ISO/IEC 27007:2011-11 (E)

Information technology - Security techniques - Guidelines for information security management systems auditing

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Principles of auditing 1

5 Managing an audit programme 1
5.1 General 1
5.1.1 IS 5.1 General 2
5.2 Establishing the audit programme objectives 2
5.2.1 IS 5.2 Establishing the audit programme objectives 2
5.3 Establishing the audit programme 2
5.3.1 Role and responsibilities of the person managing the audit programme 2
5.3.2 Competence of the person managing the audit programme 2
5.3.3 Determining the extent of the audit programme 2
5.3.4 Identifying and evaluating audit programme risks 3
5.3.5 Establishing procedures for the audit programme 3
5.3.6 Identifying audit programme resources 3
5.4 Implementing the audit programme 3
5.4.1 General 3
5.4.2 Defining the objectives, scope and criteria for an individual audit 3
5.4.3 Selecting the audit methods 4
5.4.4 Selecting the audit team members 4
5.4.5 Assigning responsibility for an individual audit to the audit team leader 5
5.4.6 Managing the audit programme outcome 5
5.4.7 Managing and maintaining audit programme records 5
5.5 Monitoring the audit programme 5
5.6 Reviewing and improving the audit programme 5

6 Performing an audit 5
6.1 General 5
6.2 Initiating the audit 5
6.2.1 General 5
6.2.2 Establishing initial contact with the auditee 5
6.2.3 Determining the feasibility of the audit 5
6.3 Preparing audit activities 6
6.3.1 Performing document review in preparation for the audit 6
6.3.2 Preparing the audit plan 6
6.3.3 Assigning work to the audit team 6
6.3.4 Preparing work documents 6
6.4 Conducting the audit activities 6
6.4.1 General 6
6.4.2 Conducting the opening meeting 6
6.4.3 Performing document review while conducting the audit 6
6.4.4 Communicating during the audit 6

6.4.5 Assigning roles and responsibilities of guides and observers 6
6.4.6 Collecting and verifying information 6
6.4.7 Generating audit findings 7
6.4.8 Preparing audit conclusions 7
6.4.9 Conducting the closing meeting 7
6.5 Preparing and distributing the audit report 7
6.5.1 Preparing the audit report 7
6.5.2 Distributing the audit report 7
6.6 Completing the audit 7
6.7 Conducting audit follow-up 7

7 Competence and evaluation of auditors 7
7.1 General 7
7.2 Determining auditor competence to fulfil the needs of the audit programme 7
7.2.1 General 7
7.2.2 Personal behaviour 8
7.2.3 Knowledge and skills 8
7.2.4 Achieving auditor competence 9
7.2.5 Audit team leader 9
7.3 Establishing the auditor evaluation criteria 9
7.4 Selecting the appropriate auditor evaluation method 9
7.5 Conducting auditor evaluation 9
7.6 Maintaining and improving auditor competence 9

Annex A (informative) Practice Guidance for ISMS Auditing 10

Bibliography 27