ISO/IEC 27005:2018 (E)

Information technology — Security techniques — Information security risk management

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Structure of this document

5 Background

6 Overview of the information security risk management process

7 Context establishment

- 7.1 General considerations
- 7.2 Basic criteria
- 7.2.1 Risk management approach
- 7.2.2 Risk evaluation criteria
- 7.2.3 Impact criteria
- 7.2.4 Risk acceptance criteria
- 7.3 Scope and boundaries
- 7.4 Organization for information security risk management

8 Information security risk assessment

- 8.1 General description of information security risk assessment
- 8.2 Risk identification
- 8.2.1 Introduction to risk identification
- 8.2.2 Identification of assets
- 8.2.3 Identification of threats
- 8.2.4 Identification of existing controls
- 8.2.5 Identification of vulnerabilities
- 8.2.6 Identification of consequences
- 8.3 Risk analysis
- 8.3.1 Risk analysis methodologies
- 8.3.2 Assessment of consequences
- 8.3.3 Assessment of incident likelihood
- 8.3.4 Level of risk determination
- 8.4 Risk evaluation

9 Information security risk treatment

- 9.1 General description of risk treatment
- 9.2 Risk modification
- 9.3 Risk retention
- 9.4 Risk avoidance
- 9.5 Risk sharing

10 Information security risk acceptance

11 Information security risk communication and consultation

12 Information security risk monitoring and review

12.1 Monitoring and review of risk factors
12.2 Risk management monitoring, review and improvement

Annex A (informative) Defining the scope and boundaries of the information security risk management process

A.1 Study of the organization
A.2 List of the constraints affecting the organization
A.3 List of the constraints affecting the scope

Annex B (informative) Identification and valuation of assets and impact assessment

B.1 Examples of asset identification
B.1.1 General
B.1.2 The identification of primary assets
B.1.3 List and description of supporting assets
B.2 Asset valuation
B.2.1 General
B.2.2 Criteria
B.2.3 Reduction to the common base
B.2.4 Scale
B.2.5 Dependencies
B.2.6 Output
B.3 Impact assessment

Annex C (informative) Examples of typical threats

Annex D (informative) Vulnerabilities and methods for vulnerability assessment

D.1 Examples of vulnerabilities
D.2 Methods for assessment of technical vulnerabilities

Annex E (informative) Information security risk assessment approaches

E.1 High-level information security risk assessment
E.2 Detailed information security risk assessment
E.2.1 General
E.2.2 Example 1 Matrix with predefined values
E.2.3 Example 2 — Ranking of Threats by Measures of Risk
E.2.4 Example 3 — Assessing a value for the likelihood and the possible consequences of risks

Annex F (informative) Constraints for risk modification

Page count: 56