Information security risk management for computerized health information systems in hospitals: a case study of Iran

Javad Zarei1
Farahnaz Sadoughi2

1Health Information Management, Health Management and Economics Research Center, School of Health Management and Information Science, Iran University of Medical Sciences, Tehran, Islamic Republic of Iran.
2Health Information Management Department, School of Health Management and Information Science, Iran University of Medical Sciences, Tehran, Islamic Republic of Iran.

Background: In recent years, hospitals in Iran – similar to those in other countries – have experienced growing use of computerized health information systems (CHISs), which play a significant role in the operations of hospitals. But, the major challenge of CHIS use is information security. This study attempts to evaluate CHIS information security risk management at hospitals of Iran.

Materials and methods: This applied study is a descriptive and cross-sectional research that has been conducted in 2015. The data were collected from 551 hospitals of Iran. Based on literature review, experts’ opinion, and observations at five hospitals, our intensive questionnaire was designed to assess security risk management for CHISs at the concerned hospitals, which was then sent to all hospitals in Iran by the Ministry of Health.

Results: Sixty-nine percent of the studied hospitals pursue information security policies and procedures in conformity with Iran Hospitals Accreditation Standards. At some hospitals, risk identification, risk evaluation, and risk estimation, as well as risk treatment, are unstructured without any specified approach or methodology. There is no significant structured approach to risk management at the studied hospitals.

Conclusion: Information security risk management is not followed by Iran’s hospitals and their information security policies. This problem can cause a large number of challenges for their CHIS security in future. Therefore, Iran’s Ministry of Health should develop practical policies to improve information security risk management in the hospitals of Iran.

Keywords: information security, risk management, health information systems, hospital
Computerized information systems of organizations are faced with a variety of internal and external threats, which can cause different types of damages. They can have adverse effects on organizational operations, information assets, individuals, organizations, and national areas of studies. Therefore, information security is crucial for organizational survival, minimizing threats endangering organizational operations, and protection of confidentiality, integrity, and availability of information. The main objective of “information security” is implementing appropriate control measures for eliminating or minimizing the impacts of different organizational security-related threats and organizational vulnerabilities. The main question is how information security can be effectively and economically implemented in organizations. The answer is Information Security Risk Management (ISRM).

ISRM is a structured and continuous process with the purpose of identifying, evaluating, and minimizing some types of risks, as well as achieving appropriate acceptability. ISRM is very important for organizational successful information security programs for the following reasons. First, information security risks are not constant over time and vary depending on the conditions of the organizations, development and changes in the information system, new users, and so on. ISRM is one of the ways to reduce the negative impact of risks on the organization. Second, through risk management, organizations can concentrate on resources of high-risk areas and can manage them by using appropriate and measurable ways while limiting risks reasonably. Third, one of the characteristics of a successful security program is cost–benefit analysis of the implementation of information security controls. This accurate analysis is performed by the risk management process.

In Iran, a hospital is the main health care organization. Thus, one of the major pieces of health information is recorded at hospitals. In the past decade, CHIS has been increasingly used by Iran’s hospitals. Accordingly, clinical, financial, and administrative activities of hospitals are increasingly dependent on the performance of the CHIS, as compared with the past. Therefore, ensuring information security in these systems is of crucial importance for the hospitals. However, in recent years, CHIS security at Iran’s hospitals has faced greater challenges. In 2014, for the purpose of reducing public costs of health care, a health reform plan was implemented as one of the major policies of the new government. Accordingly, hospitals are required to connect their hospital information system programs to the Iranian system of electronic health records (SEPAS system) through the Internet. Connection through public Internet network considerably increases the risks of unauthorized access to information; meanwhile, some findings reveal lack of specified rules on confidentiality of patient information in electronic health systems of hospitals. Moreover, in recent years, due to the disputes concerning Iran’s nuclear program and Iran’s disagreements with Western countries and some of the Middle East countries, Iran’s computer information system has been exposed to cyber threats, such as the Internet viruses Stuxnet and Flame. These viruses, according to many information security experts in the world, are very complex and cannot easily be confronted. In 2014, the information security firms Kaspersky Lab and Symantec reported an advanced espionage malware (Regin), one of whose target countries was Iran.

Considering the information security risks at Iran’s hospitals and importance of ISRM in reducing and minimizing adverse effects of information security risks, as well as the effectiveness of the information security programs in hospitals, this study investigates the ISRM status at hospitals of Iran. Findings of this study can provide a comprehensive view of the ISRM situation and its place in health information security policies of hospitals and can help researchers and policy makers interested in ISRM in health care.

**Materials and methods**

This applied research is a descriptive cross-sectional study conducted in 2015. All active hospitals in Iran (until August 2014) were studied. In the first step, the research instrument for the assessment of ISRM situation in the hospitals of Iran was designed. To design the instrument, key processes of ISRM were identified by using the literature review in related information sources. The gathered data included guidelines, frameworks, standards, and methodologies for information security risk assessment and risk management, previous studies on ISRM in the hospitals, and other documents related to ISRM.

Several search engines and databases such as Google Scholar, Institute of Electrical and Electronics Engineers Digital Library, Association for Computing Machinery Digital Library, and PubMed were searched to find the relevant documents. Documents were identified by the following keywords: “Information security risk management” and “Information security risk assessment”, combined with the terms “Standard”, “Method”, “Model”, “Framework”, “Guideline”, and “Best practice” or “Hospital”, and “Health” in English language. We confined our search to documents published from 2000 to 2014. Inclusion criteria for selecting resources included the...
following: 1) availability of documents in English language and 2) free access to full-text documents. Non-full-text articles and documents were excluded. Literature was reviewed to data saturation level. When at least a risk assessment and management process principle appears in five retrieved sources, including articles, books, standards, guidelines, and methodologies, it was considered data saturation level. The data saturation level was determined based on three experts’ judgment (specialist in information security risk management). Sampling was not performed, and all the relevant literature, retrieved based on inclusion criteria, were evaluated.

A checklist was used to extract content from retrieved documents. In total, the specific guidelines, standards, and methodologies for information security risk assessment and risk management were as follows: International Standard Organization/International Electrotechnical Commission (ISO/IEC) 27005, National Institute of Standards and Technology Special Publication 800-30 (NIST SP 800-30), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) allegro, Method for Harmonized Analysis of Risk (MEHARI), Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGRIT), Information Technology Security Guidance- IT security risk management: a lifecycle approach-33 (ITSG-33), Security Officers Management & Analysis Project (SOMAP), Threat Agent Risk Assessment (TARA), CORAS, Threat Vulnerability and Risk Analysis (TVRA), Factor Analysis of Information Risk (FAIR) Analysis (O-RA), and Expressions des Besoins et Identification des Objectifs de Sécurité (EBIOS); and international standards of information security management (ISM), including ISO/IEC 17799 and ISO 27799, were identified and surveyed. Moreover, eight studies related to information security risk assessment and risk management in hospital, one report, and one book were retrieved and reviewed. In the second step, key processes of ISRM were extracted from the retrieved literatures. Figure 1 shows these stages.

In the third step, based on results of the previous stage, health information management and computer experts’ opinions, and observations of the five selected hospitals, a comprehensive form was designed to assess the status of ISRM for computerized health information systems, including four distinct parts encompassing general information about hospitals, specifications of computerized health information systems, information security incidences, and self-assessment checklist of ISRM. Its content validity was confirmed by 12 experts of health information management, medical informatics, information technology (IT), and computer engineering (three professionals per area of study). These scholars were selected on the basis of their previous work experience in the hospital’s IT departments or their familiarity with the structure of the IT department in the hospitals of Iran. For data collection, this questionnaire and its guideline were sent to all 908 active hospitals in Iran by the Ministry of Health of Iran. To remove any possible ambiguity, an instruction sheet was attached to this questionnaire, explaining all sections. The hospitals were selected with regard to their CHIS application, such as hospital information system, Electronic Medical Record, Patient’s Admission and Discharge Systems, and so on. Hospitals that did not use CHIS at the time of this research were excluded. To facilitate and expedite the collection of data, this form was placed electronically in the official Web site (portal) of the Ministry of Health of Iran and hospitals were asked to register the relevant information in the aforementioned Web site.

After data collection, primary analysis was conducted in order to fix the defects and correct the information. Then,

---

**Figure 1** Key process of information security risk management.
hospitals were asked through a second formal letter to take action to correct the defect. The collected data were analyzed by using descriptive statistics (frequency) in Excel 2003 software.

Ethical issues
The study was approved by the Deputy of Research and Technology of the Iran University of Medical Sciences, Tehran, Iran.

Results
Information related to the studied hospitals
Out of 908 active hospitals in Iran, 551 hospitals (60.7%) participated in the study. Two hospitals were setting up CHIS at the time of this research. Therefore, they were excluded from the study and 549 hospitals (60.5%) were studied. The highest percentage of participation in the study was related to the hospitals affiliated to the Medical Sciences Universities (Table 1).

Table 1 Distribution of hospitals in Iran that participated in the study

<table>
<thead>
<tr>
<th>Type of ownership</th>
<th>Active hospitals in Iran</th>
<th>Hospitals participating in the study</th>
<th>Participation percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Teaching hospital</td>
<td>Nonteaching hospital</td>
<td>Total</td>
</tr>
<tr>
<td>Universities of Medical Sciences</td>
<td>241</td>
<td>324</td>
<td>565</td>
</tr>
<tr>
<td>Private</td>
<td>2</td>
<td>140</td>
<td>142</td>
</tr>
<tr>
<td>Military</td>
<td>6</td>
<td>45</td>
<td>51</td>
</tr>
<tr>
<td>Charity</td>
<td>1</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td>Others</td>
<td>20</td>
<td>100</td>
<td>120</td>
</tr>
<tr>
<td>Total</td>
<td>270</td>
<td>638</td>
<td>908</td>
</tr>
</tbody>
</table>

Information security policies and procedures in hospitals
There were some policies and procedures for information security in 379 hospitals (69%). Only in eight hospitals (1.4%), these policies and procedures were provided based on specific information security standards such as ISO/IEC 27001. Additionally, all of these hospitals had a framework for ISM. Other hospitals pursued Iranian Hospitals Accreditation Standards. Only eight hospitals had a framework for ISRM, of which seven hospitals implemented security policies and procedures of specific information security standards. None of the hospitals had a systematic approach for ISRM (Table 2).

Table 2 Policies and procedures for information security in hospitals

<table>
<thead>
<tr>
<th>Type of ownership</th>
<th>Policies and procedures for information security</th>
<th>Framework for information security management</th>
<th>Framework for information security RA/RM</th>
<th>Number of hospitals</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Based on Iranian Hospital Accreditation Standard</td>
<td>Defining framework for ISM</td>
<td>Using a systematic approach to defining framework for ISM</td>
<td>Using a systematic approach to defining framework for information security RA/RM</td>
</tr>
<tr>
<td></td>
<td>Policy and procedures based on information security standards</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Universities of Medical Sciences</td>
<td>245</td>
<td>3</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Private</td>
<td>65</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Military</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Charity</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other organizations</td>
<td>54</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>379</td>
<td>8</td>
<td>10</td>
<td>3</td>
</tr>
</tbody>
</table>

Abbreviations: ISM, information security management; RA/RM, risk assessment/risk management.
Process of information security risk identification at hospitals
Among the main activities of information security risk identification, only identification of assets, identification of threats, and control analysis were performed systematically in a few hospitals; these hospitals took ISM into consideration. At some hospitals, there was no sequence among the subactivities related to information security risk identification, ie, the activities were performed unrelated to their previous and subsequent activities. Altogether, the obtained findings indicated the lack of a systematic approach for risk identification. Among the subactivities related to information security risk identification, the highest frequency was related to information assets identification (415 instances; Table 3).

Process of information security risk analysis and evaluation at hospitals
None of the subactivities related to the process of information security risk analysis and evaluation was performed systematically at the selected hospitals. Although risk evaluation was not carried out in hospitals, 124 hospitals attempted to prioritize the information security risks (Table 4).

Processes of information security risk treatment and risk acceptance at hospitals
No comprehensive plan was conducted for reducing information security risks. The main approach of hospitals to risk treatment was risk reduction, along with implementation of basic information security safeguards. None of the subactivities related to the processes of information security risk treatment and acceptance in hospitals was performed systematically (Table 5).

Residual risk acceptance and mitigation occurred only in six hospitals, which established ISM policies and procedures based on specific information security standards.

Communicating and sharing risk management results at hospitals
Communicating and sharing of risk management results were not observed in any of the hospitals.

ISRM monitoring and reviewing at hospitals
Information security policies and procedures, as well as implementation of control measures, were continuously monitored and reviewed at 146 hospitals and 142 hospitals, respectively, though it was not done systematically (Table 6).

Discussion
The results show lack of a systematic and comprehensive approach to ISRM at the studied hospitals. Although some activities are conducted for risk identification, risk evaluation, and risk treatment, they are not systematically structured, ie, the hospitals do not use the specialized methodologies or standards for ISRM. Therefore, there is no coherence between the activities related to ISRM at most hospitals. ISRM is a systematic, structured, and continuous process, through which various interdependent steps are taken, and the activities of each step are affected by the results of the previous stage. Without following a systematic and structured method, accurate risk assessment and management is not possible. Hence, various standards, methodologies, and tools are developed all over the world by public and private organizations, agencies, and different companies for information security risk assessment and management.

Only a small number of hospitals pursue ISRM framework; yet, they are not systematically structured. Defining a framework for risk management is one of the initial steps of implementation of the ISRM process. The framework development specifies scopes of risk management activity, required resources, key stakeholders, and limitations and boundaries of the risk management process and also makes a contribution to the ISRM process. Lack of risk management framework at Iran’s hospitals indicates weakness of information security policies and procedures. Information security policies are developed in conformity with Iranian Hospitals Accreditation Standards. Accordingly, hospitals are obliged to formulate policies and procedures for key processes in each department. But these standards are very limited, vague, and incomplete, as compared with specific standards, rules, or guidelines for information security, and do not cover many of the important details and processes of information security.

Only in a small number of hospitals, this policy was formulated based on specific standards of information security, such as ISO/IEC 27001. All these hospitals had a framework for ISRM. Information security standards such as the ISO 2700X series provide an appropriate framework for organizational ISM. Using standard methods for ISM and ISRM is of great importance. Although Iran is a member of the ISO and ISO 2700X standards have been accepted as the national standards of Iran, hospitals do not use these standards due to the lack of specific national laws.
Table 3 Information security risk identification in hospitals

<table>
<thead>
<tr>
<th>Type of ownership</th>
<th>Asset identification</th>
<th>Threat identification</th>
<th>Vulnerability identification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Frequency</td>
<td>Frequency</td>
<td>Frequency</td>
</tr>
<tr>
<td>Universities of Medical Sciences</td>
<td>294</td>
<td>140</td>
<td>Missing: 2</td>
</tr>
<tr>
<td>Private</td>
<td>55</td>
<td>26</td>
<td>2</td>
</tr>
<tr>
<td>Military</td>
<td>7</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Charity</td>
<td>9</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>50</td>
<td>18</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>415</td>
<td>194</td>
<td>7</td>
</tr>
<tr>
<td>Missing: 2</td>
<td>Missing: 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

on health information security. One of the reasons for this problem is weakness of major policies and rules associated with the health information security of Iran. Some studies reveal that rules of health information in Iran have some defects. In many developed countries such as Australia and the US, there are national regulations, standards, and guidelines for health information security, especially in the electronic environment. These rules provide health care organizations and other stakeholders with a comprehensive and consistent point of view regarding information security. In addition, these rules act as a comprehensive guideline for implementing information security programs in health care organizations. In addition, IT governance and the IT department structure of Iran's hospitals affect upon this problem. The research carried out by Shahi at ten hospitals of Iran demonstrates no framework for IT governance and IT department structure at the studied hospitals. Additionally, the findings reveal that there are problems with the IT department personnel, information security procedures, and IT policy making. IT governance has a great impact on the information security policies of the organization. The main advantage of existing information governance in an organization is creation of an organizational point of view toward information security. According to ISO 27799 standards, there should be an organizational point of view toward information security at hospitals. Information security needs to be an organizational activity with the participation of all employees. Information governance should be unified with clinical governance.

In their risk analysis model for hospital, Sunyaev and Pflug also emphasize on the responsibility of the hospital management in the information security process. The main problem of the IT department structure at Iran's hospitals is the IT personnel. In none of the hospitals is the title of CISO practically specified in the organizational structure of the IT department. CISO has a key role in ISM in an organization. Risk management, vulnerability assessment, and management of information security are all CISO skills. Furthermore, ISRM is a complex and specialized process and therefore, for applying the major information security risk assessment and management methodologies, specialized knowledge of the executive team, including the IT personnel, is required. Tavakoli et al reveal that the hospitals selected by them were not familiar with specific information security standards.

The success of ISRM depends on identification of all risks and, most importantly, analysis and determination of each risk level. Depending on the risk model used, risks are identified by determining risk factors such as assets, threats, vulnerability, likelihood of occurrence, and consequences. This study shows that determining the likelihood of occurrence and analysis of impact are carried out in less than one-third of the hospitals. Moreover, risk analysis and evaluation are not actually carried out in the hospitals. Determining likelihood of occurrence and analysis of impact have an important role in constructing the scenario for risk incidence and risk determination. Risk analysis and evaluation form the basis for risk prioritization.
as well as decision making about risk treatment.\textsuperscript{69} In addition, determining likelihood of occurrence, impact analysis, and risk analysis and evaluation require the use of precise quantitative or qualitative methods because it is more complicated, as compared with other stages of risk management. Accordingly, a variety of tools, examples, and methods are usually provided in risk assessment and management standards and methodologies for their accurate measurement.\textsuperscript{55} One reason for this weakness at the studied hospitals could be lack of specific methodologies and standards for risk assessment and management. Some other studies also indicate a weakness in ISRM in hospitals.\textsuperscript{54,70}

The main approach of hospitals for risk reduction is implementation of basic control measures of information security, which includes a set of management, technical, and physical conservation for information security protection. Some of the studies also indicate the implementation of basic control measures of information security.\textsuperscript{68}

**Conclusion**

There is a great distance between activities carried out in Iran for ISRM and the common and standard activities of ISRM in practice. There is no appropriate and standard approach to ISRM at Iran’s hospitals. This study suggests using specific information security standards such as ISO 2700x series as an effective method in the case of ISRM implementation. Considering the lack of specific national laws for health information protection in Iran, ISRM should be addressed comprehensively in a review of Iranian Hospitals Accreditation Standards. For a better performance of these cases, they should comply as much as possible with the standards of ISO 2700x series such as ISO 27799.

To help in risk calculation, based on the methodologies and specialized tools of information security risk assessment and risk management, a computer program should be designed by the Ministry of Health of Iran to calculate the risk and this should be made available to the hospitals. Moreover, hospitals should be asked to plan their ISM based on professional standards of information security such as ISO 2700x series.

**Acknowledgments**

This study was part of a PhD dissertation supported by the Iran University of Medical Sciences (grant number IUMS/SHMIS-1391/489). The authors thank the Office of Hospital Management and Clinical Service Excellence, Vice-Chancellor for Treatment, and the Ministry of Health of Iran for contributions to the study.

**Author contributions**

FS supervised the group, contributed to the first and the final drafts, and supervised the analysis of data. JZ designed the study, wrote the first draft and contributed to the final draft, collected data, and conducted the analysis.

**Disclosure**

The authors report no conflicts of interest in this work.
### Table 4 Information security risk analysis and evaluation in hospitals

<table>
<thead>
<tr>
<th>Type of ownership</th>
<th>Risk analysis</th>
<th>Risk evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Assessment of incidence scenarios</td>
<td>Using systematic approach to assessment of incidence scenarios</td>
</tr>
<tr>
<td></td>
<td>Frequency</td>
<td>Frequency</td>
</tr>
<tr>
<td>Universities of Medical Sciences</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Private</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Military</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Charity</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other organizations</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Table 5 Information security risk treatment and risk acceptance in hospitals

<table>
<thead>
<tr>
<th>Type of ownership</th>
<th>Define criteria for risk treatment and risk acceptance</th>
<th>Risk treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Define criteria for risk treatment option and action plan</td>
<td>Define criteria for residual risk acceptance</td>
</tr>
<tr>
<td></td>
<td>Frequency</td>
<td>Frequency</td>
</tr>
<tr>
<td>Universities of Medical Sciences</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Private</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Military</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Charity</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other organizations</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

### Table 6 Continuous monitoring and reviewing of ISRM in hospitals

<table>
<thead>
<tr>
<th>Type of ownership</th>
<th>Information security policy and procedure</th>
<th>ISRM policy and procedure</th>
<th>Risk factors</th>
<th>Risk management process</th>
<th>Implementation of security control measures</th>
<th>Residual risks</th>
<th>Using systematic approach to ISRM monitor and review</th>
<th>Number of hospitals</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Frequency</td>
<td>Frequency</td>
<td>Frequency</td>
<td>Frequency</td>
<td>Frequency</td>
<td>Frequency</td>
<td>Frequency</td>
<td>Frequency</td>
</tr>
<tr>
<td>Universities of Medical Sciences</td>
<td>91</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>89</td>
<td>2</td>
<td>0</td>
<td>404</td>
</tr>
<tr>
<td>Private</td>
<td>18</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>17</td>
<td>0</td>
<td>0</td>
<td>67</td>
</tr>
<tr>
<td>Military</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>Charity</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>Other organizations</td>
<td>27</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>26</td>
<td>3</td>
<td>0</td>
<td>58</td>
</tr>
<tr>
<td>Total</td>
<td>146</td>
<td>4</td>
<td>0</td>
<td>3</td>
<td>142</td>
<td>5</td>
<td>0</td>
<td>549</td>
</tr>
</tbody>
</table>

**Abbreviation:** ISRM, Information Security Risk Management.
## Information security risk management

### Table 4: Information security risk analysis and evaluation in hospitals

<table>
<thead>
<tr>
<th>Determination of the level of risk</th>
<th>Using systematic approach to determination of the level of risk</th>
<th>Risk evaluation Using systematic approach to risk evaluation</th>
<th>Prioritization of risks Using systematic approach to risk evaluation</th>
<th>Using systematic approach to prioritization of risks</th>
<th>Number of hospitals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>Frequency Frequency Frequency Frequency Frequency</td>
<td>Frequency Frequency Frequency Frequency Frequency Frequency</td>
<td>Frequency Frequency Frequency Frequency Frequency Frequency Frequency</td>
<td>Frequency Frequency Frequency Frequency Frequency Frequency Frequency Frequency Frequency Frequency Frequency Frequency Frequency Frequency Frequency</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0 0 3 0</td>
<td>0 0 8 0</td>
<td>0</td>
<td>0 0 124 0</td>
<td>404</td>
</tr>
<tr>
<td>1</td>
<td>0 0 1 0</td>
<td>0 0 18</td>
<td>0</td>
<td>0 0 549 0</td>
<td>67</td>
</tr>
<tr>
<td>0</td>
<td>0 0 0 0</td>
<td>0 0 4</td>
<td>0</td>
<td>0 0 12 0</td>
<td>8</td>
</tr>
<tr>
<td>0</td>
<td>0 0 0 0</td>
<td>0 0 2</td>
<td>0</td>
<td>0 0 12 0</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>0 0 4 0</td>
<td>0 0 18</td>
<td>0</td>
<td>0 0 58 0</td>
<td>58</td>
</tr>
<tr>
<td>0</td>
<td>0 0 8 0</td>
<td>0 0 124</td>
<td>0</td>
<td>0 0 549 0</td>
<td>549</td>
</tr>
</tbody>
</table>

### Table 5: Information security risk treatment and risk acceptance in hospitals

<table>
<thead>
<tr>
<th>Residual risk Identification and acceptance</th>
<th>Using systematic approach to risk treatment</th>
<th>Identification of residual risks</th>
<th>Residual risk acceptance and remedy</th>
<th>Using systematic approach to residual risk Identification and acceptance</th>
<th>Number of hospitals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency Frequency Frequency Frequency Frequency</td>
<td>Frequency Frequency Frequency Frequency Frequency</td>
<td>Frequency Frequency Frequency Frequency Frequency</td>
<td>Frequency Frequency Frequency Frequency Frequency Frequency</td>
<td>Frequency Frequency Frequency Frequency Frequency</td>
<td>Frequency Frequency Frequency Frequency Frequency Frequency Frequency Frequency Frequency Frequency Frequency Frequency Frequency Frequency</td>
</tr>
<tr>
<td>0</td>
<td>4 0 4 0</td>
<td>0 0 0</td>
<td>0</td>
<td>0 0 0 0</td>
<td>404</td>
</tr>
<tr>
<td>0</td>
<td>2 0 2 0</td>
<td>0 0 0</td>
<td>0</td>
<td>0 0 8 0</td>
<td>67</td>
</tr>
<tr>
<td>0</td>
<td>2 0 2 0</td>
<td>0 0 0</td>
<td>0</td>
<td>0 0 8 0</td>
<td>8</td>
</tr>
<tr>
<td>0</td>
<td>0 0 0 0</td>
<td>0 0 0</td>
<td>0</td>
<td>0 0 12 0</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>0 0 4 0</td>
<td>0 0 0</td>
<td>0</td>
<td>0 0 58 0</td>
<td>58</td>
</tr>
<tr>
<td>0</td>
<td>13 0 6 0</td>
<td>0 0 0</td>
<td>0</td>
<td>0 0 549 0</td>
<td>549</td>
</tr>
</tbody>
</table>

### References

18. Dubois É, Heymans P, Mayer N, Matulévicsúr A. A systematic approach 
to define the domain of information system security risk management. 
In: Nurcan S, Salinesi C, Souveyet C, Ralých J. Intentional Perspectives 
19. Silva MM, de Gasmão APs, Poloto T, e Silva LC, Costa APCs. A multi-
dimensional approach to information security risk management using 
20. Wager KA, Wickham Lee F, Glaser JP. Managing Health Care Infor-
mation System: A Practical Approach for Health Care Executives. 
Hoboken: John Wiley & Sons; 2005.
mation Technology Systems. Recommendations of the National Institute of 
Standards and Technology, Gaithersburg: Booz Allen Hamilton Inc. 2002.
22. Nikpajah A, Karimi AA. Health Promotion in Hospitals: Evidence 
and Quality Management. Tehran: Institute for modern Iranian Health 
23. Ministry of Health and Medical Education. Report of Use of Hospital 
Information Systems in Iran. Tehran: Ministry of Health and Medical 
24. Akhondzade R. Health system transformation project, an opportunity 
(In Persian).
25. Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. Security require-
ts and solutions in electronic health records: lessons learned from 
26. Fildes J. Stuxnet Virus Targets and Spread Revealed: BBC News; Febru-
Comput Fraud Secur. 2012;2012(10):8–11.
29. Wangen G. The role of malware in reported cyber espionage: a review 
of the impact and mechanism. Information. 2015;6(2):183–211.
30. GReAT. The ReGin Platform: Nation-State Ownage of GSM Networks. 
Moscow: Kaspersky Lab’s Global Research & Analysis Team (GReAT); 
2014.
Information Security Risk Management (First Edition). Geneva: Interna-
tional Organization for Standardization; 2008.
33. Caralli RA, Yousef MF, Young LR, Wilson WR. Introducing octave allegro: 
Improving the information security risk assessment process. Pittsburgh: 
Software Engineering Institute, Carnegie Mellon University, 
2010.
35. CLUSIF. MEHARI 2010 Processing Guide for Risk Analysis and 
Methodology for Information Systems Risk Analysis and Management. 
Madrid: Ministry of Finance and Public Administration-Technical Sec-
retariat, Information, Documentation and Publications Unit Publications 
Center, 2014.
37. Ferderal Office for Information Security B. Supplement to BSI-Standard 
100-3. Application of the Elementary Threats from the IT-Grundercht 
Catalogues for Performing Risk Analyses. Bonn: Ferderal Office for 
38. Communications Security Establishment Canada. editor. Overview: IT 
Canada: Communications Security Establishment Canada (CSEC); 
2012.
10. The Security Officers Management and Analysis Project (SOMAPorg); 
40. Casey T. Threat Agent Library Helps Identify Information Security 
41. Lund MS, Solhaug B, Stolen K. Model-Driven Risk Analysis: The CORAS 
42. ETSI. Telecommunications and Internet Converged Services and 
Protocols for Advanced Networking (TISPAN): Methods and pro-
tocols. Part 1: Method and Proforma for Threat, Risk, Vulnerability 
Analysis(TVRA). France: European Telecommunications Standards 
Institute (ETSI); 2006:1–100.
43. The Open Group. Open Group Standard. Risk Analysis (O-RA). Berk-
shire: The Open Group; 2013.
44. ANSSI. EBIOS 2010 – Expression of Needs and Identification of 
Available from: http://www.ssi.gouv.fr/uploads/2011/10/EBIOS-
1-GuideMethodologique-2010-01-25.pdf; French.
45. ISO. ISO/IEC 17799:2005. Information Technology – Security Tech-
niques – Code of Practice for Information Security Management. 
46. ISO. ISO 27799:2008(E). Health Informatics-Information Security 
Management in Health Using ISO/IEC 27002. Geneva: Interna-
tional Organization for Standardization; 2008.
47. Trilitanun S, Tongsrisomboon A. Risk analysis and security manage-
ment of IT information in hospital. Int J Comput Inform Technol. 
48. Mortaza MB. Risk management for health information security and 
49. Macedo FN. Models for assessing information security risk, MSc 
thesis, Instituto Superior Técnico da Universidade Técnica de Lisboa, 
2009.
50. Van Deursen N, Buchanan WJ, Duff A. Monitoring information security 
51. Shahri AB, Ismail Z. A tree model for identification of threats as 
the first stage of risk assessment in HIS. J Inform Secur. 2012; 
3(2):169.
52. Jansen A. The cyber security risk assessment maturity of hospitals, 
MSc thesis, Institute of Information and Computer Science, Utrecht 
University, 2014.
security risk assessment in healthcare: the experience of an Italian Pa-
diatric Hospital. Computational Intelligence, Communication Systems 
and Networks, 2009 CICSYN’09 First International Conference on. 
Indore: IEEE; 2009.
54. Temesgen DK. Analysis of The Health Information Security Manage-
ment Practices of Healthcare Organizations in Amhara Region, Ethiopia 
the Case of Felege Hiwot Regional Referral, MSc thesis, The School of 
Graduate Studies of Addis Ababa University, 2011.
55. Technical Department of European Network and information Security 
Agency (ENISA), Section Risk Management. Risk Management: 
Implementation Principles and Inventories for Risk Management/ 
Risk Assessment Methods and Tools. Greece: Technical Department of 
European Network and information Security Agency (ENISA), Section 
Risk Management; 2006.
56. Kouns J, Minoli D. Information Technology Risk Management in 
57. Pandey SK, Mustafa K. A comparative study of risk assessment 
58. Razavi H, Mohaghegh M, EmamiRazavi S. Hospital Accreditation 
(In Persian).


