality, integrity, and availability to asset value. In this study, the weight values were obtained by using the expert investigation method. This survey was oriented toward librarians, management personnel and technical personnel of 30 digital libraries of China. The computation process was as follows: (1) compute the average degree of importance of each respondent to the confidentiality, integrity, and availability of each asset; (2) determine the value of the weight set by normalizing the average values.
6. Results of multi-factor comprehensive assessment (asset value A). The fuzzy comprehensive assessment set B can be determined by multiplying the weight set (W) by the comprehensive assessment matrix (R), that is, $B = W \times R$. To comprehensively consider the degree of belongingness of each element in the assessment set, the result of multi-factor comprehensive assessment can be obtained by using the weighted average method; that is, asset value A can be formularized as follows:

$$A = \text{int}(B \times V^T) = \text{int}(W \times R \times V^T) \quad (2)$$

Identification and computation model for threat severity

Threats refer to the potential causes of unanticipated events that may damage digital libraries. The severity of threats is jointly determined by the possibility of threats and the damage they cause to assets. The degree of damage to assets can be further classified into damage to confidentiality, integrity and availability of assets. Therefore, threats (T) can be formularized as $T = T(T_M, T_A) = \text{T}(T_M, L(T_I, T_C, T_U, W))$, where, T_M represents the occurrence frequency of threats, T_A is the degree of damage to assets caused by threats, T_I, T_C, and T_C represent the degree of damage caused by the threat to the confidentiality, the integrity and the availability of assets, respectively, W stands for the degree of importance of confidentiality, integrity and availability to asset value, and $\sum W_i = 1$.

1. Computing the possibility of threats (T_M)

(i) Create an assessment set (V). Five grades of values are assigned to T_M, that is, $V = \{1, 2, 3, 4, 5\}$. For details concerning the meaning of the different grades, refer to Table 1.

(ii) Compute the single-factor assessment matrix (R). The mapping matrix of T_M in the assessment set (V) can

Table 1. Meanings of the grades of possibility of threats.

Grade	Value	Meaning
Very high	5	The frequency of occurrence is very high (at least once a week), threats are almost inevitable in most cases, or it is proved that threats occur frequently.
High	4	The frequency of occurrence is high (at least once a month), threats are very likely to occur in most cases, or it is proved that threats occur repeatedly.
Medium	3	The frequency of occurrence is medium (more than once every six months), threats are likely to occur in certain cases, or it is proved that threats have occurred.
Low	2	The frequency of occurrence is low, threats are unlikely to occur in normal cases, or it is not proved that threats have occurred.
Very low	1	Threats are almost impossible, or threats are likely to occur only in very rare cases, or in exceptional cases.

be calculated according to the specific survey results of the attributes of the threats to digital libraries, that is, $R = \{r_1, r_2, r_3, r_4, r_5\}$, and $\sum_{j=1}^{5} r_j = 1 \cap r_j \geqslant 0$, where, r_j (j = 1, 2, 3, 4, 5) stands for the degree of belongingness of T_M to v_j . For details regarding its values, refer to the computation method for r_{ij} in Section 3.1.

(iii) Result of single-factor assessment (T_M). The possibility of threats can be formularized as $T_M = R \times V^T$.

2. Computing the degree of damage to assets caused by threats (T_A)

(i) Create a factor set (U). $U = \{u_1, u_2, u_3\}$ u_1 stands for the impact of threats on confidentiality, u_2 stands for the effects of threats on integrity, and u_3 represents the impact of threats on availability.

(ii) Create an assessment set (V). Five grades of values are assigned to the impact of threats on confidentiality, integrity, and availability. Therefore, $V = \{1, 2, 3, 4, 5\}$, where, 1 to 5, respectively, stand for the five assessment grades (very low, low, medium, high, very high). For details concerning the meanings of the different grades, refer to Han et al. (2016).

(iii) Compute the single-factor assessment matrix (R_i). The mapping matrices of the impact of threats on the three attributes in the assessment set (V) can be obtained according to the specific survey results of the values assigned to the threats to digital libraries, that is,

$$R_i = \{r_{i1}, r_{i2}, r_{i3}, r_{i4}, r_{i5}\}, \sum_{j=1}^{5} r_{ij} = 1 \cap r_{ij} \geqslant 0 \text{ (I = 1, 2, 3)} \quad (3)$$

For details regarding the value of r_{ij} , refer to the computation method for r_{ij} in the section 'Identification and computation model for asset value'.

3. Creating a comprehensive assessment matrix (R)

By combining the three single-factor assessment matrices, the comprehensive assessment matrix from the factor set to the assessment set is attained, that is, $R_i = \left(r_{ij}\right)_{3\times5}$.

4. Creating a weight set (W). The weight set (W) reflects the degree of importance of confidentiality, integrity, and availability to assets. For details concerning the value assignment method, refer to the weight set in the section 'Identification and computation model for asset value'.
5. Result of multi-factor comprehensive assessment (T_A : degree of damage to assets caused by threats) To comprehensively consider the degree of belongingness of each element to the assessment set, the aforementioned weight set (W) is multiplied by the comprehensive assessment matrix (R), and the multi-factor comprehensive assessment result of the assessment object can be obtained by using the weighted average method. That is, T_A (the degree of damage to assets caused by assets) can be formularized as $\mathrm{T}_A = \mathrm{L}(T_i, T_c, T_a, w) = W \times R \times V^T$.
6. Computing the severity of threats

The possibility of threats and the degree of damage to assets caused by threats can be calculated as described above. Then, the severity of threats to each asset can be determined by integrating two types of factors via the geometrical average method, that is,

$$T = T(T_M, T_A) = \mathrm{int}(\sqrt{T_M \times T_A} \quad (4)$$

where, T_M stands for the frequency of occurrence of threats, and T_A stands for the degree of damage to assets caused by assets.

Identification and computation model for degree of vulnerability

Vulnerabilities refer to the weaknesses of assets or asset groups in a digital library that can be exploited by threats. Vulnerabilities may arise out of deficiencies in organizational structure, personnel, management, procedures and assets. The identification process of vulnerabilities needs to incorporate prevalent control measures. The influential factors in vulnerabilities are extremely complex, and difficult to capture and compute. In order to identify vulnerabilities

objectively and accurately and reduce computation errors, this paper combines quantitative assessment and qualitative assessment by using three methods: vulnerability scanning, questionnaire survey and on-site survey. Therefore, the influential factors for vulnerabilities (V) can be formularized as $V = V(V_I, V_Q, V_T)$, where, V_I and V, respectively, stand for the vulnerability values that the assessors directly assign via on-site survey and vulnerability scanning, and V_Q stands for the vulnerability value determined via a questionnaire survey.

Following the five-grade conversion, the results are represented by V_I, V_Q, V_T. Then,

$$V = \text{int} \sum_{i_in_(I,Q,T)} w_i V_i \text{ and } \sum_{i_in_(I,Q,T)} w_i = 1 \quad (5)$$

where, V_i and V_T are directly determined by the assessors via an on-site survey and vulnerability scanning, respectively, V_Q is determined via statistical analysis for all questionnaire data, and w represents the weight of the vulnerability assessment mode.

Case study

To verify the feasibility of the proposed methods and models, this study chose Dongguan Library (located in Dongguan City, Guangdong Province, China) as the object of empirical study. Dongguan Library is a digital library-based modern urban library that embodies the philosophy of knowledge interaction and incorporates traditional library functions into its operation. In light of the development goal of Dongguan City, the library is intended to become an urban center library that not only integrates traditional literature resources and modern network resources, but also integrates information resources and human talent resources. The case study aimed to determine the types and values of assets, threats, and vulnerabilities to the digital library by using the processes and models specified in the Methodology section. Finally, the risk value of the digital library was determined by using the multiplicative method specified in GB/T 20984.

Nine staff members from different departments of the library were selected to participate in the survey. The surveyors found that the degree of familiarity and access to the library assets somewhat differed among staff members. By their job categories, the nine staff members were classified into three types (management personnel, technical personnel and service personnel). The weight assigned to management personnel was 0.45, that to technical personnel was 0.35, and the weight assigned to service personnel was 0.2. While assets are typically correlated to threats, the respondents were asked to assign values to the possibility of threats to each asset and the degree of damage of threats to the three security attributes of each asset. Five grades of value were assigned to the four attributes. The vulnerability value package comprised the questionnaire survey, the on-site survey and vulnerability scanning. For the questionnaire survey, different questionnaires were designed for management personnel, technical personnel and ordinary librarians. The on-site survey focused on 11 control domains specified in ISO 27002. The related departments were interviewed to survey specific items, and the environment, implementation status, data documentation and operation habits were observed, inspected and queried. The Remote Security Assessment System (RSAS) developed by NSFOCUS was used for vulnerability scanning, and the test objects consisted of various mainstream operating systems (for example, Windows, Unix and Linux), application services (for example, FTP, Telnet and SMTP), and network devices. The assessors analyzed the results of the vulnerability test and converted them into five grades of values.

Following data collection, the assessors obtained 3111 items correlated to assets, threats and vulnerabilities. These were risky items encountered by the library. According to the values of assets, threats and vulnerabilities, the assessors computed the values of the 3111 risky items using the direct value assignment method together with the practical matrix method and the multiplicative method. For details regarding the results of computation, refer to Table 2. The risks were classified into five grades. Risk Grade 1 means that the risk was very low and the library services were almost completely unaffected. Risk Grade 2 means that risk was low and acceptable, and the library services were only slightly affected. Risk Grade 3 means that the risk was medium, library services were affected by the average value and measures were temporarily not required. Risk Grade 4 means that risk was high, library services were severely affected and certain measures needed to be taken to reduce risk. Risk Grade 5 means that risk was very high, the library services were severely affected and measures needed to be taken in a timely manner.

Conclusion and discussion

The methods for the identification and computation of influential factors regarding assets, threats and vulnerabilities directly determine the computational results of risk values. In accordance with ISO 27002 and GB/T 20984, this paper subdivided factors influencing assets, threats and vulnerabilities, and proposed an asset and threat computation model based on the fuzzy comprehensive assessment matrix, and a vulnerability computation model based on the multi-channel weighted average method. The following findings were made:

1. The assessment results based on the fuzzy assessment method were more consistent with the status quo for information security risks encountered by digital libraries.

Table 2. Grades of risk to digital library.

Computation method		Risk grade					Medium risk (or above)	High risk (or above)
		1	2	3	4	5		
Direct value assignment	Practical matrix	6	309	1248	1407	141	89.87%	49.76%
	Multiplicative	119	2038	950	4	0	30.57%	0.13%
Methods specified herein	Practical matrix	84	852	1599	545	30	69.9%	18.49%
	Multiplicative	874	1806	403	28	0	13.90%	0.9%

If both the cost of risk control and the possible impact of risks are taken into account, a digital library should ensure that more risk values are within an acceptable range. Normally, certain control measures should be taken to deal with medium-risk (or higher-risk) items. After discussions with some personnel who deal with digital libraries, the assessors found it impractical to take control measures for more than half the total risky items from the perspectives of cost and workload. They found that risky items under control measures should be controllable, and the control results should be operable. If values are directly assigned to assets, threats and vulnerabilities, the proportion of medium-risk (or higher-risk) items in the final assessment results increases. In particular, in the assessment results based on the practical matrix method, as many as 1578 risky items should have been subjected to control measures by the related departments of the digital library. In this risk assessment, regardless of whether the practical matrix method or multiplicative method was used to compute the risk values of the digital library, the proportions of medium-level (or higher-risk) items and high-risk (or higher) items in the assessment results were more consistent with the status of the digital library. Compared with the operation status of the digital library, the methods specified here combined with the multiplicative method were superior to those combined with the practical matrix method. The methods specified here enable a digital library to focus on medium-risk items and high-risk items, and are more feasible from the perspective of risk control.

2. Theoretically, the factor identification and computation methods are more comprehensive and objective.

Theoretically, the asset and threat computation method proposed here, based on the fuzzy comprehensive assessment matrix and the vulnerability computation method, which is in turn based on the multi-channel weighted average method, showed its objectivity and scientificity in the following two aspects: (1) The methods take into account both the general features of digital libraries and the specific features of the assessed digital library. The weight set (W) for assets and threats was determined by surveying experts from 30 digital libraries, and possessed a certain degree of generality. The scores of each factor were determined by staff members of the digital library that was assessed, and embodies the particularity of the digital library; (2) The methods can be used in conjunction with the risk computation methods specified in ISO 27002 and GB/T 20984, and increase the proportion of quantitative analysis in the entire risk assessment process while complying with related information security standards. Therefore, the methods strike a balance between quantitative analysis and qualitative analysis.

Based on the assessment results, an outstanding issue is to screen risk control measures for the digital library. This research was oriented toward a typical public library in China, and the assessment results showed that the proposed methods are significantly superior to the direct value assignment method. However, the reliability of assessment results remains to be further verified if the methods proposed here are used to assess information security risks to other digital libraries.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The authors acknowledge financial support for this study by the national social science fund project of China, project number 12ATQ001.

References

Adam NR, Atluri V, Bertino E, et al. (2002) A content-based authorization model for digital libraries. *IEEE Transactions on Knowledge and Data Engineering* 4(2): 296–315.

Ajegbomogun F (2004) Users' assessment of library security: A Nigerian university case study. *Library Management* 25(8/9): 386–390.

Anday A, Francese E, Huurdeman HC, et al. (2012) Information security issues in a digital library environment: A literature review. *BİLGİ DÜNY* 13(1): 117–137.

AQSIQ (2007) GB/T 20984 *Information Security Technology-Risk Assessment Specification for Information Security*. China: Administration of Quality Supervision, Inspection and Quarantine. (In Chinese).

Balas JL (2005) Close the gates, lock the windows, bolt the doors: Securing library computers. *Computers in Libraries* 25(3): 28–30.

Fox E and ElSherbiny N (2011) Security and digital libraries. In: Huang KH (ed.) *Digital Libraries-Methods and Application*. Rijeka, Croatia: InTech, pp: 151–160.

Fox R (2006) Vandals at the gates. *OCLC Systems & Services* 22(4): 249–255.

Frias-Martinez E, Magoulas G, Chen S, et al. (2006) Automated user modeling for personalized digital libraries. *International Journal of Information Management* 26(3): 234–248.

German Federal Office for Information Security (2000) *IT Baseline Protection Manual: 2000. Standard Security Measures*. Available at: http://www.iwar.org.uk/comsec/resources/standards/germany/itbpm.pdf (accessed 1 September 2016).

Hagen JM, Albrechtsen E and Hovden J (2008) Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security* 16(4): 377–397.

Han Z, Huang S, Li H and Ren N (2016) Assessing the status of digital library information security risk: A case study. *The Electronic Library* 34(3): 471–487.

Holt E (2007) Theft by library staff. *Bottom Line: Managing Library Finances* 20(2): 85–92.

Huang S (2011) *Information Security Management of Digital Library*. Nanjing, China: Nanjing University Press.

Huang S and Ren N (2014) Study on risk assessment method and model of digital libraries' information security. *Library and Information Service* 58(2): 14–20.

Ismail R and Zainab A (2013) Assessing the status of library information systems security. *Journal of Librarianship and Information Science* 45(3): 232–247.

ISO/IEC (2011) ISO/IEC 27005:2011 *Information Technology-Security Techniques-Information Security Risk Management*. International Organization for Standardization. Available at: http://www.iso27001security.com/html/27005.html (accessed 1 September 2016).

ISO/IEC (2013) ISO/IEC 27001:2013 *Information Technology-Security Techniques-Information Security Management Systems-Requirements*. International Organization for Standardization. Available at: http://www.iso.org/iso/catalogue_detail?csnumber=54534 (accessed 1 September 2016).

Kuzma J (2010) European digital libraries: Web security vulnerabilities. *Library Hi Tech* 28(3): 402–413.

Li C, Zhang W and Lan Y (2015) Dynamic risk assessment model of information system security in digital library. *Information Science* 33(5): 76–80

Li W (2011) *Study in information security risk assessment of library based on fault tree*. Master's Thesis, Tianjin University of Finance and Economics, China.

OCLC (2015) *Security White Paper: OCLC's Commitment to Secure Library Services*. Available at: http://www.oclc.org/content/dam/oclc/policies/security/oclcinformationsecuritywhitepaper.pdf (accessed 12 July 2015).

Saeednia S (2000) How to maintain both privacy and authentication in digital libraries. *International Journal of Digital Libraries* 2(4): 251–258.

Shao C (2009) The implication of fuzzy comprehensive evaluation method in evaluating internal financial control of enterprise. *International Business Research* 2(1): 210–214.

Thompson STC (2013) Helping the hacker? Library information, security, and social engineering. *Information Technology and Libraries* 25(4): 222–225.

Zeng S (2012) *A research in information security risk assessment of library based on ITBPM*. Master's Thesis, Shanxi Normal University, China.

Zhu L, Wang M and Bu S (2009) Research on the application of grey analytical hierarchy process in academic libraries' information security assessment system. *Library Work in Colleges and Universities* 29(2): 48–50.

Author biographies

Shuiqing Huang is a professor at the Research Center for Correlation of Domain Knowledge, College of Information Science and Technology, Nanjing Agricultural University, Nanjing, China. His current research interest includes information security of digital library and information retrieval.

Ni Ren is a doctoral student at the Research Center for Correlation of Domain Knowledge, College of Information Science and Technology, Nanjing Agricultural University. She is also a librarian of the Institute of Agricultural Economics and Information, Jiangsu Academy of Agricultural Sciences, Nanjing, China. Her current research interest includes information security of digital library and informetrics.

Zhengbiao Han is an associate professor at the Research Center for Correlation of Domain Knowledge, College of Information Science and Technology, Nanjing Agricultural University, Nanjing, China. His current research interest includes information security of digital library and information user behavior.

Bo Yang is an associate professor at the Research Center for Correlation of Domain Knowledge, College of Information Science and Technology, Nanjing Agricultural University, Nanjing, China. His current research interest includes information security of digital library and informetrics.

Appendix: Standards discussed in study

GB/T 20984 (AQSIQ, 2007:18–21)

附 录 A

（资料性附录）

风险的计算方法

对风险进行计算，需要确定影响风险要素、要素之间的组合方式以及具体的计算方法，将风险要素按照组合方式使用具体的计算方法进行计算，得到风险值。

目前通用的风险评估中风险值计算涉及的风险要素一般为资产、威胁、脆弱性（其关系如图 1 所示）；这些要素的组合方式如 5.6.1 的风险计算原理中指出，由威胁和脆弱性确定安全事件发生的可能性，由资产和脆弱性确定安全事件的损失，以及由安全事件发生的可能性和安全事件的损失确定风险值。目前，常用的计算方法是矩阵法和相乘法。

本附录首先说明矩阵法和相乘法的原理，然后基于 5.6.1 的风险计算原理中指出的风险要素和要素组合方式，以示例的形式说明采用矩阵法和相乘法计算风险值的过程。

在实际应用中，可以将矩阵法和相乘法结合使用。

A.1 使用矩阵法计算风险

A.1.1 矩阵法原理

矩阵法主要适用于由两个要素值确定一个要素值的情形。首先需要确定二维计算矩阵，矩阵内各个要素的值根据具体情况和函数递增情况采用数学方法确定，然后将两个元素的值在矩阵中进行比对，行列交叉处即为所确定的计算结果。

即 $z=f(x,y)$，函数 f 可以采用矩阵法。

矩阵法的原理是：

$x=\{x_1,x_2,\cdots,x_i,\cdots,x_m\}$，$1\leqslant i\leqslant m$，$x_i$ 为正整数

$y=\{y_1,y_2,\cdots,y_j,\cdots,y_n\}$，$1\leqslant j\leqslant n$，$y_j$ 为正整数

以要素 x 和要素 y 的取值构建一个二维矩阵，如表 A.1 所示。矩阵行值为要素 y 的所有取值，矩阵列值为要素 x 的所有取值。矩阵内 $m\times n$ 个值即为要素 z 的取值，$z=\{z_{11},z_{12},\cdots,z_{ij},\cdots,z_{mn}\}$，$1\leqslant i\leqslant m$，$1\leqslant j\leqslant n$，$z_{ij}$ 为正整数。

表 A.1 矩阵构造

	y	y_1	y_2	…	y_j	…	y_n
x	x_1	z_{11}	z_{12}	…	z_{1j}	…	z_{1n}
	x_2	z_{21}	z_{22}	…	z_{2j}	…	z_{2n}
	…	…	…	…	…	…	…
	x_i	z_{i1}	z_{i2}	…	z_{ij}	…	z_{in}
	…	…	…	…	…	…	…
	x_m	z_{m1}	z_{m2}	…	z_{mj}	…	z_{mn}

对于 z_{ij} 的计算，可以采取以下计算公式：

$z_{ij}=x_i+y_j$，

或 $z_{ij}=x_i\times y_j$，

或 $z_{ij}=\alpha\times x_i+\beta\times y_j$，其中 α 和 β 为正常数。

z_{ij} 的计算需要根据实际情况确定，矩阵内 z_{ij} 值的计算不一定遵循统一的计算公式，但必须具有统一的增减趋势，即如果 f 是递增函数，z_{ij} 值应随着 x_i 与 y_j 的值递增，反之亦然。

矩阵法的特点在于通过构造两两要素计算矩阵，可以清晰罗列要素的变化趋势，具备良好灵活性。

在风险值计算中，通常需要对两个要素确定的另一个要素值进行计算，例如由威胁和脆弱性确定安全事件发生可能性值、由资产和脆弱性确定安全事件的损失值等，同时需要整体掌握风险值的确定，因此矩阵法在风险分析中得到广泛采用。

A.1.2 计算示例

以下基于5.6.1的风险计算原理，具体说明使用矩阵法计算风险的过程。

A.1.2.1 条件

共有三个重要资产，资产A1、资产A2和资产A3；

资产A1面临两个主要威胁，威胁T1和威胁T2；

资产A2面临一个主要威胁，威胁T3；

资产A3面临两个主要威胁，威胁T4和T5；

威胁T1可以利用的资产A1存在的两个脆弱性，脆弱性V1和脆弱性V2；

威胁T2可以利用的资产A1存在的三个脆弱性，脆弱性V3、脆弱性V4和脆弱性V5；

威胁T3可以利用的资产A2存在的两个脆弱性，脆弱性V6和脆弱性V7；

威胁T4可以利用的资产A3存在的一个脆弱性，脆弱性V8；

威胁T5可以利用的资产A3存在的一个脆弱性，脆弱性V9。

资产价值分别是：资产A1=2，资产A2=3，资产A3=5；

威胁发生频率分别是：威胁T1=2，威胁T2=1，威胁T3=2，威胁T4=5，威胁T5=4；

脆弱性严重程度分别是：脆弱性V1=2，脆弱性V2=3，脆弱性V3=1，脆弱性V4=4，脆弱性V5=2，脆弱性V6=4，脆弱性V7=2，脆弱性V8=3，脆弱性V9=5。

A.1.2.2 计算重要资产的风险值

三个资产的风险值计算过程类似，下面以资产A1为例使用矩阵法计算风险值。

资产A1面临的主要威胁包括威胁T1和威胁T2，威胁T1可以利用的资产A1存在的脆弱性包括两个，威胁T2可以利用的资产A1存在的脆弱性包括三个，则资产A1存在的风险值包括五个。五个风险值的计算过程类似，下面以资产A1面临的威胁T1可以利用的脆弱性V1为例，计算安全风险值。

a) 计算安全事件发生可能性

威胁发生频率：威胁T1=2；

脆弱性严重程度：脆弱性V1=2。

首先构建安全事件发生可能性矩阵，如表A.2所示。

表A.2 安全事件可能性矩阵

	脆弱性严重程度	1	2	3	4	5
威胁发生频率	1	2	4	7	11	14
	2	3	6	10	13	17
	3	5	9	12	16	20
	4	7	11	14	18	22
	5	8	12	17	20	25

然后根据威胁发生频率值和脆弱性严重程度值在矩阵中进行对照，确定安全事件发生可能性值等于6。

由于安全事件发生可能性将参与风险事件值的计算，为了构建风险矩阵，对上述计算得到的安全风险事件发生可能性进行等级划分，如表A.3所示，安全事件发生可能性等级等于2。

表 A.3 安全事件可能性等级划分

安全事件发生可能性值	1~5	6~11	12~16	17~21	22~25
发生可能性等级	1	2	3	4	5

b) 计算安全事件的损失

资产价值:资产 A1=2;

脆弱性严重程度:脆弱性 V1=2。

首先构建安全事件损失矩阵,如表 A.4 所示。

表 A.4 安全事件损失矩阵

	脆弱性严重程度	1	2	3	4	5
资产价值	1	2	4	6	10	13
	2	3	5	9	12	16
	3	4	7	11	15	20
	4	5	8	14	19	22
	5	6	10	16	21	25

然后根据资产价值和脆弱性严重程度值在矩阵中进行对照,确定安全事件损失值等于 5。

由于安全事件损失将参与风险事件值的计算,为了构建风险矩阵,对上述计算得到的安全事件损失进行等级划分,如表 A.5 所示,安全事件损失等级等于 1。

表 A.5 安全事件损失等级划分

安全事件损失值	1~5	6~10	11~15	16~20	21~25
安全事件损失等级	1	2	3	4	5

c) 计算风险值

安全事件发生可能性=2;安全事件损失等级=1,

首先构建风险矩阵,如表 A.6 所示。

表 A.6 风险矩阵

	可能性	1	2	3	4	5
损失等级	1	3	6	9	12	16
	2	5	8	11	15	18
	3	6	9	13	17	21
	4	7	11	16	20	23
	5	9	14	20	23	25

然后根据安全事件发生可能性和安全事件损失等级在矩阵中进行对照,确定安全事件风险等于 6。

按照上述方法进行计算,得到资产 A1 的其他的风险值,以及资产 A2 和资产 A3 的风险。然后再进行风险结果等级判定。

A.1.2.3 结果判定

确定风险等级划分 如表 A.7 所示。

表 A.7 风险等级划分

风险值	1~6	7~12	13~18	19~23	24~25
风险等级	1	2	3	4	5

根据上述计算方法,以此类推,得到三个重要资产的风险值,并根据风险等级划分表,确定风险等

级，结果如表 A.8 所示。

表 A.8 风险结果

资产	威胁	脆弱性	风险值	风险等级
资产 A1	威胁 T1	脆弱性 V1	6	1
	威胁 T1	脆弱性 V2	8	2
	威胁 T2	脆弱性 V3	3	1
	威胁 T2	脆弱性 V4	9	2
	威胁 T2	脆弱性 V5	3	1
资产 A2	威胁 T3	脆弱性 V6	11	2
	威胁 T3	脆弱性 V7	8	2
资产 A3	威胁 T4	脆弱性 V8	20	4
	威胁 T5	脆弱性 V9	25	5

重要资产的风险等级柱状图如图 A.1 所示。

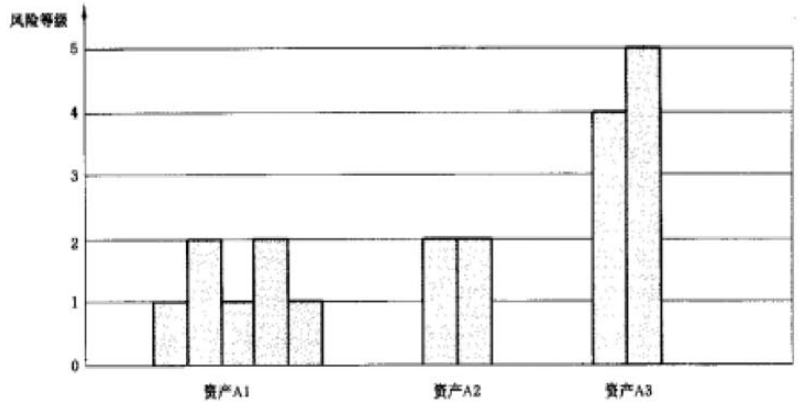


图 A.1 风险等级柱状图

A.2 使用相乘法计算风险

A.2.1 相乘法原理

相乘法主要用于两个或多个要素值确定一个要素值的情形。即 $z=f(x,y)$，函数 f 可以采用相乘法。

相乘法的原理是：

$z=f(x,y)=x\otimes y$。

当 f 为增量函数时，$\otimes$ 可以为直接相乘，也可以为相乘后取模等，例如：

$z=f(x,y)=x\times y$，

或 $z=f(x,y)=\sqrt{x\times y}$，

或 $z=f(x,y)=\lfloor\sqrt{x\times y}\rfloor$，

或 $z=f(x,y)=\left[\frac{\sqrt{x\times y}}{x+y}\right]$ 等。

相乘法提供一种定量的计算方法，直接使用两个要素值进行相乘得到另一个要素的值。相乘法的特点是简单明确，直接按照统一公式计算，即可得到所需结果。

ISO/IEC 27005:2011(E)

E.2.1 Example 1 Matrix with predefined values

In risk assessment methods of this type, actual or proposed physical assets are valued in terms of replacement or reconstruction costs (i.e. quantitative measurements). These costs are then converted onto the same qualitative scale as that used for information (see below). Actual or proposed software assets are valued in the same way as physical assets, with purchase or reconstruction costs identified and then converted to the same qualitative scale as that used for information. Additionally, if any application software is found to have its own intrinsic requirements for confidentiality or integrity (for example if source code is itself commercially sensitive), it is valued in the same way as for information.

The values for information are obtained by interviewing selected business management (the "data owners") who can speak authoritatively about the data, to determine the value and sensitivity of the data actually in use, or to be stored, processed or accessed. The interviews facilitate assessment of the value and sensitivity of the information in terms of the worst case scenarios that could be reasonably expected to happen from adverse business consequences due to unauthorized disclosure, unauthorized modification, non-availability for varying time periods, and destruction.

The valuation is accomplished using information valuation guidelines, which cover such issues as:

- Personal safety
- Personal information and privacy
- Legal and regulatory obligations
- Law enforcement
- Commercial and economic interests
- Financial loss/disruption of activities
- Public order
- Business policy and operations
- Loss of goodwill
- Contract or agreement with a customer

The guidelines facilitate identification of the values on a numeric scale, such as the 0 to 4 scale shown in the example matrix below, thus enabling the recognition of quantitative values where possible and logical, and qualitative values where quantitative values are not possible, e.g. for endangerment of human life.

The next major activity is the completion of pairs of questionnaires for each threat type, for each grouping of assets that a threat type relates to, to enable the assessment of the levels of threats (likelihood of occurrence) and levels of vulnerabilities (ease of exploitation by the threats to cause adverse consequences). Each question answer attracts a score. These scores are accumulated through a knowledge base and compared with ranges. This identifies threat levels on say a high to low scale and vulnerability levels similarly, as shown in the example matrix below, differentiating between the types of consequences as relevant. Information to complete the questionnaires should be gathered from interviews with appropriate technical, personnel and accommodation people, and physical location inspections, and reviews of documentation.

The asset values, and the threat and vulnerability levels, relevant to each type of consequence, are matched in a matrix such as that shown below, to identify for each combination the relevant measure of risk on a scale of 0 to 8. The values are placed in the matrix in a structured manner. An example is given below:

www.kubok.net

© ISO/IEC 2011 – All rights reserved

Table E.1 a)

	Likelihood of occurrence – Threat	Low			Medium			High		
	Ease of Exploitation	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

For each asset, the relevant vulnerabilities and their corresponding threats are considered. If there is a vulnerability without a corresponding threat, or a threat without corresponding vulnerability, there is presently no risk (but care should be taken in case this situation changes). Now the appropriate row in the matrix is identified by the asset value, and the appropriate column is identified by the likelihood of the threat occurring and the ease of exploitation. For example, if the asset has the value **3**, the threat is "**high**" and the vulnerability "**low**", the measure of risk is **5**. Assume an asset has a value of 2, e.g. for modification, the threat level is "low" and the ease of exploitation is "high", then the measure of risk is 4. The size of the matrix, in terms of the number of threat likelihood categories, ease of exploitation categories and the number of asset valuation categories, can be adjusted to the needs of the organization. Additional columns and rows will necessitate additional risk measures. The value of this approach is in ranking the risks to be addressed.

A similar Matrix as shown in Table E.1 b) results from the consideration of the likelihood of an incident scenario, mapped against the estimated business impact. The likelihood of an incident scenario is given by a threat exploiting a vulnerability with a certain likelihood. The Table maps this likelihood against the business impact related to the incident scenario. The resulting risk is measured on a scale of 0 to 8 that can be evaluated against risk acceptance criteria. This risk scale could also be mapped to a simple overall risk rating, for example as:

- Low risk: 0-2
- Medium Risk: 3-5
- High Risk:6-8

Table E.1 b)

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

© ISO/IEC 2011 – All rights reserved

E.2.2 Example 2 Ranking of Threats by Measures of Risk

A matrix or table such as that shown in Table E.2 can be used to relate the factors of consequences (asset value) and likelihood of threat occurrence (taking account of vulnerability aspects). The first step is to evaluate the consequences (asset value) on a predefined scale, e.g. 1 through 5, of each threatened asset (column "b" in the table). The second step is to evaluate the likelihood of threat occurrence on a predefined scale, e.g. 1 through 5, of each threat (column "c" in the table). The third step is to calculate the measure of risk by multiplying (b × c). Finally the threats can be ranked in order of their associated measure of risk. Note that in this example, 1 is taken as the lowest consequence and the lowest likelihood of occurrence.

Table E.2

Threat descriptor (a)	Consequence (asset) value (b)	Likelihood of threat occurrence (c)	Measure of risk (d)	Threat ranking (e)
Threat A	5	2	10	2
Threat B	2	4	8	3
Threat C	3	5	15	1
Threat D	1	3	3	5
Threat E	4	1	4	4
Threat F	2	4	8	3

www.klubok.net

As shown above, this is a procedure which permits different threats with differing consequences and likelihood of occurrence to be compared and ranked in order of priority, as shown here. In some instances it will be necessary to associate monetary values with the empirical scales used here.

E.2.3 Example 3 Assessing a value for the likelihood and the possible consequences of risks

In this example, the emphasis is placed on the consequences of information security incidents (i.e. incident scenarios) and on determining which systems should be given priority. This is done by assessing two values for each asset and risk, which in combination will determine the score for each asset. When all the asset scores for the system are summed, a measure of risk to that system is determined.

First, a value is assigned to each asset. This value relates to the potential adverse consequences that can arise if the asset is threatened. For each applicable threat to the asset, this asset value is assigned to the asset.

Next a likelihood value is assessed. This is assessed from a combination of the likelihood of the threat occurring and the ease of exploitation of the vulnerability, see Table E.3 expressing the likelihood of an incident scenario.

Table E.3

Likelihood of Threat	Low			Medium			High		
Levels of Vulnerability	L	M	H	L	M	H	L	M	H
Likelihood Value of an incident scenario	0	1	2	1	2	3	2	3	4

© ISO/IEC 2011 – All rights reserved

数字图书馆信息资产调查表

尊敬的先生/女士：

您好！这是国家社科基金”数字图书馆信息安全管理与评价”课题组的调查问卷。您的回答将为我们的研究提供非常有用的信息，希望能够得到您的大力支持。您提供的信息将仅用于本项目的研究用，我们承诺不会对外泄露您与贵馆的任何信息。我们在研究中引用与贵馆有关的数据时，不会出现贵馆的名称。非常感谢您的配合！如果填写过程中有任何问题请通过邮件与我们联系。

“数字图书馆信息安全管理与评价”课题组

zbh1985@njau.edu.cn

填写说明

1. 本问卷包括资产识别和资产赋值两部分内容。通过对数字图书馆的信息资产进行调研，列出与信息安全有关的资产清单，然后对每一项资产进行确认和适当的评估。在列出所有信息资产后，从保密性、完整性和可用性这三个方面对信息资产进行赋值，并采用定性的方式来建立资产的价值或重要度，即按照事先确定的价值尺度将资产的价值划分为不同等级。
2. 对资产进行识别时，若贵馆拥有这项资产，请您在该资产对应的”是否存在”栏打勾（√），若没有这项资产空白即可。
3. 您可以根据贵馆的实际情况添加表中没有的资产，或改变表中的资产名称。
4. 对资产的进行赋值时，按照等级赋值法，将资产的安全属性（保密性、完整性、可用性）以及资产的价值分别进行了五级划分，请您从保密性、完整性和可用性这三个方面对信息资产进行赋值，并采用定性的方式来划分资产的价值或重要度，并将赋值结果填写在表格中。

信息资产列表			是否存在	重要性赋值		
				保密性	完整性	可用性
电子资源类	电子图书					
	电子期刊					
	学位论文					
	多媒体资源库					
	文摘数据库					
	其他类数据库					
数据文档类	书目数据					
	用户信息数据					
	源代码					
	系统文档					
	软件相关数据					
	安全相关数据					
	查新报告（电子/纸质）					
	各类合同（电子/纸质）					
	用户手册					
	培训资料					
	规章制度					
实物资产类	基础设施	供电设施（包括外部电源、内部电源和UPS）				
		空调系统（包括空气过滤系统）				
		消防设施				
		防雷设施				
	网络设备	交换机				
		路由器				
		集线器				
		调制解调器				
		无线设备				
	计算机设备	台式计算机				
		移动笔记本				

Appendix. (Continued)

信息资产列表			是否存在	重要性赋值		
				保密性	完整性	可用性
		PC服务器				
		小型机				
		大型机				
		工作站				
	存储设备	光盘塔				
		磁盘阵列				
	移动存储设备	U盘				
		光盘				
		移动硬盘				
	安全保障设备	数据备份设备				
		系统备份（镜像，克隆，容灾）				
		硬件防火墙				
		监控设备				
	其他电子设备	扫描仪				
		复印机				
		打印机				
		传真机				
		投影仪				
		录音设备				
		影像设备				
		条形码阅读器（CCD）				
软件资产类	应用软件	图书管理系统（业务管理系统）				
		一卡通系统				
		学科导航系统				
		门户网站系统				
		门禁系统				
		电子资源服务平台				
		馆内自行开发的应用系统（请填写在下面）				
	系统服务平台	操作系统平台				
		数据库平台				
	安全防护软件	入侵检测系统				
		身份验证系统				
		防病毒软件				
		漏洞扫描系统				
服务类	办公服务	电力支持				
		物业管理（卫生，安全）				
	网络服务	提供的网络连接服务（校园网、电信）				
	第三方服务	外购产品享受的服务				
		软硬件维保				
人员类	管理人员（馆长、书记等）					
	维护人员	硬件维护人员				
		网络维护人员				
		系统维护人员				
	研发人员	软件研发人员				
		数据库研发人员				
	其他人员					