

ISO 22340:2024-11 (E)

Security and resilience - Protective security - Guidelines for an enterprise protective security architecture and framework

Contents

Page

- Foreword..... iv
- Introduction..... v
- 1 Scope..... 1**
- 2 Normative references..... 1**
- 3 Terms and definitions..... 1**
- 4 Enterprise protective security architecture..... 4**
 - 4.1 General..... 4
 - 4.2 Integration..... 5
 - 4.3 Elements of the architecture..... 5
- 5 Protective security principles and domains..... 6**
 - 5.1 Protective security principles..... 6
 - 5.2 Protective security domains..... 7
- 6 Security governance domain..... 7**
 - 6.1 Objective..... 7
 - 6.2 Security controls..... 8
 - 6.2.1 The responsible security executive..... 8
 - 6.2.2 Security management structure..... 9
 - 6.3 Implementation..... 19
- 7 Personnel security domain..... 20**
 - 7.1 Objective..... 20
 - 7.2 Security controls..... 20
 - 7.2.1 General..... 20
 - 7.2.2 Eligibility and suitability of personnel..... 21
 - 7.2.3 Ongoing assessment of personnel..... 21
 - 7.2.4 Separating personnel..... 21
 - 7.2.5 Cooperation between human resources and security in applying controls..... 21
 - 7.3 Implementation..... 21
- 8 Information security domain..... 22**
 - 8.1 Objective..... 22
 - 8.2 Security controls..... 23
 - 8.2.1 Business impact and security classification of information..... 23
 - 8.2.2 Control access to the organization’s information..... 23
 - 8.3 Implementation..... 24
- 9 Cybersecurity domain..... 24**
 - 9.1 Objective..... 24
 - 9.2 Security controls..... 25
 - 9.2.1 Defining the system and selecting security controls..... 25
 - 9.2.2 Implementing and evaluating security controls..... 25
 - 9.2.3 Authorizing cyber systems..... 25
 - 9.2.4 Monitoring cyber systems..... 25
 - 9.3 Implementation..... 26
 - 9.4 Rapid development of the digital domain..... 26
- 10 Physical security domain..... 26**
 - 10.1 Objective..... 26

| | | |
|-----------|--|-----------|
| 10.2 | Security controls | 27 |
| 10.2.1 | Organizational physical assets | 27 |
| 10.2.2 | Organizational facilities | 27 |
| 10.3 | Implementation | 27 |
| 11 | Developing the organization's security maturity | 28 |
| | Bibliography | 31 |