DIN EN ISO/IEC 27007:2022-10 (E)

Information security, cybersecurity and privacy protection - Guidelines for information security management systems auditing (I SO/IEC 27007:2020)

Contents

Page

European foreword 4

Foreword 5

Introduction 6

1 Scope 7

2 Normative references 7

3 Termsanddefinitions 7

4 Principles of auditing 7

5 Managing an audit programme 7
5.1 General 7
5.2 Establishing audit programme objectives 7
5.3 Determining and evaluating audit programme risks and opportunities 8
5.4 Establishing audit programme 8
5.4.1 Roles and responsibilities of the individual(s) managing audit programme 8
5.4.2 Competence of individual(s) managing audit programme 8
5.4.3 Establishing extent of the audit programme 8
5.4.4 Determining audit programme resources 9
5.5 Implementing audit programme 9
5.5.1 General 9
5.5.2 Defining the objectives, scope and criteria for an individual audit 9
5.5.3 Selecting and determining audit methods 10
5.5.4 Selecting audit team members 10
5.5.5 Assigning responsibility for an individual audit to the audit team leader 10
5.5.6 Managing audit programme results 10
5.5.7 Managing and maintaining audit programme records 10
5.6 Monitoring audit programme 11
5.7 Reviewing and improving audit programme 11

6 Conducting an audit 11
6.1 General 11
6.2 Initiating audit 11
6.2.1 General 11
6.2.2 Establishing contact with auditee 11
6.2.3 Determining feasibility of audit 11
6.3 Preparing audit activities 11
6.3.1 Performing review of documented information 11
6.3.2 Audit planning 11
6.3.3 Assigning work to audit team 12
6.3.4 Preparing documented information for audit 12
6.4 Conducting audit activities 12
6.4.1 General 12
6.4.2 Assigning roles and responsibilities of guides and observers 12
6.4.3 Conducting opening meeting 12
6.4.4 Communicating during audit 12
6.4.5 Audit information availability and access 12

6.4.6 Reviewing document information while conducting audit 12
6.4.7 Collecting and verifying information 13
6.4.8 Generating audit findings 13
6.4.9 Determining audit conclusions 13
6.4.10 Conducting closing meeting 13
6.5 Preparing and distributing audit report 13
6.5.1 Preparing audit report 13
6.5.2 Distributing audit report 13
6.6 Completing audit 13
6.7 Conducting audit follow-up 13

7 Competence and evaluation of auditors 14
7.1 General 14
7.2 Determining auditor competence 14
7.2.1 General 14
7.2.2 Personal behaviour 14
7.2.3 Knowledge and skills 14
7.2.4 Achieving auditor competence 15
7.2.5 Achieving audit team leader competence 15
7.3 Establishing auditor evaluation criteria 15
7.4 Selecting appropriate auditor evaluation method 15
7.5 Conducting auditor evaluation 15
7.6 Maintaining and improving auditor competence 15

Annex A (informative) Guidance for ISMS auditing practice 16

Bibliography 45