

Information Security Risk Analysis - ISO/IEC 27005:2008 International Standard

Prof. Dr Milan Marković

Faculty of Electrical Engineering, University of Banja Luka

Content

- Introduction
- Scope of ISO/IEC 27005:2008
- Structure of the Standard
- Proposed method to Information Security Risk Management
- Conclusion

Introduction

- This International Standard provides guidelines for Information Security Risk Management in an organization, supporting in particular the requirements of an ISMS (Information Security Management System) according to ISO/IEC 27001:2005 standard.
- However, this International Standard does not provide any specific methodology for information security risk management.
- A number of existing methodologies can be used under the framework described in this International Standard to implement the requirements of an ISMS.
- This first edition of ISO/IEC 27005 cancels and replaces ISO/IEC TR 13335-3:1998, and ISO/IEC TR 13335-4:2000, of which it constitutes a technical revision.

Scope of the Standard

- This International Standard provides guidelines for information security risk management.
- This International Standard supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.
- Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this International Standard.
- This International Standard is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.

Structure of the Standard

- This standard contains the description of the information security risk management process and its activities.
- The background information is provided in Clause 5.
- A general overview of the information security risk management process is given in Clause 6.
- All information security risk management activities as presented in Clause 6 are subsequently described in the following clauses:
 - Context establishment in Clause 7,
 - Risk assessment in Clause 8,
 - Risk treatment in Clause 9,
 - Risk acceptance in Clause 10,
 - Risk communication in Clause 11,
 - Risk monitoring and review in Clause 12.

Structure of the Standard

- Additional information for information security risk management activities is presented in the annexes.
- The context establishment is supported by Annex A (Defining the scope and boundaries of the information security risk management process).
- Identification and valuation of assets and impact assessments are discussed in Annex B (examples for assets),
- Annex C (examples of typical threats) and Annex D (examples of typical vulnerabilities).
- Examples of information security risk assessment approaches are presented in Annex E.
- Constraints for risk reduction are presented in Annex F.

Structure of the Standard

- All risk management activities as presented from Clause 7 to Clause 12 are structured as follows:
 - Input: Identifies any required information to perform the activity.
 - Action: Describes the activity.
 - Implementation guidance: Provides guidance on performing the action. Some of this guidance may not be suitable in all cases and so other ways of performing the action may be more appropriate.
 - Output: Identifies any information derived after performing the activity.

Overview of the Information security risk management process

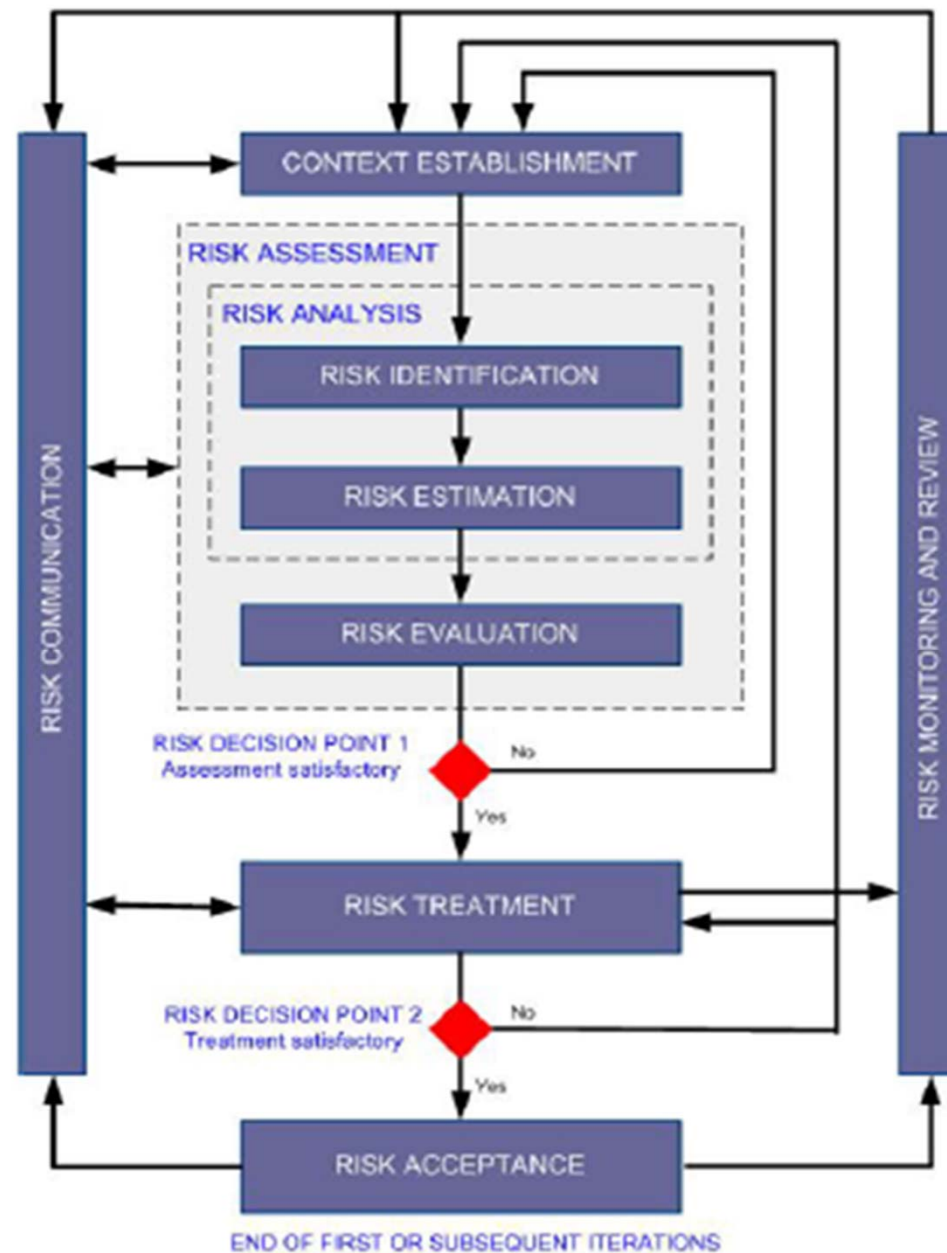


Figure 1 — Information security risk management process

Overview of the Information security risk management process

- In an ISMS, establishing the context, risk assessment, developing risk treatment plan and risk acceptance are all part of the “plan” phase.
- In the “do” phase of the ISMS, the actions and controls required to reduce the risk to an acceptable level are implemented according to the risk treatment plan.
- In the “check” phase of the ISMS, managers will determine the need for revisions of the risk assessment and risk treatment in the light of incidents and changes in circumstances.
- In the “act” phase, any actions required, including additional application of the information security risk management process, are performed.

Overview of the Information security risk management process

Table 1 — Alignment of ISMS and Information Security Risk Management Process

ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Developing risk treatment plan Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process

7 Context establishment

- 7.1 General considerations
- 7.2 Basic criteria
- 7.3 The scope and boundaries
- 7.4 Organization for Information security risk management

8 Information security risk assessment

- A risk is a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event.
- Risk assessment quantifies or qualitatively describes the risk and enables managers to prioritize risks according to their perceived seriousness or other established criteria.
- Risk assessment consists of the following activities:
 - Risk analysis (Clause 8.2) which comprises:
 - Risk identification (Clause 8.2.1)
 - Risk estimation (Clause 8.2.2)
 - Risk evaluation (Clause 8.3)
- Risk assessment determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist (or could exist), identifies the existing controls and their effect on the risk identified, determines the potential consequences and finally prioritizes the derived risks and ranks them against the risk evaluation criteria set in the context establishment.

8 Information security risk assessment

- Risk assessment is often conducted in two (or more) iterations.
 - First a high level assessment is carried out to identify potentially high risks that warrant further assessment.
 - The next iteration can involve further in-depth consideration of potentially high risks revealed in the initial iteration.
- Where this provides insufficient information to assess the risk then further detailed analyses are conducted, probably on parts of the total scope, and possibly using a different method.
- It is up to the organization to select its own approach to risk assessment based on the objectives and the aim of the risk assessment.

8 Information security risk assessment

- 8.1 General description of Information security risk assessment
- 8.2 Risk analysis
 - 8.2.1 Risk identification
 - 8.2.1.1 Introduction to risk identification
 - 8.2.1.2 Identification of assets
 - 8.2.1.3 Identification of threats
 - 8.2.1.4 Identification of existing controls
 - 8.2.1.5 Identification of vulnerabilities
 - 8.2.1.6 Identification of consequences

8 Information security risk assessment

- 8.2.2 Risk estimation
 - 8.2.2.1 Risk estimation methodologies
 - 8.2.2.2 Assessment of consequences
 - 8.2.2.3 Assessment of incident likelihood
 - 8.2.2.4 Level of risk estimation
- 8.3 Risk evaluation

9 Information security risk treatment

- 9.1 General description of risk treatment
- 9.2 Risk reduction
- 9.3 Risk retention
- 9.4 Risk avoidance
- 9.5 Risk transfer

9 Information security risk treatment

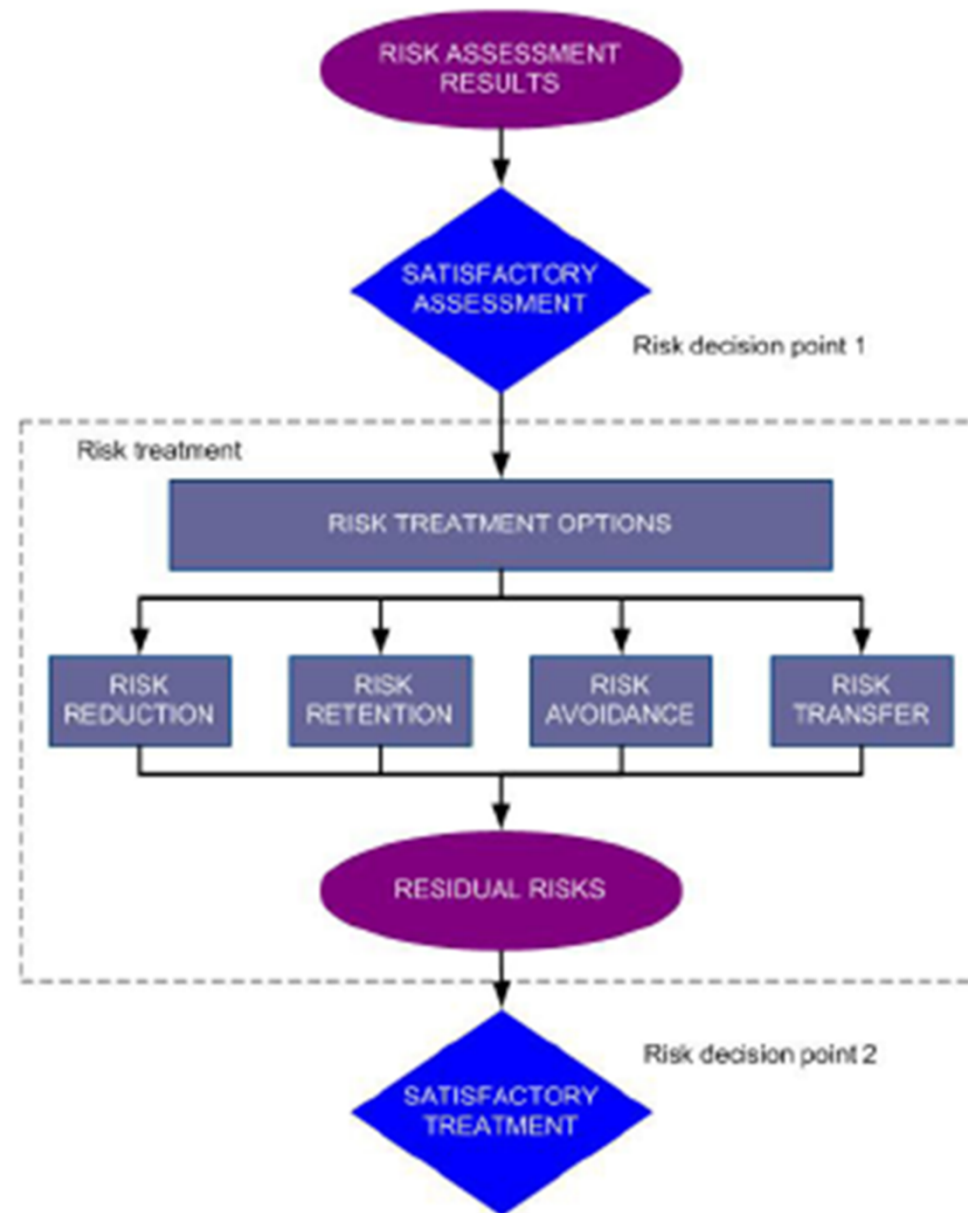


Figure 2 — The risk treatment activity

Further chapters of the Standard

- 10 Information security risk acceptance
- 11 Information security risk communication
- 12 Information security risk monitoring and review
 - 12.1 Monitoring and review of risk factors
 - 12.2 Risk management monitoring, reviewing and improving

Appendices

- Annex A (informative) Defining the scope and boundaries of the information security risk management process
- Annex B (informative) Identification and valuation of assets and impact assessment
- Annex C (informative) Examples of typical threats
- Annex D (informative) Vulnerabilities and methods for vulnerability assessment
- Annex E (informative) Information security risk assessment approaches
- Annex F (informative) Constraints for risk reduction

Proposed method - Risk assessment process

- Risk assessment process according to international standards ISO/IEC 27001:2005 and ISO/IEC 27005:2008 consists of following phases:
 - Identification and Valuation of Assets
 - Identification and Assessment of Threats and Vulnerabilities, as well as their combinations (security incidents)
 - Analysis and Identification of the impacts and influences on possible CIA losses which given security incidents could have on the particular asset
 - Probability estimation of the particular incident
 - Calculation of risk level
 - Selection of an appropriate option for risk treatment
 - Selection of controls in order to reduce risk to previously defined acceptable level
 - Creation of Risk Treatment Plan

Proposed method - Risk assessment process

- Security Risk Assessment in the Organization could be done in two types:
 - I type – an overall risk assessment on a level of the whole Organization and selection/definition of security controls that should be urgently implemented in order to reduce identified risks to the pre-defined acceptable level. Implementation of an overall ISMS (Information Security Management System). Considered assets are in fact categories/groups of assets according to which the overall risks are considered
 - II type – definition of the narrower scope of the ISMS which covers some appropriate and important segments of linked business processes in the Organization and realization of a detailed security risk assessment for the given scope and selection/definition of a detailed set of security controls that should be implemented in order to reduce identified risks to the acceptable level. Considered assets are individual assets from the scope.

Proposed method - Identification and valuation of assets

- One example of possible asset identification and valuation is given in the following Table:

Asset	Valuation			Calculation method			
	C	I	A	Highest	Sum	Multiplication	Average

Proposed method - Identification and valuation of assets

- Identified assets are evaluated for each of CIA parameters by values from 1 to 5, where 5 is the highest level.
- A total value of the asset is calculated as a multiple of the assessed values for each of the CIA parameters.
- A normalized asset value is used in the further risk level calculation. One possible way of normalized asset value calculation is given in the following Table:

Total asset value	Normalized asset value
1 – 24	1
25 – 49	2
50 – 74	3
75 – 99	4
100 – 125	5

Asset Categories in the Overall Risk Analysis

- Databases
- Data Rooms
- Information systems
- Authentication services
- Computer network
- Internet services
- Workstations
- Collaboration services
- User assets
- Human resources
- Offices
- Documentation

Proposed method - Vulnerabilities Identification

- Identified vulnerabilities could be grouped in following categories:
 - Missing of logical/technical controls
 - Missing of administrative controls
 - Missing of high-availability infrastructural system
 - Missing of security awareness for users
 - Missing of physical access control

Proposed method - Threat Identification

- The threats that are identified are the ones which are the most frequent and characteristic for areas of the Organization.
- Threats are grouped in three categories:
 - Natural disasters
 - Technological threats
 - Human threats

Proposed method - Identification and assessment of threats and vulnerabilities

- In a matrix below, joint impact levels of threats and vulnerabilities are given.
- Levels are estimated with L (Low), Medium (M) and H (High).
- In the matrix, joint impacts of threats and vulnerabilities on the asset itself are given, depending on normalized asset value.

	Vulnerability levels	L			M			H		
	Threats levels	L	M	H	L	M	H	L	M	H
Asset value	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

Measuring of security risks and incident ranking

1. Measure of an impact which given security incident has on relating assets, i.e. a measure of an possible regulation, financial and reputational consequences to the Organization by losses of CIA for the given assets (ranked from 1 to 10 where 10 is the biggest impact)
2. Probability that the incident will happen (from 1 to 5 where 5 is the biggest probability)
3. A risk measure is a multiple of 1 and 2
4. Group value of threats-vulnerabilities level from the previous table which is an average of all possible combination of threats and vulnerabilities leading to the given incident
5. A risk is calculated as a multiple of risk measure (3) and group value of threats-vulnerabilities level (4)
6. Risk ranking – according to highest risk value (5)

Conclusions

1. The Security Risk Assessment is the most important activity in the ISMS establishment in the Organization.
2. Already existing standards help but they do not specify an exact methodology for the security risk assessment.
3. The method for the security risk assessment is proposed.
4. Recommendation is that first an overall risk assessment should be done with whole organization as the scope and asset categories considered.
5. After the overall risk assessment is done (the overall ISMS established), apply detailed risk assessment to the most critical and sensitive business processes of the organization (often based on results of the overall ISMS establishment),

Thanks for your attention