ISO/IEC 27007:2020-01 (E)

Information security, cybersecurity and privacy protection - 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
5.2 Establishing audit programme objectives 1
5.3 Determining and evaluating audit programme risks and opportunities 2
5.4 Establishing audit programme 2
5.4.1 Roles and responsibilities of the individual(s) managing audit programme 2
5.4.2 Competence of individual(s) managing audit programme 2
5.4.3 Establishing extent of the audit programme 2
5.4.4 Determining audit programme resources 3
5.5 Implementing audit programme 3
5.5.1 General 3
5.5.2 Defining the objectives, scope and criteria for an individual audit 3
5.5.3 Selecting and determining audit methods 4
5.5.4 Selecting audit team members 4
5.5.5 Assigning responsibility for an individual audit to the audit team leader 4
5.5.6 Managing audit programme results 4
5.5.7 Managing and maintaining audit programme records 4
5.6 Monitoring audit programme 5
5.7 Reviewing and improving audit programme 5

6 Conducting an audit **5**

6.1 General 5
6.2 Initiating audit 5
6.2.1 General 5
6.2.2 Establishing contact with auditee 5
6.2.3 Determining feasibility of audit 5
6.3 Preparing audit activities 5
6.3.1 Performing review of documented information 5
6.3.2 Audit planning 5
6.3.3 Assigning work to audit team 6
6.3.4 Preparing documented information for audit 6
6.4 Conducting audit activities 6
6.4.1 General 6
6.4.2 Assigning roles and responsibilities of guides and observers 6
6.4.3 Conducting opening meeting 6
6.4.4 Communicating during audit 6
6.4.5 Audit information availability and access 6
6.4.6 Reviewing document information while conducting audit 6
6.4.7 Collecting and verifying information 7
6.4.8 Generating audit findings 7
6.4.9 Determining audit conclusions 7
6.4.10 Conducting closing meeting 7

6.5 Preparing and distributing audit report 7
6.5.1 Preparing audit report 7
6.5.2 Distributing audit report 7
6.6 Completing audit 7
6.7 Conducting audit follow-up 7

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

Annex A (informative) **Guidance for ISMS auditing practice 10**

Bibliography 39