A New Model for Information Security Risk Management

Ali Shirazi and Mozaffar Kazemi

Abstract This article introduces a new risk management method for information security risk management, proposed and applied for the first time in the IT department of a telecommunication company in Iran. According to law requirements and security strategic plan, the mentioned company implemented information security risk management (ISMS). So one of the main phases of ISMS is the risk management. The results show that the methodology of the information security risk management containing the risk identification, risk analysis, risk evaluation and risk treatment, uses the frameworks of ISO 27005, ISO 27002, ISO 27011, OCTAVE and NIST 800-30 and OWASP standards. This new method is practical and accurate and is suitable for large scale organizations.

Keywords Information security · Risk assessment model · Security risk management · Risk management in ISMS

1 Introduction

In a large scale organization, risk assessment, risk analysis and risk treatment should be conducted in more than one phase. These phases can be defined in accordance with organizational processes or chart. In this case, the organization as a whole is divided into four parts. The criterion met in this division is the good match of organizational processes with organizational chart. One of these parts is the Department of Information Technology. Considering the legal requirements (AFTA document), senior management requirements (in the forms of project-based security strategy and ISO 27001 standard) as well as lack of knowledge about information security risk and insecurity and absence of a plan for risk management, there is need for a systematic information risk management to be implemented in the organization. In this

A. Shirazi (✉)
IT Management Department, Tarbiyat Modares University, Tehran, Iran
e-mail: shirazi@parsasharif.ir

M. Kazemi
Parsa-Sharif Research Center, Tehran, Iran

Y. Baghdadi et al. (eds.), *ICT for an Inclusive World*,
Lecture Notes in Information Systems and Organisation 35,
https://doi.org/10.1007/978-3-030-34269-2_38

research, a new method for information security risk management was introduced. Identification and valuation of assets, recognition of vulnerabilities and threats, and important risk scenarios which are the significant inputs of the risk treatment plan (RTP) process are the main outputs of the proposed method.

2 A Review of Literature

2.1 Information Security and Objectives

Information security is related to providing a secure condition, in which only those with the right of having access to the information can be able to read, hear, change, and broadcast it [1]. Thus, its major objective in an organization is maintaining confidentiality, integrity, and availability of information [2].

2.2 Definition of Risk

A risk is defined as the potential of the probable occurrence of an undesired event and its outcomes [3], through which an asset or a group of assets will be threatened to undergo a loss or damage due to their vulnerabilities [4]. An asset is any valuable thing to be protected in an organization [5].

There are 3 conditions known as risk factors (contextual problems) that can cause a risk: existence of a threat (hazard), an asset being exposed to the threat, and the asset's vulnerability [6]. A threat can be caused by a natural or man-made event incorporating potential individuals, entities, or actions to produce a disturbance in the information, environment, operations, and/or properties [2, 7]. There are 3 types of threat namely: deliberate, accidental, and environmental (natural) threats, which may lead to a damage or loss of crucial services [5]. Threatening actions can be intentionally undertaken by a capable adversary to jeopardize the interests of an organization [2]. The issue of information security exposure might be related to a system configuration, software mistake, or some reasonable security policies that allow an attacker to enter a system or network and find an access to information [8]. Vulnerability is the combination of a facility's attractiveness and the deterrence level of an existing countermeasure [9].

2.3 Risk Management Concept and Its Steps

Risk management helps an organization to meet its objectives of planning, decision-making, and performing productive activities by allocating resources [10]. Risk management deals with uncertainties, including the probable occurrence of harmful events and their resulting consequences in an organization, thus differing from other management activities [10].

Risk assessment and analysis are the two major activities of risk management [2, 11]. The former involves risk identification, characterization, and realization by studying, analyzing, and describing the probable outcomes for an effort [7, 12], while further identification of security risks and their magnitudes as well as the corresponding areas to be safeguarded are associated with the latter [4]. To reduce the risk level or eliminate it, countermeasures prove to be helpful as the most crucial steps in the establishment of ISMS. To address threats at all informational infrastructure layers, an effective overall security solution may be formulated by establishing security countermeasures [13]. Depending on the existing threats and exploitable vulnerabilities in computer and information systems, various information security mechanisms are selected [14].

Aimed at avoiding intrinsic damages to the risk factor or using organizational advantages, risk treatment selects and applies the most suitable risk security measures to modify it [12, 15]. Risk avoidance, acceptance, transference, and treatment are the 4 outstanding risk treatment strategies commonly utilized [2, 11]. In their method of selecting both technical and non-technical countermeasures, Kim and Lee (2005) considered the value of information, level of threat, and scope of security services [13].

2.4 Methods of Risk Management and Their Objectives

Several methodologies have been recognized for risk management [16]:

- Some have been issued by national and international organizations (ISO/IEC TR 13335, 1998; NIST SP800-30, 2002; AS/NZS 4360, 2004; HB231, 2004; BSI Standard 100-3, 2005; ISO/IEC 27005, 2008).
- Some others have been proposed by professional organizations (CRAMM, 2001; CORAS, 2003; OCTAVE, 2005; Magerit, 2006; Microsoft, 2006; Mehari, 2007).
- The other methodologies not accounted for by the first two procedures have been introduced by research projects (Kailay and Jarratt 1995; Smith and Eloff 2002; Robert and Rolf 2003; Karabacak and Sogukpinar 2005; Hoffanvik and Stolen 2006; Mayer et al. 2007).

All the above-mentioned approaches follow the common goals of prioritizing and estimating the risk value and suggesting the most proper plan to eliminate that risk or minimize it to an acceptable level [17]. Within a given organizational context, a risk management chooses its method based on its ability to appropriately understand and apply that method, the case which is difficult for the small-scale organizations due to the fact that they are constrained by resources and expertise [2]. ISO 27005 framework was selected by comparing it with those of some enterprises with general

Table 1 Comparison of information security risk management framework

Framework	Description	Target organization	Target level organization
ISO 27005	Complete process in generic manner	Governments, large companies, SME	Management, operational
OCTAVE	Self-directed approach	SME	Management, operational
NIST SP 800-53	Very detailed guidance and identifications	Governments, large companies, SME	Management, operational

information security risk management like NIST SP 800-30, Octave, and ISO 27005. The results of the comparison are shown in Table 1 as follows [18]:

The process of information security risk management can be applied to the whole or part of an organization, or any information system together with its existing aspects, or certain planned controls [5]. A summary of the mentioned process is displayed in Fig. 1 [5].

Establishment of the context: The context of this kind of risk management should be established to determine its necessary basic criteria, define its scope and boundaries, and appropriately organize its activities.

Risk assessment: This involves managers' qualitative risk measurement or description for a risk prioritization based on the seriousness perceived or other established criteria. Activities of risk analysis incorporating risk identification, estimation and evaluation will be plausible through risk assessment.

Risk treatment: The risk is selected to be reduced, maintained, avoided, or transferred and the plans are set accordingly. Based on the results of risk assessment and the expected costs and benefits, risk management options are selected and implemented.

Risk acceptance: This indicates an officially recorded decision to accept the risk and its responsibility.

Risk communication: This involves the activities between decision makers and other stakeholders to reach an agreement on how a risk management should be conducted by exchanging and/or sharing information about the risk.

Risk monitoring and reviewing: Risk is not static since threats, vulnerabilities, probabilities, and consequences can suddenly change with no signs. Therefore, a constant monitoring powered by an external service of providing information about new threats or vulnerabilities is required to detect these changes.

2.5 Qualitative and Quantitative Approaches of Risk Management

Based on the risk analysis and assessment applied, risk management follows a quantitative or qualitative method [19]. Detailed academic studies usually plunge into specific areas in an attempt to propose an effective solution to a specified problem

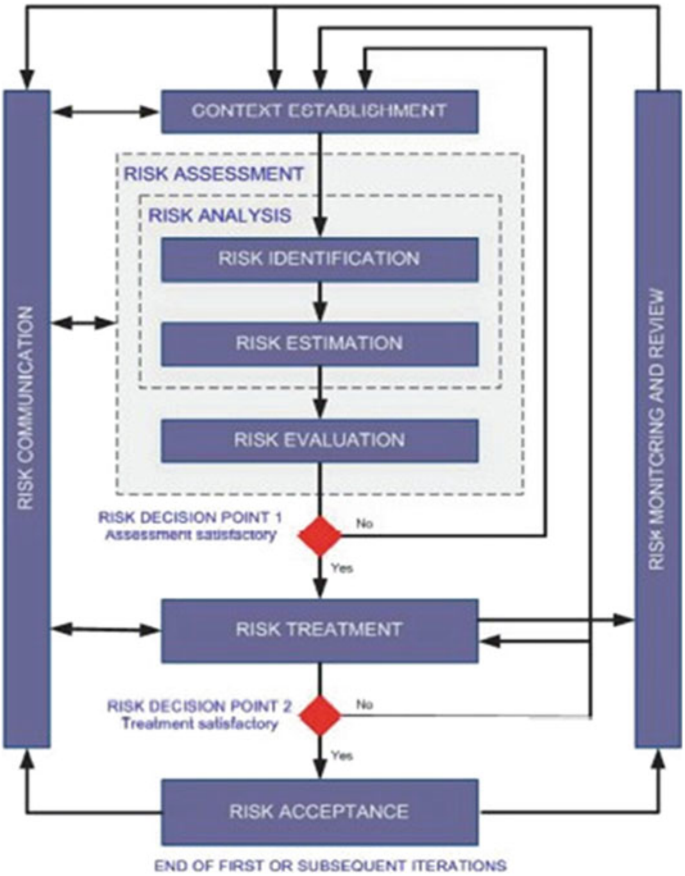


Fig. 1 Information security risk management process of ISO 27005

in the process of information security risk analysis through a number of quantitative methods. Yet, simpler and more generic and collaborative approaches are needed for public organizations [20]. Information security risk management is mostly based on the quantitative methodologies employed by financial institutions and insurance companies [2, 21]. Annualized Loss Expectancy (ALE) and Livermore Risk Analysis Methodology (LRAM) are among the popular examples of quantitative methods of risk analysis and assessment [2, 7] that use numerical results to express the probability of each risk factor and its effects on organizational objectives [19]. Therefore, the infrastructures of large information systems supported by reinforced human and financial resources are properly in need of quantitative methods [22], the objectivities of which are capitalized based on mathematical formulae that can be readily verified [2]. These methods depend on the estimations of probable damages to assets or loss of information systems [2, 23]. Rot [24] argues that generally more costs, greater

Table 2 Qualitative risk metrics

	Likelihood		
Consequences	Low	Medium	Low
High	M	H	H
Medium	L	M	H
Low	L	L	M
Key: H: high risk M: medium risk L: low risk			

experiences, and more advanced tools are involved in a quantitative method when compared with a qualitative method exercised for a risk management [25].

On the other hand, to make a decision on how to solve the potential risk factors, qualitative risk management is required to assess their identified effects on the assets of the information systems and create priorities [19]. Any available expertise in an organization can modify the qualitative methods for easy uses [22]. Due to their simplicity for using the very familiar 'jargon' for non-technical people, less time, finance, and effort are needed since risks can be expressed based on descriptive variables instead of accurate monetary terms [2]. They are further based on the risk management exercise conducted by the judgment, intuition and experience of an individual [21]. However, due to some complexities, serious problems are posed by some identified techniques of qualitative risk assessment and analysis. For instance, a highly trained technical team and strong financial basis are required to carry out risk assessment and analysis using Hazard and Operability study (HAZOP), Failure Mode and Effects Analysis (FMEA) or Failure Mode and Effects Criticality Analysis (FMECA), the Central Computer and Telecommunications Agency, and CCTA-Risk Analysis and Management Method (CRAMM), which are thus labor-intensive [25]. Of course, highly technical people or robust financial supports are not always needed for the techniques of qualitative risk assessment and analysis. For example, as any other easy, cheap, and viable methods, the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) technique is conducted to achieve the same objectives [26]. OCTAVE as a most appropriate approach in organizations with no experts of information risk management is from among the common examples cited for qualitative risk management [22, 27]. An example of a qualitative risk metrics is shown in Table 2 [14].

2.6 Problems of Risk Management Approaches

Due to the lack of awareness, high cost, need of expertise, and long process, the present risk management methods have been demonstrated by various reports, surveys, and relevant literature not to be widely used within organizations so far despite the increasing number of standard and commercial ones [28].

Regarding the poor results, bulky confusing reports, and narrow technological scopes, these methods are less relied upon [29].

Any organizations willing to adopt one of these methods are confused by their huge numbers (more than 200 methods at present) while no agreeable benchmarks or comparative frameworks can be referred to for the evaluation of information security risks of enterprises and thus they are less practical [30].

As noted by Solms [31], information security is not a technical matter, but a social, business, and regulatory issue" protecting all the elements of an information system, including hardware, software, information, people, and processes [2]. These traditional methods focused generally on the technology and are used to manage risks and propose technical solutions to them within enterprises. Human, organizational, strategic, and environmental factors are seldom considered by most of them. Technology is not the only element to be recognized in this process, though it is a necessary consideration [32]. In an IT-based approach to security risk analysis, it is not so much necessary for business users to identify a comprehensive set of risks or promote security awareness throughout an organization [33]. A practical business continuity risk analysis should be adopted and applied to the business as a whole in a consistent, manageable, and cost-effective manner and not just to the IT department [34]. Some shortcomings of the traditional risk management approaches can be minimized via a holistic risk management method of information security as has been recently suggested by many authors [29, 35–37]. Small-scale organizations may surrender to unsanctioned methods or avoid practicing a complete risk management since its techniques are too difficult to understand [2, 26].

3 Theoretical Framework

Based on literature review, the theoretical framework for this research was conducted as shown in Fig. 2. Figure 2 illustrates the planning process of information security risk management by which the IT Department is influenced.

Figure 3 shows the process of information security risk management.

3.1 Context Establishment

Risk evaluation criteria: In this research, risk evaluation criteria are the impacts of losses of information confidentiality, integrity and availability (CIA) on the business.

Impact criteria: In this research, the impact of losses of CIA was examined in three dimensions of loss of financial value, service disruption and loss of image of the organization.

Risk Acceptance Criteria: in this research, risk acceptance criteria are based on comparison of impact of the security incident and cost of preventing that incident.

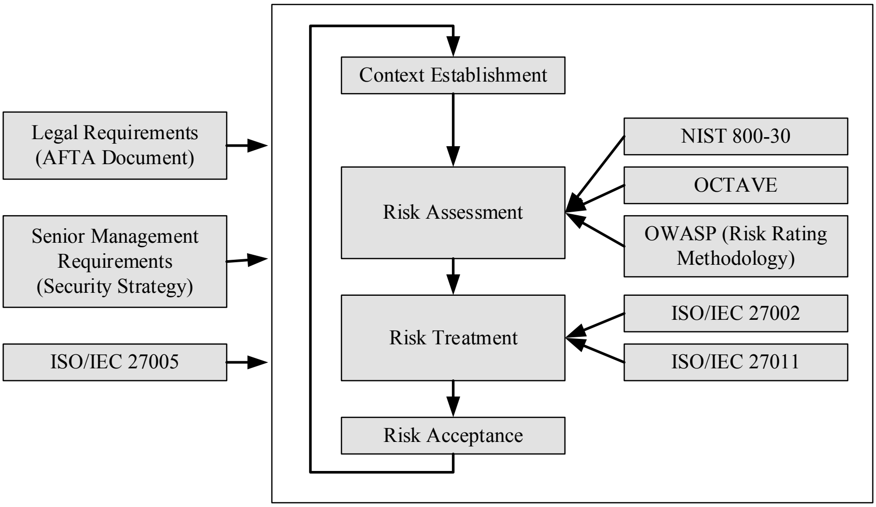


Fig. 2 Theoretical framework

Scope and boundaries: This research focused on the IT department because it is responsible for the storage, processing and transmitting of organization information.

Organization for information security risk management: In this research, the security department is responsible for the information security risk management process.

3.2 Information Security Risk Assessment

A. **Risk identification**

Risk identification includes three steps which are described as follow:

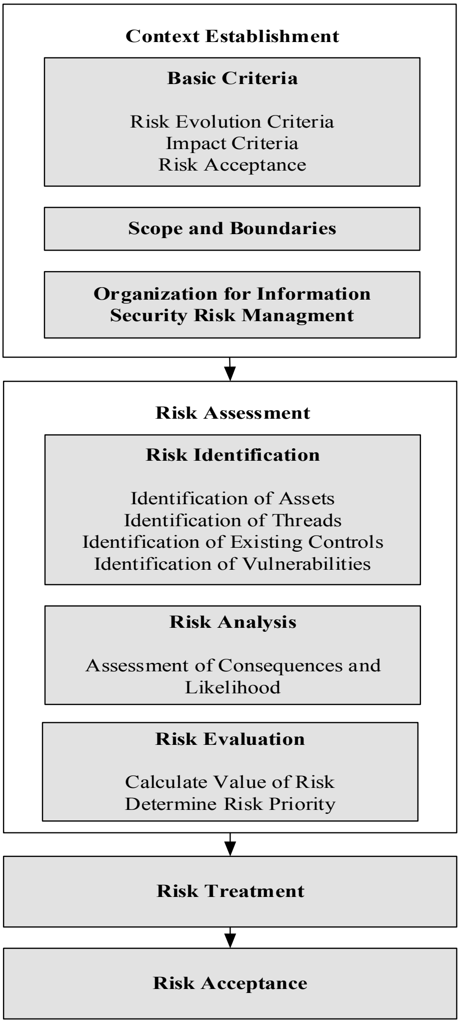
1. Identification of assets: Identification of the assets of IT department, identification of owner and location of asset.

There are 4 main types of asset in this research:

- Information assets
- Assets that are carriers of information assets
- Infrastructure devices
- Intangible assets.

2. Identification of threats: Identification of the threat of every asset and the origin of the threat. There are 38 kinds of threats that can affect risks.
3. Identification of existing control: It is used to ensure that the controls are working correctly and avoid dispensable work or cost.

Fig. 3 Information security risk management planning process



This identification is checked with the relevant personnel of the IT department and with the onsite review for the physical controls.

4. Identification of vulnerability: After identification of threats and existing controls on any asset, the vulnerabilities that may occur in them are identified. Vulnerabilities are identified by interviewing relevant staff, observations and using technical tools such as Nessus. Vulnerability may occur due to the lack of control or an existing control that cannot manage or reduce the threat that occurred. Types of identified vulnerabilities are listed as follow:

   - Organization;
   - Human resource;

- Network;
- Hardware;
- Software;
- Sites.

B. **Risk Analysis**

1. Assessment of consequences: In this research, the assigned value to the assets is the consequences of an incident scenario. An incident scenario is defined as description of a threat exploiting a certain vulnerability or set of vulnerabilities in an information security incident [5]. The impact criteria of the context establishment activity are considered to determine the impact of these scenarios [5]. Value of each asset is determined based on the impact of loss of CIA and it is examined in three dimensions of loss of financial value, service disruption and loss of image of the organization (Table 3).

When we want calculate value of an asset, we should sum impact of loss of CIA of each asset in three dimension. For example, based on Table 3, if "Loss of financial value: Between X to Y dollars (5)", "Service disruption: between B to C minutes per year (5)" and "Loss of image of organization: at the national level (10)" then "Asset value = 5 + 5 + 10 = 20". So value of an asset can be 0 in minimum and 30 in maximum.

Then, because we use the value of the asset that is involved in an information security scenario for assessment of the consequences of that information security incident scenario, we can use Table 4.

For example, if value of an asset is 20, the consequences of the information security incident scenario that this asset is involve in, is High (=3).

Table 3 Impact of loss of CIA of each asset in three dimension

Dimension	Impact			
	0	1	5	10
Loss of financial value	Effect less	Less than X dollar	Between X to Y dollar	More than Y dollar
Service disruption	Less than A minutes per year	Between A to B minutes per year	Between B to C minutes per year	More than C minutes per year
Loss of image of organization	Effect less	At the organization level	At the customers level	At the national level

Table 4 Consequences of each information security incident scenario based on the value of the involved asset

Asset value	0	1–7	8–15	16–23	24–30
Consequence	Not important (=0)	Low (=1)	Medium (=2)	High (=3)	Very high (=4)

Table 5 Threat likelihood scale

Event recapitulation	Likelihood	Value[a]
More than 3 times a year	High	3
2 or 3 times a year	Medium	2
Maximum once a year	Low	1
This threat is not applicable	Not applicable	0

[a] In order to evaluate the likelihood of each threat easily, we assigned the value of 0–3 to them

2. Assessment of incident likelihood: In this research, two parameters of likelihood of threat and level of vulnerabilities form the likelihood of the incident scenarios. The previous experience of the events recapitulated in the IT department and interviews with relevant staff are the bases for assessment of each threat likelihood (Table 5).

Level of each vulnerability, is identified based on vulnerability factors, according to the Table 6.

Based on sum of numerical values assigned to each vulnerability, according to Table 6, we can categorize each vulnerability in one of the three categories below:

- Low: between 4 and 12,
- Medium: between 13 and 25, and
- High: between 26 and 36.

Table 7 gives an example for each level.

Table 6 Level of each vulnerability

Vulnerability factors	Description	Options
Ease of discovery	How easy is it for this group of threat agents to discover this vulnerability?	Practically impossible (=1), difficult (=3), easy (=7), automated tools available (=9)
Ease of exploit	How easy is it for this group of threat agents to actually exploit this vulnerability?	Theoretical (=1), difficult (=3), easy (=7), automated tools available (=9)
Awareness	How well known is this vulnerability to this group of threat agents?	Unknown (=1), hidden (=3), obvious (=7), public knowledge (=9)
Intrusion detection	How likely is an exploit to be detected?	Active detection in application (=1), logged and reviewed (=3), logged without review (=7), not logged (=9)

Table 7 Level of vulnerability

Vulnerability factors				Level of vulnerability
Ease of discovery	Ease of exploit	Awareness	Intrusion detection	
Practically impossible (=1)	Theoretical (=1)	Unknown (=1)	Active detection in application (=1)	Low (1 + 1 + 1 + 1 = 4)
Difficult (=3)	Difficult (=3)	Hidden (=3)	Logged without review (=7)	Medium (3 + 3 + 3 + 7 = 16)
Automated tools available (=9)	Automated tools available (=9)	Public knowledge (=9)	Not logged (=9)	High (9 + 9 + 9 + 9 = 36)

As mentioned before, the likelihood of the incident scenarios is the combination of two parameters: likelihood of threat and level of vulnerabilities. In this research, Table 8 was used to determine the likelihood of each incident scenarios:

C. **Risk Evolution**

In this research, calculation of value of risk is based on NIST SP 800-30 and ISO/IEC 27005, which have risk matrix as shown in Table 9 and below risk formula:

$$\text{Risk Value} = \text{Consequence} \times \text{Incident Likelihood}$$

Based on the results of calculation of risk values in Table 9, the risk priority is listed in four categories from the highest risk to lowest as shown in Table 10.

3.3 Risk Treatment

Identification of Risk Treatment: The risk treatment has four options: reduction, acceptance, avoidance and transfer [5]:

- Reduction: Appropriate and justified controls should be selected to meet the requirements identified by the risk assessment and risk treatment. This selection should take account of the risk acceptance criteria as well as legal, regulatory and contractual requirements. This selection should also take account of cost and timeframe for implementation of controls, or technical, environmental and cultural aspects. It is often possible to lower the total cost of ownership of a system with properly selected information security controls.
- Acceptance: If the level of risk meets the risk acceptance criteria, there is no need for implementing additional controls and the risk can be retained.
- Avoidance: When the identified risks are considered too high, or the costs of implementing other risk treatment options exceed the benefits, a decision may be made to avoid the risk completely, by withdrawing from a planned or existing activity or set of activities, or changing the conditions under which the activity is

Table 8 Likelihood of incident scenarios

Likelihood of threat	Not applicable (=0)			Low (=1)			Medium (=2)			High (=3)		
Level of vulnerability	Low (4–12)	Medium (13–25)	High (26–36)	Low (4–12)	Medium (13–25)	High (26–36)	Low (4–12)	Medium (13–25)	High (26–36)	Low (4–12)	Medium (13–25)	High (26–36)
Incident likelihood	1	2	3	2	3	4	3	4	5	4	5	6

Table 9 Value of risk

Incident likelihood (Table 8)	Consequence (Table 4)			
	Low (1)	Medium (2)	High (3)	Very high (4)
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16
5	5	10	15	20
6	6	12	18	24

Table 10 Risk priority

Risk Score	Priority
1–5	Low
6–10	Medium
11–17	High
18–24	Very high

operated. For example, for risks caused by nature it may be most cost effective alternative to physically move the information processing facilities to a place where the risk does not exist or is under control.

- Transfer: Risk sharing involves a decision to share certain risks with external parties. Sharing can be done by insurance that will support the consequences, or by sub-contracting a partner whose role will be to monitor the information system and take immediate actions to stop an attack before it makes a defined level of damage.

For the sake of confidentiality agreements RTP is not presented.

4 Conclusion

The information security risk management method which is appropriate for IT Department of the telecommunication operator in Iran, covers the items listed below:

1. Context establishment based on ISO/IEC 27005, legal requirements (AFTA Document) and Senior Management Requirements (Security Strategy) includes definitions of risk evaluation criteria, the criteria of impact, risk acceptance criteria and organizational information security risk management.
2. Risk identification is done by identifying the assets, identification of threats which can cause harm to assets, identification of existing controls and the identification of vulnerabilities.

3. Risk estimation is accomplished by identifying the level of consequences and likelihood of risk level. Information security risk scenarios are divided into four levels: low, medium, high and very high.
4. Risk evaluation is done by calculating values of risk matrix and prioritizing the risks based on risk values from the highest to the lowest.
5. Risk treatment consists of four options: acceptance, reduction, avoidance and transfer. In order to reduce the risk the recommendations in accordance with ISO guidelines 27002 and 27011 are applied.

References

1. Elky, S.: An Introduction to Information System Risk (2006)
2. Karabacak, B., Sogukpinar, I.: ISRAM: information security risk analysis method. Comput. Secur. **24**(2), 147–159 (2005)
3. Dorian, L.: Risk Management: Understanding Industry Insights. http://www.ica.bc.ca/ii/ii.php?catid=17
4. Chen, M.T.: Information security and risk management. In: Encyclopedia of Multimedia Technology and Networking, 2nd edn. (2009)
5. International Standard Organization. ISO/IEC 27005:2008—Information Technology—Security Techniques—Information Security Risk Management. Switzerland (2008)
6. Siu, T. Information Security Risk management. http://wiki.edu/information_security_risk_kanagementOverarching_themes (2011)
7. Pare, G., Sicotte, C., Jaana, M., Girouard, D., Paré, G., Ph, D.: Prioritizing clinical information system project risk factors: A delphi study. Methods Inf. Med. **47**(3), 251–259 (2008)
8. Rainer, R.K., Snyder, C.A., Carr, H.H.: Risk analysis for information technology. J. Manag. Inf. Syst. **8**(1), 129–147 (1991)
9. Tiwari, A.: Information Security Risk Management: An Overview Risk Management: An Essential Guide to Protecting Critical Assets. http://www.suite101.com/profile.cfm (2010)
10. Renfroe, N.A., Smith, J.L.: Threat/Vulnerability Assessments and Risk Analysis. http://www.wbdg.org/resources/riskanalysis.php#top
11. Ciechanowicz, Z.: Risk analysis: requirements, conflicts and problems. Comput. Secur. **16**(3), 223–232 (1997)
12. Hicks, J., Craig, L., Shortreed, J.: Basic Frameworks for Risk Management. http://www.irrneram.ca/pdf_files/basicFrameworkMar2003.pdf (2003)
13. Kim, T.: Design procedure of IT systems security countermeasures. In: International Conference on Computational Science and Its Applications (ICCSA), pp. 468–473 (2005)
14. Beachboard, J., Cole, A., Mellor, M., Hernandez, S., Aytes, K., Massad, N.: Improving information security risk analysis practices for small- and medium-sized enterprises: a research agenda. J. Issues Informing Sci. Inf. Technol. **5**, 73–85 (2008)
15. Sosonkin, M.: OCTAVE: Operationally Critical Threat, Asset and Vulnerability Evaluation. http://isis.poly.edu/courses/cs996-management-s2005/Lectures/octave.pdf (2005)
16. Saleh, M.S., Alfantookh, A.: A new comprehensive framework for enterprise information security risk management. Appl. Comput. Inform **9**(2), 107–118 (2011)
17. Vorster, A., Labuschagne, L.: A framework for comparing different information security risk analysis methodologies. Inf. Secur. **193**(C), 95–103 (2005)
18. The European Union Agency for Network and Information Security (ENISA). Available: http://IIrm-inv.enisa.europa.euIcomparison.html
19. Mazareanu, V.: Risk Management and Analysis: Risk Assessment Qualitative and Quantitative. http://papers.ssrn.com/sol13/papers.cfm?abstractid=1549186 (2007)

20. Tong, C.K., Fung, K., Huang, H.Y., Chan, K.: Implementation of ISO17799 and BS7799 in picture archiving and communication system: local experience in implementation of BS7799 standard. Int. Congr. Ser. **1256**, 311–318 (2003)
21. Lo, C.C., Chen, W.J.: A hybrid information security risk assessment procedure considering interdependences between controls. Expert Syst. Appl. **39**(1), 247–257 (2012)
22. Panda, P. The OCTAVE approach to information security risk assessment. http://www.isaca.org.Journal/past-issues/2009/volume4/documents/jpdf09-OCTAVE.pdf (2009)
23. Ding, T.: Quantitative Risk Analysis Step-by-step. GSEC Practical Version. http://www.sans.org/reading_room/whitepapers/auditing/quantitative-risk-analysis-step-by-step_849 (2002)
24. Yeh, Q.J., Chang, A.J.T.: Threats and countermeasures for information system security: a cross-industry study. Inf. Manag. **44**(5), 480–491 (2007)
25. Rot, A.: IT Risk Assessment: Quantitative and Qualitative Approach. In Proceedings of the World Congress on Engineering and Computer Science (WCECS), pp. 22–24. San Francisco (SANS) (2008)
26. Alberts, C., Dorofee, A.: Managing Information Security Risks: The {OCTAVE} Approach. Addison-Wesley Anderson, Boston (2002)
27. Alberts, C., Dorofee, A.: An introduction to OCTAVE SM Method. http://www.cert.org/octave/methodintro.htm/#intro (2001)
28. N.C.C. (NCC).: The Business Information Security: 2000 Survey. National Computing Center, UK (2000)
29. Spears, J.L.: A holistic risk analysis method for identifying information security risks. pp. 185–202 (2006)
30. Syalim, A.: Comparison of risk analysis methods : Mehari, Magerit, NIST800–30 and microsoft's security management guide. In: 2009 International Conference on Availability, Reliability and Security, pp. 726–731 (2009)
31. von Solms, B.: The 10 deadly sins of information security management. Comput. Secur. **23**(5), 371–376 (2004)
32. Werlinger, R., Hawkey, K., Beznosov, K.: An integrated view of human, organizational, and technological challenges of IT security management. Inf. Manag Comput. Secur. **17**(1), 4–19 (2009)
33. Lategan, N., von Solms, R.: Towards enterprise information risk management—a body analogy. Comput. Fraud Secur **2006**(12), 15–19 (2006)
34. Nosworthy, J.D.: A practical risk analysis approach: managing BCM risk. Comput. Secur. **19**(7), 596–614 (2000)
35. Zuccato, A.: Holistic security management framework applied in electronic commerce. Comput. Secur. **26**(3), 256–265 (2007)
36. Anderson, K.: Convergence: A holistic approach to risk management. Netw. Secur. **2007**(5), 4–7 (2007)
37. Huang, J.-W., Ding, Y.-S., Hu, Z.-H.: Knowledge based model for holistic information security risk analysis. In: 2008 International Symposium on Computer Science and Computational Technology. vol. 1 (2008)