ISO/IEC TS 27008:2019 (E)

Information technology — Security techniques — Guidelines for the assessment of information security controls

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Structure of this document

5 Background

6 Overview of information security control assessments

6.1 Assessment process
6.1.1 General
6.1.2 Preliminary information
6.1.3 Assessment checklists
6.1.4 Review fieldwork
6.1.5 The analysis process
6.2 Resourcing and competence

7 Review methods

7.1 Overview
7.2 Process analysis
7.2.1 General
7.3 Examination techniques
7.3.1 General
7.3.2 Procedural controls
7.3.3 Technical controls
7.4 Testing an validation techniques
7.4.1 General
7.4.2 Blind testing
7.4.3 Double Blind Testing
7.4.4 Grey Box Testing
7.4.5 Double Grey Box Testing
7.4.6 Tandem Testing
7.4.7 Reversal
7.5 Sampling techniques
7.5.1 General
7.5.2 Representative sampling
7.5.3 Exhaustive sampling

8 Control assessment process

8.1 Preparations
8.2 Planning the assessment
8.2.1 Overview
8.2.2 Scoping the assessment
8.2.3 Review procedures
8.2.4 Object-related considerations
8.2.5 Previous findings
8.2.5.1 Overview

8.2.5.2 Changing conditions
8.2.5.3 Acceptability of reusing reviews.
8.2.5.4 Time aspects
8.2.6 Work assignments
8.2.7 External systems
8.2.8 Information assets and organization
8.2.9 Extended review procedure
8.2.10 Optimization
8.2.11 Finalization
8.3 Conduction reviews
8.4 Analysis and reporting results

Annex A (Informative) Initial information gathering (other than IT)

A.1 General
A.1.1 Human resources and security
A.1.2 Policies
A.1.3 Organization
A.2 Physical and environmental security
A.2.1 Are the sites safe for information?
A.2.2 Are the sites safe for ICT? (Environmental aspects)
A.2.3 Are the sites safe for people?
A.3 Incident management

Annex B (informative) Practice guide for technical security assessments

B.1 General
B.2 Assessment of controls from ISO/IEC 27002
B.2.1 ISO/IEC 27002:2013, Clause 5 Information security policies
B.2.2 ISO/IEC 27002:2013, Clause 6 Organization of information security
B.2.3 ISO/IEC 27002:2013, Clause 7 Human resource security
B.2.4 ISO/IEC 27002:2013, Clause 8 Asset management
B.2.5 ISO/IEC 27002:2013, Clause 9 Access control
B.2.6 ISO/IEC 27002:2013, Clause 10 Cryptography
B.2.7 ISO/IEC 27002:2013, Clause 11 Physical and environmental security
B.2.8 ISO/IEC 27002:2013, Clause 12 Operations security
B.2.9 ISO/IEC 27002:2013, Clause 13 Communications security
B.2.10 ISO/IEC 27002:2013, Clause 14 System acquisition, development and maintenance
B.2.11 ISO/IEC 27002:2013, Clause 15 Supplier relationships
B.2.12 ISO/IEC 27002:2013, Clause 16 Information security incident management
B.2.13 ISO/IEC 27002:2013, Clause 17 Information security aspects of business continuity management
B.2.14 ISO/IEC 27002:2013, Clause 6 Compliance

Annex C (informative) Technical assessment guide for cloud services (Infrastructure as a service)

C.1 Positioning and purpose
C.2 Relationship with other international standards
C.3 Structure of this annex
C.4 Cloud services (infrastructure as a service) environment model
C.4.1 Meaning of the model introduced
C.4.2 Model and components
C.4.3 Correspondence to ISO/IEC 17789
C.5 Common practice in the Implementation Model
C.5.1 General
C.5.2 Application of virtualization technologies in the cloud service
C.5.3 Carrying out the technical assessment for the common aspects in the virtualization mechanism
C.5.3.1 Operation Security
C.6 Server virtualization
C.6.1 Overview of server virtualization
C.6.2 Application of server virtualization in the cloud services
C.6.3 Carrying out the technical assessment for the server virtualization
C.6.3.1 Access Control
C.7 Network virtualization
C.7.1 Overview of network virtualization
C.7.2 Application of network virtualization in the cloud services

C.7.3 Carrying out a technical assessment for the network virtualization
C.7.3.1 Access control
C.7.3.2 Cryptography
C.7.3.3 Communications security
C.8 Storage virtualization
C.8.1 Overview of storage virtualization
C.8.2 Application of storage virtualization in the cloud services
C.8.3 Carrying out the technical assessment for the storage virtualization
C.8.3.1 Access control
C.8.3.2 Cryptography
C.8.3.3 Operations security
C.9 Service management
C.9.1 Overview of Service management
C.9.2 Application of server virtualization in the cloud services
C.9.3 Carrying out the technical assessment for the Service management
C.9.3.1 User access management
C.9.3.2 Cryptography
C.9.3.3 Information security incident management
C.10 Relational table for denotations in ISO/IEC 27017 and this annex

Page count: 91