International Journal of Information Science and Management
Vol. 20, No. 1, 2022, 55-74
https://dorl.net/dor/20.1001.1.20088302.2022.20.1.4.7

Original Research

Identifying the Content Production Risk Components in Digital Libraries: A Qualitative Study

Raheleh Mohammad Salehi
Ph.D. candidate in Knowledge and Information Science, science and research Branch, Islamic Azad University, Tehran, Iran. Corresponding Author:
Raheleh.salehi.61@gmail.com
ORCID ID: https://orcid.org/0000-0001-7932-1808

Fahimeh Babalhavaeji
Associate Prof. Department of Communication and Knowledge Science, Science and Research Branch, Islamic Azad University, Tehran, Iran.
f.babalhavaeji@gmail.com
ORCID iD: https://orcid.org/0000-0002-0247-6614

Mitra Samiei
Associate Prof. Department of Communication and Knowledge Sciences, Faculty of Psychology & Educational Sciences, Alameh Tabatabai University, Tehran, Iran.
Samiei.mitra66@gmail.com
ORCID iD: https://orcid.org/0000-0001-7879-6457

Nadjla Hariri
Professor, Department of Communication and Knowledge Science, Science and Research Branch, Islamic Azad University, Tehran, Iran.
Nadjlahariri@gmail.com
ORCID iD: https://orcid.org/0000-0002-9703-5212

Received: 09 June 2020
Accepted: 21 July 2021

Abstract

Risk management is a preventive activity that identifies project risks and technical and non-technical problems for key managers and stakeholders by identifying project risks. The introduction of new digital forms of information not only has created rich and extraordinary opportunities for libraries to expand community access to information and create a positive relationship between libraries and users but poses some degree of risk. The present study employs a qualitative research approach with The Fuzzy Delphi Method (FDM). For data collection, a researcher-made questionnaire was used to identify the risks of content production in digital libraries. The FDM was employed for complete analysis using 20 IT experts on a 5-point Likert scale. The study identified 61 sub-components under nine main content production risk components: human, environmental, infrastructure, conservation and maintenance, technical, copyright, integration, evaluations of resource content, and information security risks. The present study addresses the content production risk components so that authorities can assist in planning and decision-making to prevent and resolve content production issues in digital libraries.

Keywords: risk management, risk identification, digital libraries, content production.

Introduction

ICT has affected libraries around the world so that many scientific resources are now available online. Besides, many researchers tend to use online resources over print sources

(Masrek, 2016), so digital libraries have become vital sources of information. Supporting the changes in libraries has been one of the priorities of the 2015 Strategic Plan. The rapid shift from print to digital content is one of the most dramatic developments in the current transformation of libraries of all kinds. Content production by librarians of the American Society includes precise and complete technical specifications, production of reliable main files, sufficient descriptive, managerial, and structural super data to ensure future access, accurate and meticulous quality control processes (the American Library Association, 2007). Most researchers believe that a collection is the most significant element in digital libraries. Also, the formation of appropriate collections is one of the essential elements for facilitating the digital library's achievement and use of primary goals. However, there are various problems in providing different objects and their efficiency level to users (NISO, 2007). Contemporary organizations operate under turbulent conditions. In fast-changing environments that are difficult to predict, in addition to creating opportunities for development and success, they are involved with significant risks and dangers (Bombiak, 2017).

The source of this turbulence is the complexity and multiplicity of new technologies as well as global developments that in recent years have made it possible to predict their risks accurately and possible consequences, and human beings, more than ever, face uncertainty in their activities (Becker & Smidt, 2015). The risk of an event, its size, and severity, or a combination of both (Merna, Al-Thani, 2005) and a mental phenomenon involving exposure and uncertainty (Svetlozar, Stoyan & frank, 2011) has been discussed. The literature shows that the term “risk” is presented in many definitions; however, there are two concepts in most of these definitions: 1. Expected probability and values, 2. Incidents, consequences, and uncertainty (Aven, 2010). The goal of risk management in a digital library is to identify, evaluate, and eliminate risk factors before the risks become a disaster for the digital library. Researchers have seen risk management as an opportunity, but it should be noted that risk characteristics vary. The key to organizing digital libraries is identifying and measuring them, facing the risks of digital libraries, and managing them to benefit all-digital library stakeholders. An essential element of the risk management process is ensuring identified risks and carefully reviewing their control process. Risk management benefits include centralized organization by creating the best practices and awareness risks, effective use of resources, especially human resources (Haimes, 2004). The first and most important step in the risk process is risk identification. Risk identification aims to create a list of risks based on events that can have significant consequences (Green, 2016).

Proper implementation of digital libraries requires managers to be aware of the risk and deal with it. The present study attempts to identify the risks in the production of digital library content to achieve the success and survival of digital libraries. The goal of risk management in digital libraries is to protect assets from all external risks (e.g., natural disasters) and internal risks (e.g., barriers such as unauthorized access, incorrect selection of templates for data protection and storage, etc.). Therefore, in the absence of understanding such risks, the relevant organization may suffer financial and time losses and ultimately will make digital libraries incapable of achieving their goals. Moreover, the most important, most costly, and time-consuming work process in a digital library is producing and providing digital resources. Thus, to produce content in digital libraries, traditional knowledge and specialized skills and familiarity with the risk factors as a threat factor, enjoy the ability to control them, and turn threats into opportunities seem necessary. New forms of digital information are rich and extraordinary opportunities for libraries to expand community access to information and build a positive relationship between libraries and users. Nevertheless, these new forms of digital content pose new challenges (American Library Association, 2007). The present study intends to identify the categories of risk of content production in digital libraries from the library experts' perspectives. It also seeks to identify the content production risks in digital libraries from the library experts' perspectives. It also provides the highest and lowest levels of agreement with identified risk categories.

Literature Review

The concept of risk dates back to 2,400 years ago when the Greeks considered the possibilities before deciding. Until Probability theory was developed, the only solution was to appeal to the gods. Then with the advent of human risk management, a significant step was taken to advance modern society. Several studies have found that there are challenges and risks in digital libraries. They can be divided into 2 general groups:1. Studies were focusing on the human resource risks in digital libraries such as Moghrabi Manzari (2019), Basafa, Babalhaveji & Alipour Hafezi (2017), Bagheri and Isfandyari Moghaddam (2014); and 2. Studies focusing on the risks of information protection and information technology in digital libraries such as Salajegheh, Soleimaninezhad & Ghaeemaghami (2016), Han, Huang, Li & Ren (2016), Andy et al. (2012), Myongho (2011), Kuzma (2010), and the OCLA Research Organization (2010).

Research focusing on human resource risks

In a study titled "evaluating human resource risks in digital libraries of public universities in Tehran", Moghrebi Manzari (2019) evaluated human resource risks. The results of this evaluation show that among the four risk groups, specialized skills, operational skills, human capital, and individual skills risks are the most prioritized ones, respectively. In a thesis, Basafa et al. (2017) identified the technical skills of digital librarians. This study, in addition to emphasizing the significance and identification of technical skills (hardware, software, Internet and networking, collecting, digital information processing, digital services, protection and maintenance of digital resources), showed that the technical skills of digital librarians working in libraries of Tehran state universities are not at the desired level.

Bagheri and Esfandiari Moghaddam (2014) conducted a study titled "human and technical skills in the management of specialized libraries" to identify professors' and library managers' opinions on the specialized libraries managers' skills. A questionnaire was employed to collect the data. The results showed that professors and managers considered human skills essential for managers of specialized libraries. Organization (2010) identified, classified, and prioritized the risks of research libraries' risks and ranked risks based on probability of occurrence and the effects estimated by the respondents. The results showed that the most significant risks include those related to human resources and organizational cultures, such as no attention to the employees' training and relocation, lack of technical skills in managing collections and data, prevention of innovation due to organizational culture, risk of attracting and retaining the staff, and uncertainty about the library managers' qualifications.

In addition to technology, these studies emphasize the significance and influential role of human resources in digital libraries, specialized technical and scientific knowledge and skills, human perceptions, and individual skills in digital libraries.

Research focusing on information protection & information technology

Salajegheh et al. (2016) Divided the challenges related to digital resources into 3 group Information challenges Include data protection and selecting and requesting appropriate resources. Economic challenges include infrastructure and equipment. Technology challenges included Userability and Inability to compete with print resources. Han et al. (2016) used an ISO 2700 to assess information protection risk in a Chinese digital library. The evaluation showed that the investigated library exposed seven significant information security risks. Besides, researchers made some suggestions for data protection. Andy et al. (2012) reviewed research on the issue of information security between 2000 and 2010. The results indicated that infrastructure, digital content, users and standards, legal issues, and in general, both technology and management play a vital role in the security of digital library information. Oehlerts and Shu (2013) stated that digital protection is integral to digital asset management. von Hielmcrone, Maiello, Bainton & Bonnet (2012) expressed that one of the main problems of electronic resources is gathering and copyright.

Myongho (2011) recommended a library security guideline by combining management, technology, and physical institutions to ensure the security of a digital library collection, users, and physical structure. Kuzma (2010) evaluated the damage to the European Library's website and its effects on user information security. The study found that librarians in charge of network systems did not appropriately assess online information security. In this group of research, categories such as software, hardware and equipment factors, management principles, and infrastructure, standards, legal issues, and spirituality have been identified and evaluated

Previous studies have identified and assessed the risks and hazards of information technology projects and libraries, most often human resources and information protection risks and technical and management equipment risks. This research has always emphasized the role of risk management in the success rate of information technology projects. They also show that risks and risks always target the goals and performance of IT projects and that digital libraries, as the crystallization of information technology, are no exception. Therefore, identifying and evaluating them plays a vital role in turning threats into opportunities for the growth and flourishing of digital libraries. Libraries should identify potential threats to their assets, find out how to respond to them, and ultimately create a policy as quickly as possible.

Methodology

The present study employed an applied, qualitative method and the FDM in two stages. First, with the initial studies and the use of previous studies, a set of indicators related to content production risks in digital libraries was obtained. A researcher-made questionnaire based on information obtained from the research literature was used to identify the content production risks in digital libraries to collect the data. In this method, the goal is a complete analysis using a large group of experts. The Delphi measurement was done using a 5-point Likert scale.

No sampling was performed in this study. According to the following criteria of the research population, 20 participants were selected via a purposive sampling method, among whom 13 participated in the study with the following inclusion criteria:

1. Those holding at least a bachelor's degree in information science and science assessment and 15 years of experience;

2. Experts engineering and management with at least 15 years of experience in risk management. Thus, a purposive sampling method was employed.

The initial list of library studies, including nine main items and 70 sub-items, was distributed among the experts. According to their comments, some risks were eliminated due to overlap or irrelevance to the research topic, and some were merged. So, a list with 9 main items and 61 sub-items was finalized. After preparing the final list in a letter, 20 experts in the field of information science and scientometrics, as well as experts in engineering and management with experience in the field of risk management, were asked to comment on each of the criteria and declare the level of agreement with the risks by selecting Likert options. Of 20 individuals, 13 answered the questionnaire. The mean scores of the answers to the questionnaire were estimated by the FDM and were ready to be sent again for the second stage of the survey. In the second stage, the experts were asked to reconsider and report the degree of agreement with the risks, considering the mean scores and eliminating one case of low-risk human resource index due to low scores. Figure (1) shows the research procedure:

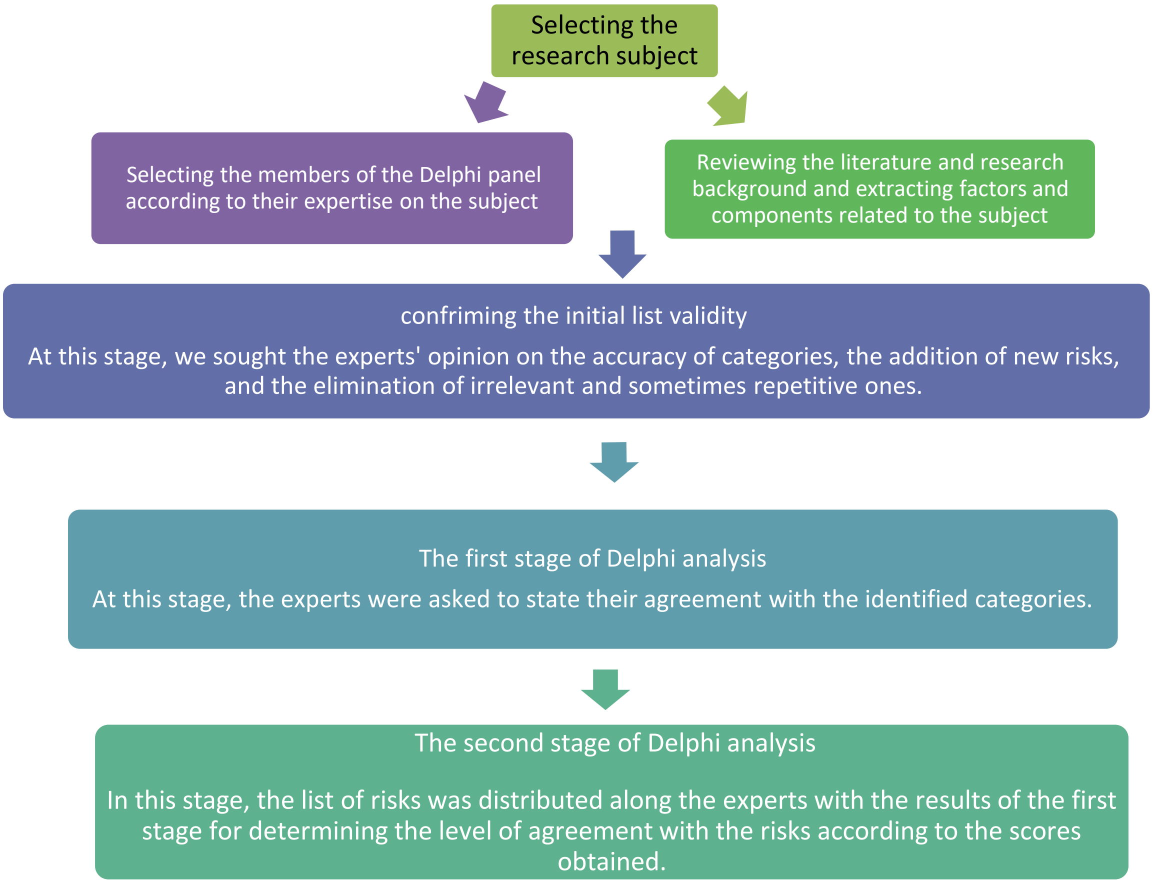
Selecting the research subject
Selecting the members of the Delphi panel according to their expertise on the subject
Reviewing the literature and research background and extracting factors and components related to the subject
confriming the initial list validity
At this stage, we sought the experts' opinion on the accuracy of categories, the addition of new risks, and the elimination of irrelevant and sometimes repetitive ones.
The first stage of Delphi analysis
At this stage, the experts were asked to state their agreement with the identified categories.
The second stage of Delphi analysis
In this stage, the list of risks was distributed along the experts with the results of the first stage for determining the level of agreement with the risks according to the scores obtained.

Figure 1: the research procedure

Research findings

As can be seen in Table 1, the main and secondary risks of content production in digital libraries, which was obtained from the knowledge gained from previous studies.

Table 1

List of the main and secondary extracted content production risks

Secondary risks	Main risks
1. Lack of knowledge in the field of new technologies and communication sciences	Human resource risks (Salari, 2010, Moghrebi Manzari, 2019)
2. Lack of skills in using new technologies and communication sciences	
3. Low-level information literacy[1]	
4. Lack of high level of ability in matters related to collecting, organizing and providing information[2]	
5. Lack of human resources	
6. Employees' low commitment	
7. Managers' inappropriate support	
8. Lack of personal skills in group work, problem-solving and decision making	
9. Lack of perceptual skills such as flexibility in times of risk, ability to negotiate and ability to communicate socially	
Secondary risks	Main risks
10. Risk of fire	Environmental risks (International Standard Organization, 2005)
11. Risk of natural disasters	
12. Cultural changes	
13. Social changes	
14. Political changes	
15. Humidity	
16. Lack of proper ventilation of workspaces	
17. Lack of lighting in workspaces	
18. Fungal and bacterial air pollution caused by fungi and bacteria in print information sources for digitization	
Secondary risks	Main risks
19. Lack of policy and lack of organizational perspectives due to the growth of information resources	Infrastructure risks (Norouzi, 2011; Salari 2010; Gatenby, 2005)
20. Use of employees' different opinions for building the organization	
21. Use of managers' different opinions for building the organization	
22. Incorrect forecasting of operating costs and provision of resources and facilities	
23. Improper selection of digital devices to build the collection	
24. Incorrect prioritization in digitalization of resources	
25. Instability of the parent organization	
26. Lack of suitable hardware infrastructure for digital library[3]	
27. Lack of proper bandwidth	
28. Lack of a digitalization manual	
Secondary risks	Main risks
29. Distortion of information (change of information)	Protection and maintenance risks (Samiei, Rezaei Sharifabadi, 2011; Rasouli & Vahdat, 2009; Han et al., 2016)
30. Data loss (deletion of some files)	
31. Insufficient variety of formats for the supply of digital items	
32. Incorrect selection of storage media[4]	
33. Lack of a backup file of motherboard information format	

Secondary risks	Main risks
34. Existence of duplicate resources and waste of cost, energy and time	
Secondary risks	Main risks
35. Obsolescence of technology equipment and supplies	Technical risks (Samiei, Rezaei Sharifabadi,2011; Norouzi, 2011; Garud, Hardy, & Maguire, 2007; International Standard Organization, 2005)
36. Negligence in software development	
37. Network and Internet connection slowness	
38. Improper hardware and software maintenance	
39. Destructive attacks of viruses and hackers	
40. Lack of well-designed and highly qualified software[5]	
41. Lack of software support for standards	
42. The inability of library software to interact with other libraries (interoperability)[6]	
43. Software's low security	
Secondary risks	Main risks
44. False and vague strategies for copyright protection	Copyright risks (Soltanifar,2010;Alipourhafezi,2019; Soltsnifar's diary (as cited in Samoelson, 2007)
45. Lack of legislative activity and legal considerations regarding access, copying, and publishing of resources	
46. Authors' ignorance of copyright law	
Secondary risks	Main risks
47. Lack of syntactic integration[7]	Integration risks (Alipourhafezi,2015)
48. Lack of semantic integration[8]	
49. Non-compliance with integration standards	
Secondary risks	Main risks
50. Lack of evaluation of information content by knowledgeable and specialized individuals	Evaluations of the resource content and copyright risks (Norouzi,2011; Samadi,2005)
51. Failure to update information content of continuous resources[9]	
52. No evaluation and review of the credibility of the authors or providers of the information source to validate and measure the quality of information content	
53. Lack of comprehensiveness of information	
Secondary risks	Main risks
54. Poor cryptographic management[10]	Information security risks (Baghbanzadeh, 2014; Samadi,2005 ; Han & et.,2016)
55. Non-commitment of employees to the organization and information retention (information theft)	
56. Failure to review and control audit of event registration, and failure to review user activities	
57. Disruption of user authentication	
58. Negligence of the use of security management standards	
59. Disruption of server security	
60. Disruption of cable security	
61. Malfunctions of security alarm systems in unauthorized time and accesses	

Description of demographic characteristics

Tables 2 and 3 illustrate the frequency and percentage of frequency related to the gender and field of participants. As Table (2) illustrates, of 13 participants, 10 (76.9%) were female, and 3 (23.1%) were male.

Table 2

Frequency and percentage of the participants' gender

Cumulative percentage	Valid percentage	percentage	F	Gender
76.9	76.9	76.9	10	Male
100	23.1	23.1	3	Female
-	100	100	13	Total
-	-	-	-	No answer
-	-	100	13	Total

As Table (3) illustrates, of 13 participants, 8 participants (61.5%) held a degree in information science, and 5 (38.5%) had a degree in engineering.

Table 3

Frequency and percentage of the participants' field

Cumulative percentage	Valid percentage	percentage	F	field
61.5	61.5	61.5	8	information science
38.5	38.5	38.5	5	engineers
-	100	100	13	Total
-	-	-	-	No answer
-	-	100	13	Total

The fuzzy mean method was employed to cumulate the experts' opinions. A simple relation $\frac{l+m+u}{3}$ was also used for defuzzification and the absolution of their opinions. Also, the threshold value is 0.6. Table 4 illustrates the results of the categories obtained from the first stage of the fuzzy mean.

Table 4

Defuzzification results of the aggregate values of the experts' opinions

Items	Mean opinion scores	Absolute value	Results
Lack of knowledge in the field of new technologies and communication sciences	(0.634, 0.884, 1)	0.839	Confirmed
Lack of skills in using new technologies and communication sciences	(0.692, 0.942, 1)	0.878	Confirmed
Low level information literacy	(0.570, 0.826, 0.961)	0.787	Confirmed
High level of inability to collect, organize, and present information	(0.576, 0.823, 0.942)	0.780	Confirmed
Lack of human resources	(0.288, 0.538, 0.807)	0.544	Rejected
Low commitment in employees	(0.596, 0.846, 1)	0.814	Confirmed
Managers' poor and inappropriate support from	(0.106, 0.846, 0.98)	0.644	Confirmed
Lack of individual skills in group work, problem-solving and decision making	(0.557, 0.807, 1)	0.788	Confirmed
Lack of perceptual skills such as flexibility in times of risk, ability to negotiate, and ability to	(0.519, 0.769, 0.961)	0.749	Confirmed

Items	Mean opinion scores	Absolute value	Results
communicate socially			
Risk of fire	(0.365, 0.557, 0.807)	0.576	Confirmed
Risk of natural disasters	(0.365, 0.615, 0.846)	0.608	Confirmed
Cultural changes	(0.480, 0.769, 0.961)	0.736	Confirmed
Social changes	(0.519, 0.765, 0.961)	0.748	Confirmed
Political changes	(0.5, 0.75, 0.961)	0.737	Confirmed
Humidity	(0.48, 0.711, 0.942)	0.711	Confirmed
Lack of proper ventilation of workspaces	(0.365, 0.576, 0.865)	0.602	Confirmed
Lack of lighting in workspaces	(0.403, 0.603, 0.903)	0.636	Confirmed
Fungal and bacterial air pollution caused by fungi and bacteria in print information sources for digitization	(0.519, 0.75, 0.923)	0.730	Confirmed
Lack of policy and lack of organizational perspectives due to the growth of information resources	(0.634, 0.884, 1)	0.839	Confirmed
Use of employees' different opinions for building the organization	(0.423, 0.703, 0.942)	0.689	Confirmed
Use of managers' different opinions for building the organization	(0.615, 0.865, 1)	0.826	Confirmed
Incorrect forecasting of operating costs and provision of resources and facilities	(0.575, 0.826, 1)	0.800	Confirmed
Improper selection of digital devices to build the collection	(0.576, 0.807, 1)	0.794	Confirmed
Incorrect prioritization in digitalization of resources	(0.596, 0.842, 1)	0.812	Confirmed
Instability of the parent organization	(0.596, 0.846, 1)	0.814	Confirmed
Lack of suitable hardware infrastructure for digital library	(0.75, 0.88, 1)	0.876	Confirmed
Lack of proper bandwidth	(0.557, 0.846, 1)	0.801	Confirmed
Lack of a digitalization manual	(0.557, 0.807, 1)	0.788	Confirmed
Distortion of information (change of information)	(0.653, 0.923, 1)	0.858	Confirmed
Data loss (deletion of some files)	(0.692, 0.923, 1)	0.871	Confirmed
Insufficient variety of formats for the supply of digital items	(0.408, 0.692, 1)	0.700	Confirmed
Incorrect selection of storage media	(0.364, 0.884, 1)	0.749	Confirmed
Lack of a backup file of motherboard information format	(0.576, 0.846, 1)	0.807	Confirmed
Existence of duplicate resources and waste of cost, energy and time	(0.615, 0.865, 1)	0.826	Confirmed
Obsolescence of technology equipment and supplies	(0.615, 0.715, 1)	0.776	Confirmed
Negligence in software development	(0.884, 0.826, 1)	0.903	Confirmed
Network and Internet connection slowness	(0.615, 0.884, 1)	0.833	Confirmed
Improper hardware and software maintenance	(0.557, 0.807, 1)	0.788	Confirmed
Destructive attacks of viruses and hackers	(0.692, 0.942, 1)	0.878	Confirmed
Lack of well-designed and highly qualified	(0.596, 0.846, 1)	0.814	Confirmed

Items	Mean opinion scores	Absolute value	Results
software			
Lack of software support for standards	(0.634, 0.884, 1)	0.839	Confirmed
The inability of library software to interact with other libraries (interoperability)	(0.634, 0.903, 1)	0.845	Confirmed
Software’s low security	(0.692, 0.884, 1)	0.858	Confirmed
False and vague strategies for copyright protection	(0.576, 0.826, 1)	0.800	Confirmed
Lack of legislative activity and legal considerations regarding access, copying, and publishing of resources	(0.615, 0.769, 1)	0.794	Confirmed
Authors’ ignorance of copyright law	(0.5, 0.73, 1)	0.743	Confirmed
Lack of syntactic integration	(0.653, 0.94, 1)	0.864	Confirmed
Lack of semantic integration	(0.669, 0.923, 1)	0.864	Confirmed
Non-compliance with integration standards	(0.634, 0.903, 1)	0.845	Confirmed
Lack of evaluation of information content by knowledgeable and specialized individuals	(0.692, 0.942, 1)	0.878	Confirmed
Failure to update information content of continuous resources	(0.634, 0.884, 0.98)	0.832	Confirmed
No evaluation and review of the credibility of the authors or providers of the information source to validate and measure the quality of information content	(0.384, 0.634, 0.865)	0.627	Confirmed
Lack of comprehensiveness of information	(0.576, 0.807, 0.942)	0.775	Confirmed
Poor cryptographic management	(0.538, 0.788, 0.942)	0.756	Confirmed
Non-commitment of employees to the organization and information retention (information theft)	(0.461, 0.711, 0.903)	0.691	Confirmed
Failure to review and control audit of event registration, and failure to review user activities	(0.519, 0.765, 0.98)	0.754	Confirmed
Disruption of user authentication	(0.576, 0.826, 1)	0.800	Confirmed
Negligence of the use of security management standards	(0.5, 0.75, 1)	0.750	Confirmed
Disruption of server security	(0.615, 0.865, 1)	0.826	Confirmed
Disruption of cable security	(0.48, 0.673, 0.942)	0.698	Confirmed
Malfunctions of security alarm systems in unauthorized time and accesses	(0.5, 0.73, 0.923)	0.717	Confirmed

Table (4) shows that the defuzzification results of the aggregate values of the experts’ opinion, i.e., the threshold value of the "the lack of human resources" criterion, is lower than the hypothetical value of 0.6. As a result, these criteria are removed from the content production risk management of framework criteria in Tehran state digital libraries because these criteria do not play a decisive role from the experts' perspectives.

The second stage of the FDM

At this stage, the difference of opinion of each expert was calculated with the mean opinion scores of the expert-panel members using equation (3). Then another questionnaire was given to them along with the previous opinion of each expert and the extent of his disagreement with the average opinion of the panel members. According to the opinions presented in the first stage and its comparison with the second stage results using equation (7), if the difference of opinion of the experts of the two stages is less than the threshold value 2, the survey process can be stopped.

The fuzzy mean method was employed to cumulate the experts' opinions. A simple relation $\frac{l+m+u}{3}$ was also used for defuzzification and the absolution of their opinions. Besides, the threshold value is 0.6. Table 5 illustrates the results of the categories obtained from the second stage of the fuzzy mean

Table 5

Defuzzification results of the aggregate values of the experts' opinions

Items	Mean opinion value	Absolute value	Results
Lack of knowledge in the field of new technologies and communication sciences	(1, 0.903, 0.653)	0.852	Confirmed
Lack of skills in using new technologies and communication sciences	(1, 0.884, 0.615)	0.833	Confirmed
Low level information literacy	(0.961, 0.769, 0.596)	0.775	Confirmed
High level of inability to collect, organize, and present information	(0.980, 0.826, 0.576)	0.794	Confirmed
Low commitment in employees	(0.923, 0.769, 0.966)	0.762	Confirmed
Managers' poor and inappropriate support from	(0.980, 0.846, 0.048)	0.624	Confirmed
Lack of individual skills in group work, problem-solving and decision making	(0.980, 0.769, 0.519)	0.756	Confirmed
Lack of perceptual skills such as flexibility in times of risk, ability to negotiate, and ability to communicate socially	(0.903, 0.692, 0.480)	0.691	Confirmed
Risk of fire	(0.923, 0.673, 0.966)	0.730	Confirmed
Risk of natural disasters	(0.903, 0.615, 0.461)	0.659	Confirmed
Cultural changes	(0.961, 0.750, 0.788)	0.749	Confirmed
Social changes	(0.903, 0.711, 0.519)	0.711	Confirmed
Political changes	(0.923, 0.769, 0.577)	0.749	Confirmed
Humidity	(0.923, 0.769, 0.519)	0.737	Confirmed
Lack of proper ventilation of workspaces	(0.865, 0.653, 0.365)	0.627	Confirmed
Lack of lighting in workspaces	(0.884, 0.673, 0.461)	0.672	Confirmed
Fungal and bacterial air pollution caused by fungi and bacteria in print information sources for digitization	(0.942, 0.788, 0.706)	0.762	Confirmed
Lack of policy and lack of organizational perspectives due to the growth of information resources	(0.961, 0.769, 0.577)	0.762	Confirmed
Use of employees' different opinions for building the organization	(1, 0.846, 0.596)	0.814	Confirmed
Use of managers' different opinions for building the organization	(1, 0.884, 0.634)	0.839	Confirmed
Incorrect forecasting of operating costs and provision of resources and facilities	(0.846, 0.769, 0.480)	0.698	Confirmed

Items	Mean opinion value	Absolute value	Results
Improper selection of digital devices to build the collection	(0.942, 0.769, 0.557)	0.756	Confirmed
Incorrect prioritization in digitalization of resources	(1, 0.884, 0.634)	0.839	Confirmed
Instability of the parent organization	(0.961, 0.826, 0.706)	0.787	Confirmed
Lack of suitable hardware infrastructure for digital library	(1, 0.903, 0.653)	0.852	Confirmed
Lack of proper bandwidth	(1, 0.846, 0.615)	0.820	Confirmed
Lack of a digitalization manual	(1, 0.865, 0.615)	0.826	Confirmed
Distortion of information (change of information)	(1, 0.865, 0.615)	0.826	Confirmed
Data loss (deletion of some files)	(1, 0.846, 0.557)	0.801	Confirmed
Insufficient variety of formats for the supply of digital items	(0.903, 0.673, 0.365)	0.647	Confirmed
Incorrect selection of storage media	(0.942, 0.634, 0.706)	0.717	Confirmed
Lack of a backup file of motherboard information format	(0.961, 0.846, 0.461)	0.756	Confirmed
Existence of duplicate resources and waste of cost, energy and time	(0.961, 0.750, 0.576)	0.762	Confirmed
Obsolescence of technology equipment and supplies	(0.961, 0.807, 0.596)	0.788	Confirmed
Negligence in software development	(0.980, 0.826, 0.538)	0.781	Confirmed
Network and Internet connection slowness	(0.942, 0.807, 0.596)	0.781	Confirmed
Improper hardware and software maintenance	(0.923, 0.750, 0.416)	0.711	Confirmed
Destructive attacks of viruses and hackers	(0.961, 0.923, 0.615)	0.833	Confirmed
Lack of well-designed and highly qualified software	(0.865, 0.769, 0.576)	0.736	Confirmed
Lack of software support for standards	(0.942, 0.807, 0.538)	0.762	Confirmed
Inability of library software to interact with other libraries (interoperability)	(0.961, 0.826, 0.706)	0.787	Confirmed
Software’s low security	(0.903, 0.750, 0.442)	0.698	Confirmed
False and vague strategies for copyright protection	(0.923, 0.826, 0.461)	0.736	Confirmed
Lack of legislative activity and legal considerations regarding access, copying, and publishing of resources	(0.923, 0.769, 0.519)	0.737	Confirmed
Authors’ ignorance of copyright law	(0.942, 0.788, 0.50)	0.730	Confirmed
Lack of syntactic integration	(0.923, 0.826, 0.706)	0.775	Confirmed
Lack of semantic integration	(0.961, 0.846, 0.596)	0.801	Confirmed
Non-compliance with integration standards	(0.923, 0.711, 0.423)	0.685	Confirmed
Lack of evaluation of information content by knowledgeable and specialized individuals	(0.942, 0.730, 0.50)	0.724	Confirmed
Failure to update information content of continuous resources	(1, 0.846, 0.596)	0.814	Confirmed
No evaluation and review of the credibility of the authors or providers of the information source to validate and measure the quality of information content	(0.903, 0.692, 0.480)	0.691	Confirmed

Items	Mean opinion value	Absolute value	Results
Lack of comprehensiveness of information	(0.923, 0.769, 0.338)	0.743	Confirmed
Poor cryptographic management	(0.961, 0.846, 0.596)	0.801	Confirmed
Non-commitment of employees to the organization and information retention (information theft)	(0.923, 0.769, 0.338)	0.743	Confirmed
Failure to review and control audit of event registration, and failure to review user activities	(0.961, 0.807, 0.776)	0.781	Confirmed
Disruption of user authentication	(0.903, 0.750, 0.50)	0.724	Confirmed
Negligence of the use of security management standards	(0.903, 0.711, 0.50)	0.704	Confirmed
Disruption of server security	(0.942, 0.826, 0.557)	0.775	Confirmed
Disruption of cable security	(0.961, 0.807, 0.776)	0.781	Confirmed
Malfunctions of security alarm systems in unauthorized time and accesses	(0.788, 0.807, 0.596)	0.788	Confirmed

Table (5) illustrates that the fuzzy results of the aggregate values of the experts' opinions, the tolerance threshold of all criteria is higher than the intended value of 0.6. As a result, no criterion was left out of the total criteria of the content risk management framework in Tehran state digital libraries because the experts believe these criteria play a decisive role.

According to the opinions presented in the first stage and its comparison with the second stage results, if the difference between the two stages is smaller than the threshold value of 0.2, the survey process can be stopped. From Table 6, it can be observed that differences of expert views in two stages of the fuzzy mean.

Table 6

The difference between the experts' opinions in the first and second stage of the survey

Items	First stage	Second stage	Differences
Lack of knowledge in the field of new technologies and communication sciences	0.839	0.852	0.019
Lack of skills in using new technologies and communication sciences	0.878	0.833	0.045
Low level information literacy	0.787	0.775	0.012
High level of inability to collect, organize, and present information	0.780	0.794	0.031
Low commitment in employees	0.814	0.762	0.052
Managers' poor and inappropriate support from	0.644	0.624	0.2
Lack of individual skills in group work, problem solving and decision making	0.788	0.756	0.032
Lack of perceptual skills such as flexibility in times of risk, ability to negotiate, and ability to communicate socially	0.749	0.691	0.058
Risk of fire	0.576	0.730	0.026
Risk of natural disasters	0.608	0.659	0.054
Cultural changes	0.736	0.749	0.011
Social changes	0.748	0.711	0.037
Political changes	0.737	0.749	0.012

Items	First stage	Second stage	Differences
Humidity	0.711	0.737	0.026
Lack of proper ventilation of workspaces	0.602	0.627	0.025
Lack of lighting in workspaces	0.636	0.672	0.036
Fungal and bacterial air pollution caused by fungi and bacteria in print information sources for digitization	0.730	0.762	0.032
Lack of policy and lack of organizational perspectives due to the growth of information resources	0.839	0.762	0.077
Use of employees' different opinions for building the organization	0.689	0.814	0.125
Use of managers' different opinions for building the organization	0.826	0.839	0.013
Incorrect forecasting of operating costs and provision of resources and facilities	0.800	0.698	0.102
Improper selection of digital devices to build the collection	0.794	0.756	0.038
Incorrect prioritization in digitalization of resources	0.812	0.839	0.027
Instability of the parent organization	0.814	0.787	0.027
Lack of suitable hardware infrastructure for digital library	0.876	0.852	0.024
Lack of proper bandwidth	0.801	0.820	0.019
Lack of a digitalization manual	0.788	0.826	0.038
Distortion of information (change of information)	0.858	0.826	0.032
Data loss (deletion of some files)	0.871	0.801	0.077
Insufficient variety of formats for the supply of digital items	0.700	0.647	0.053
Incorrect selection of storage media	0.749	0.717	0.032
Lack of a backup file of motherboard information format	0.807	0.756	0.051
Existence of duplicate resources and waste of cost, energy and time	0.826	0.762	0.064
Obsolescence of technology equipment and supplies	0.776	0.788	0.012
Negligence in software development	0.903	0.781	0.122
Network and Internet connection slowness	0.833	0.781	0.052
Improper hardware and software maintenance	0.788	0.711	0.077
Destructive attacks of viruses and hackers	0.878	0.833	0.045
Lack of well-designed and highly qualified software	0.814	0.736	0.078
Lack of software support for standards	0.839	0.762	0.077
Inability of library software to interact with other libraries (interoperability)	0.845	0.787	0.058
Software's low security	0.858	0.698	0.16
False and vague strategies for copyright protection	0.800	0.736	0.064
Lack of legislative activity and legal considerations regarding access, copying, and publishing of resources	0.794	0.737	0.057
Authors' ignorance of copyright law	0.743	0.730	0.013
Lack of syntactic integration	0.864	0.775	0.089
Lack of semantic integration	0.864	0.801	0.063
Non-compliance with integration standards	0.845	0.685	0.16
Lack of evaluation of information content by knowledgeable and specialized individuals	0.878	0.724	0.154
Failure to update information content of continuous resources	0.832	0.814	0.018
No evaluation and review of the credibility of the authors or providers of the information source to validate and measure the	0.627	0.691	0.008

Items	First stage	Second stage	Differences
quality of information content			
Lack of comprehensiveness of information	0.775	0.743	0.032
Poor cryptographic management	0.756	0.801	0.045
Non-commitment of employees to the organization and information retention (information theft)	0.691	0.743	0.124
Failure to review and control audit of event registration, and failure to review user activities	0.754	0.781	0.027
Disruption of user authentication	0.800	0.724	0.076
Negligence of the use of security management standards	0.750	0.704	0.046
Disruption of server security	0.826	0.775	0.051
Disruption of cable security	0.698	0.781	0.083
Malfunctions of security alarm systems in unauthorized time and accesses	0.717	0.788	0.078

Table (6) shows there was no difference of less than 0.2. As a result, no questions were removed. According to Table (6), each risk category's highest and lowest agreement levels can be extracted. For human resources risks, the highest level of agreement is related to the risk of lack of knowledge in new technologies and communication sciences. The lowest level of agreement is related to the risk of managers’ poor and inappropriate support. In the case of environmental risks, the highest level of agreement was related to cultural and political changes, and the lowest level of agreement was related to the risk of lack of proper ventilation in the workplace.

For infrastructure risks, the highest level of agreement is related to the lack of the digital library's appropriate hardware infrastructure. The lowest level of agreement is related to the risk of incorrect forecasting of operating costs and the provision of resources and facilities. Regarding the protection and maintenance risks, the highest level of agreement is related to the distortion of information. The lowest level of agreement is related to the risk of insufficient formats for the supply of digital items. Besides, for technical risks, the highest level of agreement is related to the risk of destructive attacks of viruses and hackers, and the lowest level of agreement is related to software’s low security.

For copyright risks, the highest level of agreement was related to the risk of incorrect and unspecified copyright protection strategies. In contrast, the lowest level of agreement was related to the risk of the authors' ignorance of copyright law. The highest and lowest levels of agreement are the risk of semantic non-integration and the risk of non-compliance with integration standards. For evaluations of resource content and copyright risks, the highest level of agreement is related to the risk of not updating the information content of the associated resources. In contrast, the lowest level of agreement was related to the risk of no evaluation and review of creditors' credibility. Moreover, for information security risks, the highest and the lowest level of the agreement are related to the lack of poor cryptographic management and the risk of negligence of using security management standards.

Discussion

The complexity and diversity of new technologies as well as global developments in recent years have made it impossible to predict their risks and possible consequences accurately, and human beings, more than ever, face uncertainty in their activities (Becker & Smidt, 2015), So to increase the probability of projects success, avoid or decrease of risks and optimization of opportunities, risk management will be done. The first and most important step in risk management is risk identification. Risk identification aims to create a list of risks based on events that can have significant consequences (Green, 2016). Forming appropriate collections is one of the most important elements for facilitating the digital library's achievement and primary goals. However, there are various problems in providing different objects and their efficiency level to users (NISO, 2007).

The present study aimed to identify content production risks in digital libraries. The present study employed an applied, qualitative method and the FDM in two stages. It showed that content production is the first and most important step in forming digital libraries, due to the emergence of the web, software, and hardware and diversity in providing information resources threatened by many risks and experts on various risks with They agreed. At first glance, digital libraries do not pose significant risks to society compared to other technology projects, but in most cases, paying attention to and identifying this amount of risk can be very important in the decision-making process and having a valid and ideal digital library. Also, by identifying risks, threats can be turned into opportunities. The findings of this study can prevent the barriers and problems of digital libraries in the production of content and take advantage of opportunities. For example, when the destructive attacks of viruses and hackers in a library are a serious threat and have been repeatedly damaged in this area, recognizing this category can prevent it by strengthening security systems and making the best decision to deal with it when it occurs.

In the present study, the experts identified sixty-one secondary risks in the field of content production under nine main risks (human resources risks, environmental risks, infrastructure risks, protection and maintenance risks, technical risks, copyright risks, and integration risks, evaluations of resource content risks, copyright risks, and information security risks). The research findings suggest that digital libraries will be further threatened by neglecting to upgrade their data in new technologies and communication sciences and ignoring appropriate hardware equipment. Today, however, we are witnessing significant growth in new technologies and communication sciences and advances in hardware technology. Therefore, it requires more attention and importance in these categories because not paying attention to them can create many problems in producing valuable and valid content.

Numerous studies have been conducted to assess the status or feasibility of creating a digital library which has identified several challenges. It can be observed that the results of the present study are consistent with those of Mogharebi Manzari (2019), Basafa et al. (2017), and Bagheri and Esfandiari Moghaddam (2014) in terms of the human resources risks. The results indicate the significance of human resources and technical skills in digital libraries. The literature focused on information security, technical risks, and library equipment risks in digital libraries and information technology, confirming the present study's findings. Han et al. (2016), Andy et al. (2012). , Kuzma (2010), Salajegheh et al. (2016), the OCLC Research Organization (2010) cited infrastructure, standards, legal issues, security guidelines, and intellectual property risks, Information challenges, Economic challenges, Technology challenges. Also, it was found based on research that there are numerous risks in digital libraries that can be better managed by identifying risks. Therefore the first accomplishment of this study is to obtain criteria for risk management in Iranian digital library; it is in line with researches of Myongho (2011) that recommended a library security guideline by combining management, technology, and physical institutions to ensure the security of a digital library collection, users, and physical structure.

Conclusion

The mission of digital libraries is to deliver accurate information to users without time or space constraints. The findings suggest that digital library projects contain several risk factors. The successful implementation of these projects depends on the effective management of these risks. Therefore, the results of this study are the beginning of effective risk management in digital libraries. These risks' probability of occurrence, severity, and effectiveness will vary from digital to other digital libraries. The results of this research can be used separately in future research to assess risks in each digital library and plan, deal with, or eliminate risks and make optimal use of opportunities for each digital library.

According to the results, there are suggestions for improving things:

1. Each digital library should form a risk management team and review and identify positive and negative events over the past years to identify the highest rate of occurrence and the most significant impact of error and problem;

2. The risk management research team should propose solutions to prevent, or minimize, the negative impact of errors and risks and their benefits;

3. Implement strategies to address or mitigate risks;

4. Revising and being aware of the progress of the work process and fixing errors and problems; and

5. Revising the proposed solutions.

If the risk management process is dynamic and current, it requires repeated processes over time. Besides, according to the results, the following strategies can be used to respond to risks:

1. Holding training courses to improve technical and scientific skills, as well as individual and perceptual skills;

2. The entry of documentary information on the names of authors and publishers;

3. Controlled indexing on the agenda of indexers;

4. Careful completion of information fields to integrate effective meaning;

5. Choose the right and efficient software

6. Regular monitoring of the accuracy and security of equipment and hardware upgrades;

7. Updating the content of information resources and reviewing the credibility of the authors;

8. Adherence to standards;

9. Determine the exact policy and follow it;

10. Carefully enlighten employees about information security;

11. Determining the right of access and updating it;

12. Use passive defense techniques with the participation of security systems to design hacker attacks and identify security holes, install and update antivirus;

13. Sterilize polluted environments and information resources for digitalization;

14. Predicting and estimating costs;

15. Preparing the appropriate infrastructure to create a suitable and reliable digital warehouse.

Endnotes

1. Low speed in responding to external sources, lack of skill in finding useful information, lack of awareness in actively providing information services and adding value to information.
2. Inability to select information and evaluate its usefulness, inability to collect information in the best way, inability to process, organize information, and inability to disseminate information to users at the right time and place.
3. Lack of hardware equipment for installation, deployment, commissioning such as scanners, digitizers, storage tanks, communication equipment for remote customer service
4. As the volume of digital resources increases, so does the size of the storage tank. Therefore, choosing the right storage media is essential.
5. Features of good software: simplicity, hierarchy, its clear and transparent design, and its part-by-part nature.
6. The ability of one system to interact and exchange information without intermediaries with other systems is called interoperability.
7. In syntactic integration, factors such as the hardware and software communication of digital library information systems and issues such as metadata output and input standards, a memorandum of understanding, and metaphysical descriptive language are discussed.
8. Semantic integration establishes a semantic relationship between scattered information resources in digital libraries and enables semantic retrieval and semantic communication between scattered information sources.
9. Regarding the continuously provided resources, due to the rapid changes in the web environment and the Internet, if the information provider is not updated, the provision of resources and new resources to users will face many problems. Therefore, it is important to evaluate and update them.

References

Alipour Hafezi, M. (2019). Digital Libraries: Interoperability. Tehran: SAMT. [in Persian]

Alipour Hafizi, M. (2015). Semantic integration of information resources in Iranian digital libraries. *Journal of National Studies on Librarianship and Information Organization* (NASTINFO), 26(3), 93-113. [in Persian]

American Library Association. (2007). definition of digital library collection & technical services. Retrieved from https://www.ala.org/alcts/resources/preserv/defdigpres0408

Aven T., Renn O. (2010). *Risk management and governance: Concepts, guidelines, and applications.* Berlin: Springer- Verlag.

Bagheri, T. & Isfandyari Moghaddam, A. (2014). Human and technical skills required to manage special libraries: Views of LIS academics and practitioners. *Journal of National Studies on Librarianship and Information Organization* (NASTINFO), 25(4), 89- 99. [in Persian]

Basafa, M., Babalhaveji, F., & Alipour Hafezi, M. (2017). Digital librarians' technical skills in central libraries of Tehran State Universities. *Knowledge Retrieval and Semantic Systems*, 4(12), 79- 108. [in Persian]

Becker, K. & Smidt, M. (2015). A risk perspective on human resource management: A review and directions for future research. *Human Resource Management Review*, 26(2), *149-195.* https://doi.org/10.1016/j.hrmr.2015.12.001

Bombiak, E. (2017). Human resources risk as an aspect of human resources management in turbulent environments. In Strategica : Shift, Major challenges of today's economy. eds.

Florina Pînzaru [et al.] (pp. 121–132). Tritonic Publishing House.

Garud, R., Hardy, C., & Maguire, S. (2007). Institutional entrepreneurship as embedded agency: An introduction to the special issue. *Organization Studies.,* 28(7), 957-969. https://doi.org/10.1177/0170840607078958

Gatenby, P. (2005). *Getting started: What needs to be in place to maintain access to digital collections.* Retrieved from http://archive.ifla.org/IV/ifla71/papers/032e-Gatenby.pdf

Green, P. E. (2016). Introduction to Risk Management Principles. In P. E. Green, *Enterprise Risk Management* (p. 7). Amsterdam: Elsevier.

Haimes. (2004). *Risk modeling, assessment, and management* (2 ed.). New Hersey: Wiley-IEEE.

Han, Z., Huang, S., Li, H. & Ren, N. (2016). Risk assessment of digital library information security: a case study. *The electronic library*, 34(3), 471-487. https:// doi.org/10.1108/EL-09-2014-0158

Kuzma, J. (2010). European digital libraries: Web security vulnerabilities. *Library Hi Tech, 28*(3), 402-413. https://doi.org/10.1108/07378831011076657

Masrek MN, G. J. (2016). Assessing users satisfaction with web digital library: The case of Universiti Teknologi MARA. *The International Journal of Information and Learning Technology*, 33(1), 36-56. https://doi.org/10.1108/IJILT-06-2015-0019

Merna T., Al-Thani F. (2005). *Corporate risk management: An organizational perspective.* England: John Wiley & Sons.

Moghrebi Manzari, H. (2019). *Assessing Human Resource Risks in Digital Libraries of Tehran State Universities*. M. A thesis. Allameh Tabatabai University, Faculty of Educational Sciences and Psychology. [in Persian]

Myongho, Y. (2011). Balanced security controls for 21st-century libraries. *Library & Archival Security,* 24(1), 39-45. https://doi.org/10.1080/01960075.2011.563132

NISO National Information Standards Organization (2007). *A Framework of Guidance for building good digital collections.* Retrieved from https://www.niso.org/sites/default/files/2017-08/framework3.pdf

Norouzi, Y. (2011). Axes of development of digital libraries. Research on Information Science and Public Libraries, 17 (1), 129-153. [in Persian]

Oehlerts, B. & Shu, L. (2013). Digital preservation strategies at Colorado State University Libraries. *Library Management* 34(1/2), 83–95. https://doi.org/10.1108/01435121311298298

Rasouli, N. & Vahdat, D. (2009). Key data protection methods in computers, computer networks, and wireless environments. Modern Science, No. 203. [in Persian]

Salajegheh, M., Soleimaninezhad, A. & Ghaeemaghami, M. (2016). Evaluation of the challenges of materials and digital resources at university libraries in Kerman. *International Journal of Information Science And Management (IJISM)t.* 14 (1), 39-45. Retrieved from https://ijism.ricest.ac.ir/index.php/ijism/article/view/726

Salari, M. (2010). The challenges and management issues of libraries in the transition from a traditional library to a digital library look at Iran. *Journal of Library and Information Science*, 13 (2), 97-112. [in Persian]

Samadi, M. J. (2005). Data Center Information Security Management based on BS7799 / IS017799 standard. In *Conference on the Role of Data Centers in Developing*

Information and Communication Technology. [in Persian]

Samiei, M. & Rezaei Sharifabadi, S. (2011). Digital Preservation in Digital Libraries: Review of Strategies. *Librarianship and Information Organization* (NASTINFO). 21(4),88-102. [in Persian]

Soltanifar, M. (2010). Copyright in the electronic world. *Media Studies*, 6(1), 41-62. [in Persian]

Svetlozar T., Stoyan V., frank J. (2011). *A portability metrics approach to financial risk measures.* London: John Wiley & Sons.

The international standard organization, (2005). *Information technology- security technology-code of practice for information security management: ISO/IEC 17799*. Switzerland: ISO.

von Hielmcrone, H., Maiello, R., Bainton, T. & Bonnet, V. (2012). E-publishing and the challenges for libraries. Retrieved from https://www.db.dk/files/E%E2%80%90publishing%20and%20the%20challenge%20for%20libraries%20-%20discussion%20paper.pdf