NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2025.3
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm

| FDE# | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF# | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes (optional) |
|--------|---|---|-------------------|----------------------|--|----------|--|-----------------------------|--|
| 1.0 | Scope | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | no relationship | N/A | N/A | N/A | (optional) N/A | No requirements to map to. |
| 2.0 | Normative references | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | no relationship | N/A | N/A | N/A | N/A | No requirements to map to. |
| 3.0 | Terms and definitions | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Standardized Terminology | SEA-02.1 | Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments. | | |
| 4.0 | Context of the organization | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | no relationship | N/A | N/A | N/A | N/A | No requirements to map to. |
| 4.1 | Understanding the organization and its context | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Defining Business Context & Mission | GOV-08 | Mechanisms exist to define the context of its business model and document the organization's mission. | 5 | |
| 4.1 | Understanding the organization and its context | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Define Control Objectives | GOV-09 | Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system. | 5 | |
| 4.1 | Understanding the organization and its context | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 5 | ISO 27001:2022 Amendment 1 adds *climate action changes* that a reasonable person would conclude has nothing to do with cybersecurity and is merely an inclusion for Environmental, Social & Governance (ESG) compliance to bush a political agenda. |
| 4.2 | Understanding the needs and expectations of interested parties | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Define Control Objectives | GOV-09 | Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system. | 5 | |
| 4.2 | Understanding the needs and expectations of interested parties | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Stakeholder Identification & Involvement | AST-01.2 | Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets. | 5 | |
| 4.2(a) | Understanding the needs and expectations of interested parties | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Defining Business Context & Mission | GOV-08 | Mechanisms exist to define the context of its business model and document the organization's mission. | 5 | |
| 4.2(a) | Understanding the needs and expectations of interested parties | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Stakeholder Identification & Involvement | AST-01.2 | Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets. | 5 | |
| 4.2(b) | Understanding the needs and expectations of interested parties | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Define Control Objectives | GOV-09 | Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system. | 5 | |
| 4.2(c) | Understanding the needs and expectations of interested parties | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Define Control Objectives | GOV-09 | Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system. | 5 | |
| 4.3 | Determining the scope of the information security management system | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Defining Business Context & Mission | GOV-08 | Mechanisms exist to define the context of its business model and document the organization's mission. | 5 | |
| 4.3 | Determining the scope of the information security management system | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Compliance Scope | CPL-01.2 | Mechanisms exist to document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations. | 5 | |
| 4.3 | Determining the scope of the information security management system | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Asset Scope Classification | AST-04.1 | Mechanisms exist to determine cybersecurity and data protection control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties). | 5 | |
| 4.3(a) | Determining the scope of the information security management system | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Compliance Scope | CPL-01.2 | Mechanisms exist to document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations. | 5 | |
| 4.3(b) | Determining the scope of the information security management system | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Compliance Scope | CPL-01.2 | Mechanisms exist to document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations. | 5 | |
| 4.3(c) | Determining the scope of the information security management system | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix | TPM-05.4 | Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs). | 5 | |
| 4.3(c) | Determining the scope of the information security management system | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Compliance Scope | CPL-01.2 | Mechanisms exist to document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations. | 5 | |
| 4.3(c) | Determining the scope of the information security management system | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Customer Responsibility Matrix (CRM) | CLD-06.1 | Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for controls between the Cloud Service Provider (CSP) and its customers. | 5 | |
| 4.4 | Information security management system | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Cybersecurity & Data Protection Governance Program | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | 10 | |
| 4.4 | Information security management system | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 5.0 | Leadership | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | no relationship | N/A | N/A | N/A | N/A | This is merely a section title without content. |
| 5.1 | Leadership and commitment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Cybersecurity & Data Protection Governance | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | 10 | |
| 5.1 | Leadership and commitment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Program Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, | 10 | |
| 5.1 | Leadership and | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Defining Business | GOV-08 | which meets formally and on a regular basis. Mechanisms exist to define the context of its business model and | 5 | |
| 5.1(a) | commitment Leadership and | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Context & Mission Publishing Cybersecurity & Data Protection | GOV-02 | document the organization's mission. Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 5.1(a) | commitment Leadership and | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | subset of | Documentation Cybersecurity & Data Protection Governance | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | 10 | |
| 5.1(b) | commitment Leadership and | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | subset of | Program Cybersecurity & Data Protection Governance | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | 10 | |
| 5.1(c) | commitment Leadership and commitment | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Program Cybersecurity & Data Protection Resource | PRM-02 | Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity and data protection programs and document all exceptions to this requirement. | 5 | |
| 5.1(c) | Leadership and commitment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Management Cybersecurity & Data Protection Governance | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | 10 | |
| 5.1(d) | Leadership and commitment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Program Cybersecurity & Data Protection Governance | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | 10 | |
| 5.1(e) | Leadership and commitment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Program Cybersecurity & Data Protection Governance | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | 10 | |
| 5.1(e) | Leadership and commitment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Program Cybersecurity & Data Protection Portfolio | PRM-01 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection-related resource planning controls that define a viable plan | 10 | |
| 5.1(f) | Leadership and | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Management Assigned Cybersecurity & Data Protection | GOV-04 | for achieving cybersecurity and data protection objectives. Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, | 5 | |
| 5.1(f) | commitment Leadership and | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | subset of | Responsibilities Cybersecurity & Data Protection Governance | GOV-01 | implement and maintain an enterprise-wide cybersecurity and data protection program. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | 10 | |
| | commitment Leadership and | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | | | Program Cybersecurity & Data | | data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and | | |
| 5.1(g) | commitment | https://www.iso.org/standard/27001 | Functional | subset of | Protection Governance Program | GOV-01 | data protection governance controls. | 10 | |

| FDE# | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF# | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes (optional) |
|---|--|---|---|---|--|---|--|--|--|
| 5.1(h) | Leadership and commitment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Cybersecurity & Data Protection Governance | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | 10 | |
| 5.1(h) | Leadership and commitment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Program Assigned Cybersecurity & Data Protection Responsibilities | GOV-04 | Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program. | 5 | |
| 5.2 | Policy | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 5.2(a) | Policy | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 5.2(b) | Policy | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 5.2(b) | Policy | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Define Control Objectives | GOV-09 | Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system. | 5 | |
| 5.2(c) | Policy | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 5.2(d) | Policy | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 5.2(e) | Policy | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 5.2(f) | Policy | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 5.2(g) | Policy | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 5.3 | Organizational roles, responsibilities and authorities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 5.3 | Organizational roles, responsibilities and authorities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Assigned Cybersecurity & Data Protection Responsibilities | GOV-04 | Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program. | 5 | |
| 5.3 | Organizational roles, responsibilities and authorities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Defined Roles & Responsibilities | HRS-03 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 5 | |
| 5.3(a) | Organizational roles, responsibilities and authorities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 5.3(a) | Organizational roles, responsibilities and authorities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Assigned Cybersecurity & Data Protection Responsibilities | GOV-04 | Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program. | 5 | |
| 5.3(b) | Organizational roles, responsibilities and authorities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Assigned Cybersecurity & Data Protection Responsibilities | GOV-04 | Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program. | 5 | |
| 5.3(b) | Organizational roles, responsibilities and authorities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 6.0 | Planning | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | no relationship | N/A | N/A | N/A | N/A | This is merely a section title without content. |
| 6.1 | | | | | | 1071 | *** | IVA | |
| | Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | no relationship | N/A | N/A | N/A | N/A | This is merely a section title without content. |
| 6.1.1 | and opportunities Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional Functional | no relationship | Risk Management Program Cybersecurity & Data | | | | This is merely a section title without content. |
| 6.1.1 | and opportunities Actions to address risks and opportunities Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional Functional | subset of | Risk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data | N/A RSK-01 GOV-01 | N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and | N/A 10 | This is merely a section title without content. |
| | and opportunities Actions to address risks and opportunities Actions to address risks and opportunities Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 thtps://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program | N/A RSK-01 | N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | N/A 10 10 10 | This is merely a section title without content. |
| 6.1.1 | and opportunities Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional Functional | subset of | Risk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Risk Management Program | N/A RSK-01 GOV-01 | N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | N/A 10 | This is merely a section title without content. |
| 6.1.1(a) 6.1.1(a) 6.1.1(b) | and opportunities Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional Functional Functional Functional | subset of subset of subset of subset of subset of | Risk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Risk Management | N/A RSK-01 GOV-01 GOV-01 RSK-01 | N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection sovernance controls. | N/A 10 10 10 10 10 10 | This is merely a section title without content. |
| 6.1.1 6.1.1(a) 6.1.1(a) 6.1.1(b) | and opportunities Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional Functional Functional Functional Functional Functional | subset of | Pisk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data | N/A RSK-01 GOV-01 GOV-01 RSK-01 GOV-01 | N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and facilitate in the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and facilitation in the implementation of strategic, operational and facilitation is to facilitate the implementation of cybersecurity and | N/A 10 10 10 10 10 10 10 10 | This is merely a section title without content. |
| 6.1.1(a) 6.1.1(a) 6.1.1(b) | and opportunities Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional Functional Functional Functional | subset of subset of subset of subset of subset of | Risk Management Program Ophersocurity & Data Protection Governance Program Ophersocurity & Data Protection Governance Program Risk Management Program Ophersocurity & Data Protection Governance Program Risk Management Risk Management | N/A RSK-01 GOV-01 GOV-01 RSK-01 | NIA Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | N/A 10 10 10 10 10 10 | This is merely a section title without content. |
| 6.1.1(a) 6.1.1(a) 6.1.1(b) 6.1.1(b) 6.1.1(c) | and opportunities Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional Functional Functional Functional Functional Functional Functional | subset of | Pilsk Management Program Cybersecurity & Data Protection Governance Protection Governance Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Risk Management Program Risk Management Program Program Risk Management Program Risk Management Program Risk Management Program Risk Management | N/A RSK-01 GOV-01 GOV-01 RSK-01 GOV-01 GOV-01 | N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | N/A 10 10 10 10 10 10 10 10 10 | This is merely a section title without content. |
| 6.1.1 6.1.1(a) 6.1.1(b) 6.1.1(b) 6.1.1(c) 6.1.1(c) | and opportunities Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional Functional Functional Functional Functional Functional Functional Functional | subset of | Pilsk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Protection Governance Program Risk Management Program Risk Management Program Risk Management Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Risk Management Program Risk Management Program Risk Management Risk Management Risk Management Risk Management Risk Management | N/A RSK-01 GOV-01 GOV-01 RSK-01 GOV-01 RSK-01 RSK-01 | N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | N/A 10 10 10 10 10 10 10 10 10 1 | This is merely a section title without content. |
| 6.1.1 (6.1.1(a) (6.1.1(b) (6.1.1(b) (6.1.1(c) (6.1.1(c) (6.1.1(d) | and opportunities Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program Ophersocurity & Data Protection Governance Program Ophersocurity & Data Protection Governance Program Risk Management Program Ophersocurity & Data Protection Governance Program Risk Management Program Ophersocurity & Data Protection Governance Program Risk Management Program Cybersocurity & Data Protection Governance Program Risk Management | N/A RSK-01 GOV-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 GOV-01 | NIA Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | N/A 10 10 10 10 10 10 10 10 10 1 | This is merely a section title without content. |
| 6.1.1 (a) (c) (1.1(a) (d) (d) (d) (d) (d) (d) (d) (d) (d) (d | and opportunities Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Pilsk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Risk Management Program Risk Management | N/A RSK-01 GOV-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 RSK-01 | N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | N/A 10 10 10 10 10 10 10 10 10 1 | This is merely a section title without content. |
| 6.1.1 (a) (c) (1.1(a) (d) (d) (d) (d) (d) (d) (d) (d) (d) (d | and opportunities Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Pilsk Management Program Program Program Protection Governance Program Protection Governance Program Protection Governance Program Program Program Program Program Program Protection Governance Program Program Protection Governance Program Pro | N/A RSK-01 GOV-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 | NIA Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | N/A 10 10 10 10 10 10 10 10 10 10 10 10 10 | This is merely a section title without content. |
| 6.1.1 6.1.1(a) 6.1.1(b) 6.1.1(b) 6.1.1(c) 6.1.1(c) 6.1.1(d) 6.1.1(d) 6.1.1(d) 6.1.1(d) 6.1.1(e)(1) | and opportunities Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program Ophersecurity & Data Protection Governance Program Risk Management Protection Governance Program Risk Management Program Ophersecurity & Data Protection Governance Program Risk Management Program Ophersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Ophersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data | N/A RSK-01 GOV-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 | NIA Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | N/A 10 10 10 10 10 10 10 10 10 1 | This is merely a section tritle without content. |
| 6.1.1 6.1.1(a) 6.1.1(b) 6.1.1(b) 6.1.1(c) 6.1.1(c) 6.1.1(d) 6.1.1(d) 6.1.1(d) 6.1.1(e)(1) 6.1.1(e)(1) | and opportunities Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program Ophersecurity & Data Protection Governance Program Risk Management Protection Governance Program Risk Management Program Ophersecurity & Data Protection Governance Program Risk Management Program Ophersecurity & Data Protection Governance Program Risk Management Program | N/A RSK-01 GOV-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the impl | NVA 10 10 10 10 10 10 10 10 10 10 10 10 10 | This is merely a section tritle without content. |
| 6.1.1 6.1.1(a) 6.1.1(b) 6.1.1(b) 6.1.1(c) 6.1.1(c) 6.1.1(d) 6.1.1(d) 6.1.1(e)(1) 6.1.1(e)(1) 6.1.1(e)(1) | and opportunities Actions to address risks and opportunities | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program Ophersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Risk Management | N/A RSK-01 GOV-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 RSK-01 RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk traditions the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the impleme | N/A 10 10 10 10 10 10 10 10 10 1 | This is merely a section tritle without content. |
| 6.1.1 6.1.1(a) 6.1.1(b) 6.1.1(b) 6.1.1(c) 6.1.1(c) 6.1.1(d) 6.1.1(d) 6.1.1(d) 6.1.1(e)(1) 6.1.1(e)(1) 6.1.1(e)(2) 6.1.1(e)(2) | and opportunities Actions to address risks and opportunities Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Protection Governance Program Risk Management Program | N/A RSK-01 GOV-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 RSK-01 RSK-01 RSK-01 RSK-01 RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechani | N/A 10 10 10 10 10 10 10 10 10 1 | This is merely a section tritle without content. |
| 6.1.1 6.1.1(a) 6.1.1(b) 6.1.1(b) 6.1.1(c) 6.1.1(c) 6.1.1(d) 6.1.1(d) 6.1.1(e)(1) 6.1.1(e)(2) 6.1.1(e)(2) 6.1.2 | and opportunities Actions to address risks and opportunities Information security risk assessment Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program Ophersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Risk Management Risk Management Risk Management Program Risk Management Risk Management Risk Management Program Risk Management | N/A RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 RSK-01 RSK-01 RSK-01 RSK-01 RSK-01 RSK-01 RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms stat to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms sxist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exis | N/A 10 10 10 10 10 10 10 10 10 1 | This is merely a section tritle without content. |



| FDE# | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF# | Secure Controls Framework (SCF) Control Description | Strength of Relationship (optional) | Notes (optional) |
|-------------|---|--|-------------------|----------------------|---------------------------------------|----------|---|---|------------------|
| 6.1.2(a)(1) | Information security risk | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Framing | RSK-01.1 | Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; | 5 | |
| | | | | | | | (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | | |
| 6.1.2(a)(2) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and factical risk management controls. | 10 | |
| 6.1.2(a)(2) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Framing | RSK-01.1 | Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for | 5 | |
| 6.1.2(b) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Framing | RSK-01.1 | managing risk. Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | 5 | |
| 6.1.2(b) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | 10 | |
| 6.1.2(c) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Framing | RSK-01.1 | Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for | 5 | |
| 6.1.2(c) | Information security risk | | Functional | subset of | Risk Management | RSK-01 | managing risk. Mechanisms exist to facilitate the implementation of strategic, operational | 10 | |
| 6.1.2(c) | assessment Information security risk assessment | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Program Risk Identification | RSK-03 | and tactical risk management controls. Mechanisms exist to identify and document risks, both internal and external. | 5 | |
| 6.1.2(c)(1) | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Framing | RSK-01.1 | Machanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | 5 | |
| 6.1.2(c)(1) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program | RSK-01 | menaging risk. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | 10 | |
| 6.1.2(c)(1) | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Identification | RSK-03 | Mechanisms exist to identify and document risks, both internal and external. | 5 | |
| 6.1.2(c)(2) | assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | 10 | |
| 6.1.2(c)(2) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Identification | RSK-03 | Mechanisms exist to identify and document risks, both internal and external. Mechanisms exist to identify: | 5 | |
| 6.1.2(c)(2) | assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Framing | RSK-01.1 | (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The originational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | 5 | |
| 6.1.2(d) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | 10 | |
| 6.1.2(d) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Assessment | RSK-04 | Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD). | 5 | |
| 6.1.2(d) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Framing | RSK-01.1 | Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | 5 | |
| 6.1.2(d)(1) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Management Program | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | 5 | |
| 6.1.2(d)(1) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Framing | RSK-01.1 | Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | 10 | |
| 6.1.2(d)(1) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Assessment | RSK-04 | Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD). | 5 | |
| 6.1.2(d)(2) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Framing | RSK-01.1 | Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | 5 | |
| 6.1.2(d)(2) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | 10 | |
| 6.1.2(d)(2) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Assessment | RSK-04 | Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Te | 5 | |
| 6.1.2(d)(3) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk-Based Security Categorization | RSK-02 | Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationals) in the security plan for systems; and (2) Ensure the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner. | 5 | |
| 6.1.2(d)(3) | assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Framing | RSK-01.1 | Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | 5 | |
| 6.1.2(d)(3) | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | 10 | |



Secure Controls Framework (SCF) 3 of 9

| FDE# | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF# | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes (optional) |
|-------------|---|--|-------------------|----------------------|------------------------------|----------|--|-----------------------------|---|
| | | | | | | | Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, | (optional) | |
| 6.1.2(d)(3) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Assessment | RSK-04 | disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD). | 5 | |
| | | | | | | | Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; | | |
| 6.1.2(e) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Framing | RSK-01.1 | (2) Constraints affecting risk assessments, risk response and risk monitoring; | 5 | |
| | | | | | | | (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | | |
| 6.1.2(e) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | 10 | |
| 6.1.2(e) | | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Risk Assessment | RSK-04 | Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's | 5 | |
| | assessment | https://www.iso.org/standard/27001 | | | | | Technology Assets, Applications, Services and/or Data (TAASD). | | |
| 6.1.2(e)(1) | | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Risk Assessment | RSK-04 | Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's | 5 | |
| | assessment | https://www.iso.org/standard/27001 | | | | | Technology Assets, Applications, Services and/or Data (TAASD). | | |
| | | | | | | | Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; | | |
| 6.1.2(e)(1) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Framing | RSK-01.1 | (2) Constraints affecting risk assessments, risk response and risk monitoring; | 5 | |
| | | | | | | | (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | | |
| 6.1.2(e)(1) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to identify: | 10 | |
| | | | | | | | (1) Assumptions affecting risk assessments, risk response and risk monitoring; | | |
| 6.1.2(e)(2) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Framing | RSK-01.1 | (2) Constraints affecting risk assessments, risk response and risk monitoring; | 5 | |
| | | | | | | | (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | | |
| 6.1.2(e)(2) | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Risk Management Program | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | 10 | |
| 6.1.2(e)(2) | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Assessment | RSK-04 | Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's | 5 | |
| | assessment | intps://www.iso.org/standard/27001 | | | | | Technology Assets, Applications, Services and/or Data (TAASD). | | |
| 6.1.3 | Information security risk treatment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Response | RSK-06.1 | Mechanisms exist to respond to findings from cybersecurity and data protection assessments, incidents and audits to ensure proper remediation has been performed. | 5 | |
| 6.1.3 | Information security risk treatment | https://www.iso.org/standard/27001 | Functional | intersects with | Risk Remediation | RSK-06 | Mechanisms exist to remediate risks to an acceptable level. | 5 | |
| 6.1.3(a) | Information security risk treatment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Response | RSK-06.1 | Mechanisms exist to respond to findings from cybersecurity and data protection assessments, incidents and audits to ensure proper remediation has been performed. | 5 | |
| 6.1.3(a) | Information security risk treatment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Remediation | RSK-06 | Mechanisms exist to remediate risks to an acceptable level. | 5 | |
| 6.1.3(b) | Information security risk treatment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Response | RSK-06.1 | Mechanisms exist to respond to findings from cybersecurity and data protection assessments, incidents and audits to ensure proper remediation has been performed. | 5 | |
| 6.1.3(b) | Information security risk treatment Information security risk | https://www.iso.org/standard/27001 | Functional | intersects with | Risk Remediation | RSK-06 | Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to remediate risks to an acceptable level. | 5 | |
| 6.1.3(c) | treatment | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Risk Remediation | RSK-06 | Mechanisms exist to respond to findings from cybersecurity and data | 5 | |
| 6.1.3(c) | treatment | https://www.iso.org/standard/27001 | Functional | intersects with | Risk Response | RSK-06.1 | protection assessments, incidents and audits to ensure proper remediation has been performed. Mechanisms exist to respond to findings from cybersecurity and data | 5 | |
| 6.1.3(d) | Information security risk treatment | https://www.iso.org/standard/27001 | Functional | intersects with | Risk Response | RSK-06.1 | protection assessments, incidents and audits to ensure proper remediation has been performed. | 5 | |
| 6.1.3(d) | Information security risk treatment Information security risk | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Risk Remediation | RSK-06 | Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to remediate risks to an acceptable level. | 5 | |
| 6.1.3(e) | treatment Information security risk | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Risk Remediation | RSK-06 | Mechanisms exist to respond to findings from cybersecurity and data | 5 | |
| 6.1.3(e) | treatment | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Risk Response | RSK-06.1 | protection assessments, incidents and audits to ensure proper remediation has been performed. Mechanisms exist to remediate risks to an acceptable level. | 5 | |
| 6.1.3(f) | treatment Information security risk | https://www.iso.org/standard/27001 | Functional | intersects with | Risk Remediation | RSK-06 | Mechanisms exist to respond to findings from cybersecurity and data | 5 | |
| 6.1.3(f) | treatment Information security | https://www.iso.org/standard/27001 | Functional | intersects with | Risk Response | RSK-06.1 | protection assessments, incidents and audits to ensure proper remediation has been performed. Mechanisms exist to establish control objectives as the basis for the | 5 | |
| 6.2 | objectives and planning to achieve them Information security | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Define Control Objectives | GOV-09 | selection, implementation and management of the organization's internal control system. Mechanisms exist to establish control objectives as the basis for the | 5 | |
| 6.2(a) | objectives and planning to achieve them | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Define Control Objectives | GOV-09 | rections and the establish control objectives as the basis for the selection, implementation and management of the organization's internal control system. | 5 | |
| 6.2(b) | Information security objectives and planning to achieve them | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Define Control Objectives | GOV-09 | Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system. | 5 | |
| 6.2(c) | Information security objectives and planning | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Define Control Objectives | GOV-09 | Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal | 5 | |
| 6.2(d) | to achieve them Information security objectives and planning | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Define Control Objectives | GOV-09 | control system. Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal | 5 | |
| | to achieve them Information security | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | | GOV-09 | control system. Mechanisms exist to establish control objectives as the basis for the | 5 | |
| 6.2(e) | objectives and planning to achieve them Information security | https://www.iso.org/standard/27001 | | micer secus with | Define Control Objectives | | selection, implementation and management of the organization's internal control system. Mechanisms exist to establish control objectives as the basis for the | | |
| 6.2(f) | objectives and planning to achieve them Information security | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Define Control Objectives | GOV-09 | selection, implementation and management of the organization's internal control system. Mechanisms exist to establish control objectives as the basis for the | 5 | |
| 6.2(g) | objectives and planning to achieve them | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Define Control Objectives | GOV-09 | selection, implementation and management of the organization's internal control system. | 5 | |
| 6.2(h) | Information security objectives and planning to achieve them | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Define Control Objectives | GOV-09 | Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system. | 5 | |
| 6.2(i) | Information security objectives and planning | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Define Control Objectives | GOV-09 | Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal | 5 | |
| 6.2(j) | to achieve them Information security objectives and planning | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Define Control Objectives | GOV-09 | control system. Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal | 5 | |
| | to achieve them Information security | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | | | | | control system. Mechanisms exist to establish control objectives as the basis for the | | |
| 6.2(k) | objectives and planning to achieve them Information security | https://www.iso.org/standard/27001 | Functional | intersects with | Define Control Objectives | GOV-09 | selection, implementation and management of the organization's internal control system. Mechanisms exist to establish control objectives as the basis for the | 5 | |
| 6.2(l) | objectives and planning to achieve them | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Define Control Objectives | GOV-09 | selection, implementation and management of the organization's internal control system. | 5 | |
| 6.3 | Planning of changes | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | subset of | Change Management Program | CHG-01 | Mechanisms exist to facilitate the implementation of a change management program. | 10 N/A | This is merely a section title without content. |
| 7.0 | Support | https://www.iso.org/standard/27001 | Functional | no relationship | N/A | N/A | N/A | N/A | |



ecure Controls Framework (SCF) 4 of

| FDE# | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF# | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes (optional) |
|------------------|------------|--|-------------------|----------------------|---|--------------------|--|-----------------------------|------------------|
| 7.1 | Resources | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Cybersecurity & Data Protection Resource | PRM-02 | Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity and data | (optional) | |
| 7.1 | Resources | https://www.iso.org/standard/27001 | runcuonat | intersects with | Management | PRM-02 | protection programs and document all exceptions to this requirement. | 5 | |
| 7.2 | Competence | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Competency Requirements for Security-Related Positions | HRS-03.2 | Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set. | 5 | |
| 7.2(a) | Competence | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Position Categorization | HRS-02 | Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions. | 5 | |
| 7.2(a) | Competence | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Competency Requirements for Security-Related Positions | HRS-03.2 | Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set. | 5 | |
| 7.2(b) | Competence | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Competency Requirements for Security-Related | HRS-03.2 | Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set. | 5 | |
| 7.2(b) | Competence | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Positions Personnel Screening | HRS-04 | Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access. | 5 | |
| 7.2(c) | Competence | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Personnel Screening | HRS-04 | Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access. | 5 | |
| 7.2(c) | Competence | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Competency Requirements for Security-Related Positions | HRS-03.2 | Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set. | 5 | |
| 7.2(d) | Competence | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Human Resources Security Management | HRS-01 | Mechanisms exist to facilitate the implementation of personnel security controls. | 10 | |
| 7.2(d) | Competence | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Competency Requirements for Security-Related Positions | HRS-03.2 | Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set. | 5 | |
| 7.3 | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Social Media & Social Networking Restrictions | HRS-05.2 | Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information. | 5 | |
| 7.3 | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Formal Indoctrination | HRS-04.2 | Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access. | 5 | |
| 7.3 | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | User Awareness | HRS-03.1 | Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment. | 5 | |
| 7.3 | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Use of Communications Technology | HRS-05.3 | Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously. | 5 | |
| 7.3 | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Human Resources Security Management | HRS-01 | Mechanisms exist to facilitate the implementation of personnel security controls. | 10 | |
| 7.3 | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Use of Critical Technologies | HRS-05.4 | Mechanisms exist to govern usage policies for critical technologies. | 5 | |
| 7.3 | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Use of Mobile Devices | HRS-05.5 | Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources. | 5 | |
| 7.3 | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Policy Familiarization & Acknowledgement | HRS-05.7 | Mechanisms exist to ensure personnel receive recurring familiarization with the organization's cybersecurity and data protection policies and provide acknowledgement. Mechanisms exist to define acceptable and unacceptable rules of behavior | 5 | |
| 7.3 | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Rules of Behavior | HRS-05.1 | for the use of technologies, including consequences for unacceptable behavior. | 5 | |
| 7.3 | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Terms of Employment Defined Roles & | HRS-05 | Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work. Mechanisms exist to define cybersecurity roles & responsibilities for all | 5 | |
| 7.3 | Awareness | https://www.iso.org/standard/27001 | Functional | intersects with | Responsibilities | HRS-03 | personnel. Mechanisms exist to formally educate authorized users on proper data | 5 | |
| 7.3(a) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Formal Indoctrination | HRS-04.2 | handling practices for all the relevant types of data to which they have access. | 5 | |
| 7.3(a) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Terms of Employment | HRS-05 | Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work. Mechanisms exist to define rules of behavior that contain explicit | 5 | |
| 7.3(a) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Social Media & Social Networking Restrictions | HRS-05.2 | restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information. | 5 | |
| 7.3(a) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | User Awareness | HRS-03.1 | Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment. Mechanisms exist to establish usage restrictions and implementation | 5 | |
| 7.3(a) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Use of Communications Technology | HRS-05.3 | guidance for communications technologies based on the potential to cause damage to systems, if used maliciously. | 5 | |
| 7.3(a) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Use of Critical Technologies | HRS-05.4 | Mechanisms exist to govern usage policies for critical technologies. Mechanisms exist to manage business risks associated with permitting | 5 | |
| 7.3(a) | Awareness | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Use of Mobile Devices | HRS-05.5 | mobile device access to organizational resources. Mechanisms exist to define acceptable and unacceptable rules of behavior | 5 | |
| 7.3(a) | Awareness | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Rules of Behavior Human Resources | HRS-05.1 | for the use of technologies, including consequences for unacceptable behavior. Mechanisms exist to facilitate the implementation of personnel security | 5 | |
| 7.3(a) | Awareness | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | subset of | Security Management | HRS-01 | Controls. Mechanisms exist to communicate with users about their roles and | 10 | |
| 7.3(b) 7.3(b) | Awareness | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | User Awareness Defined Roles & | HRS-03.1 HRS-03 | responsibilities to maintain a safe and secure working environment. Mechanisms exist to define cybersecurity roles & responsibilities for all | 5 | |
| 7.3(b) | Awareness | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Responsibilities Terms of Employment | HRS-05 | personnel. Mechanisms exist to require all employees and contractors to apply | 5 | |
| 7.3(b) | Awareness | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Social Media & Social | HRS-05.2 | cybersecurity and data protection principles in their daily work. Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting | 5 | |
| 7.3(b) | Awareness | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Use of Communications Technology | HRS-05.3 | information on commercial websites and sharing account information. Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to | 5 | |
| 7.3(b) | Awareness | Buy a copy of ISO 27001 for control content: | Functional | subset of | Human Resources | HRS-01 | cause damage to systems, if used maliciously. Mechanisms exist to facilitate the implementation of personnel security | 10 | |
| 7.3(b) | Awareness | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Security Management Use of Critical Technologies | HRS-05.4 | controls. Mechanisms exist to govern usage policies for critical technologies. | 5 | |
| 7.3(b) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Formal Indoctrination | HRS-04.2 | Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access. | 5 | |
| 7.3(b) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Rules of Behavior | HRS-05.1 | Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior. | 5 | |
| 7.3(b) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Use of Mobile Devices | HRS-05.5 | Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources. | 5 | |
| 7.3(c) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | User Awareness | HRS-03.1 | Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment. | 5 | |
| 7.3(c) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Social Media & Social Networking Restrictions | HRS-05.2 | Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information. | 5 | |
| 7.3(c) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Human Resources Security Management | HRS-01 | Mechanisms exist to facilitate the implementation of personnel security controls. | 10 | |
| 7.3(c) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Terms of Employment | HRS-05 | Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work. Mechanisms exist to ensure personnel receive recurring familiarization | 5 | |
| 7.3(c) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Policy Familiarization & Acknowledgement | HRS-05.7 | with the organization's cybersecurity and data protection policies and provide acknowledgement. | 5 | |
| 7.3(c) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Formal Indoctrination | HRS-04.2 | Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access. Mechanisms exist to manage business risks associated with permitting | 5 | |
| 7.3(c) | Awareness | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Use of Mobile Devices Use of Communications | HRS-05.5 | mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources. Mechanisms exist to establish usage restrictions and implementation | 5 | |
| 7.3(c) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Use of Communications Technology | HRS-05.3 | guidance for communications technologies based on the potential to cause damage to systems, if used maliciously. | 5 | |



| FDE# | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF# | Secure Controls Framework (SCF) Control Description | Strength of Relationship (optional) | Notes (optional) |
|----------|-----------------------------------|--|-------------------|----------------------|---|----------|--|---|---|
| 7.3(c) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Rules of Behavior | HRS-05.1 | Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable | (optional) 5 | |
| 7.3(c) | Awareness | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Use of Critical Technologies | HRS-05.4 | behavior. Mechanisms exist to govern usage policies for critical technologies. | 5 | |
| 7.4 | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Threat Intelligence Feeds Feeds | THR-03 | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, tachniques and procedures to facilitate the implementation of preventative and compensating controls. | 5 | |
| 7.4 | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Cybersecurity & Data Protection-Minded Workforce | SAT-01 | Mechanisms exist to facilitate the implementation of security workforce development and awareness controls. | 10 | |
| 7.4 | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 7.4 | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Cybersecurity & Data Protection Awareness Training | SAT-02 | Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function. | 5 | |
| 7.4(a) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Cybersecurity & Data Protection Awareness Training | SAT-02 | Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function. | 5 | |
| 7.4(a) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 7.4(a) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Cybersecurity & Data Protection-Minded Workforce | SAT-01 | Mechanisms exist to facilitate the implementation of security workforce development and awareness controls. | 10 | |
| 7.4(a) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Threat Intelligence Feeds Feeds | THR-03 | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls. | 5 | |
| 7.4(b) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Cybersecurity & Data Protection-Minded Workforce | SAT-01 | Mechanisms exist to facilitate the implementation of security workforce development and awareness controls. | 10 | |
| 7.4(b) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Cybersecurity & Data Protection Awareness Training | SAT-02 | Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function. | 5 | |
| 7.4(b) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 7.4(b) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Threat Intelligence Feeds Feeds | THR-03 | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls. | 5 | |
| 7.4(c) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Cybersecurity & Data Protection Awareness Training | SAT-02 | Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function. | 5 | |
| 7.4(c) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Cybersecurity & Data Protection-Minded Workforce | SAT-01 | Mechanisms exist to facilitate the implementation of security workforce development and awareness controls. | 10 | |
| 7.4(c) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Threat Intelligence Feeds Feeds | THR-03 | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, tachniques and procedures to facilitate the implementation of preventative and compensating controls. | 5 | |
| 7.4(c) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 7.4(d) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Cybersecurity & Data Protection Awareness Training | SAT-02 | Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function. | 5 | |
| 7.4(d) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Threat Intelligence Feeds Feeds | THR-03 | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls. | 5 | |
| 7.4(d) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Cybersecurity & Data Protection-Minded Workforce | SAT-01 | Mechanisms exist to facilitate the implementation of security workforce development and awareness controls. | 10 | |
| 7.4(d) | Communication | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 7.5 | Documented information | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | no relationship | N/A Publishing Cybersecurity | N/A | N/A Mechanisms exist to establish, maintain and disseminate cybersecurity | N/A | This is merely a section title without content. |
| 7.5.1 | General | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | & Data Protection Documentation Publishing Cybersecurity | GOV-02 | and data protection policies, standards and procedures. Mechanisms exist to establish, maintain and disseminate cybersecurity | 5 | |
| 7.5.1(a) | General | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | & Data Protection Documentation | GOV-02 | and data protection policies, standards and procedures. | 5 | |
| 7.5.1(b) | General | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. Mechanisms exist to review the cybersecurity and data protection program, | 5 | |
| 7.5.2 | Creating and updating | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Periodic Review & Update of Cybersecurity & Data Protection Program | GOV-03 | including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | 5 | |
| 7.5.2 | Creating and updating | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 7.5.2(a) | Creating and updating | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Periodic Review & Update of Cybersecurity & Data Protection Program | GOV-03 | Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | 5 | |
| 7.5.2(a) | Creating and updating | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 7.5.2(b) | Creating and updating | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Periodic Review & Update of Cybersecurity & Data Protection Program | GOV-03 | Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | 5 | |
| 7.5.2(b) | Creating and updating | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 7.5.2(c) | Creating and updating | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 7.5.2(c) | Creating and updating | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Periodic Review & Update of Cybersecurity & Data Protection Program | GOV-03 | Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | 5 | |
| 7.5.3 | Control of documented information | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 7.5.3(a) | Control of documented information | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 7.5.3(b) | Control of documented information | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 7.5.3(c) | Control of documented information | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |



| FDE# | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF# | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes (optional) |
|-----------------|--|--|--------------------------|------------------------------|--|--------------------|---|-----------------------------|---|
| 7.5.3(d) | Control of documented information | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Publishing Cybersecurity & Data Protection | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | (optional) 5 | |
| 7.5.3(e) | Control of documented | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Documentation Publishing Cybersecurity & Data Protection | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures. | 5 | |
| 7.5.3(f) | information Control of documented | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Documentation Publishing Cybersecurity & Data Protection | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity | 5 | |
| 7.5.3(T) 8.0 | information | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | | | Documentation N/A | N/A | and data protection policies, standards and procedures. | N/A | This is merely a section title without content. |
| 8.0 | | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional Functional | no relationship subset of | Operations Security | OPS-01 | N/A Mechanisms exist to facilitate the implementation of operational security | 10 | |
| 8.1 | | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | subset of | Cybersecurity & Data Protection Governance | GOV-01 | controls. Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. | 10 | |
| 8.1 | | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Program Cybersecurity & Data Protection Controls | CPL-02 | Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership. | 5 | |
| | control Operational planning and | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | | | Oversight Standardized Operating | | Mechanisms exist to identify and document Standardized Operating | | |
| 8.1 | control | https://www.iso.org/standard/27001 | Functional | intersects with | Procedures (SOP) | OPS-01.1 | Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks. Mechanisms exist to regularly review processes and documented | 5 | |
| 8.1 | Operational planning and control | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Cybersecurity & Data Protection Assessments | CPL-03 | procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements. | 5 | |
| 8.1 | Operational planning and control | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Service Delivery (Business Process Support) | OPS-03 | Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area. | 5 | |
| 8.2 | Information security risk assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Risk Assessment | RSK-04 | Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Te | 5 | |
| 8.2 | assessment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | subset of | Risk Management Program | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to remediate risks to an acceptable level. | 10 | |
| 8.3 | treatment Information security risk | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional Functional | intersects with | Risk Remediation Risk Response | RSK-06 RSK-06.1 | Mechanisms exist to respond to findings from cybersecurity and data protection assessments, incidents and audits to ensure proper | 5 | |
| 9.0 | treatment Performance evaluation | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | no relationship | N/A | N/A | remediation has been performed. N/A | N/A | This is merely a section title without content. |
| | Monitoring, | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | | | N/A Status Reporting To | | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about | | |
| 9.1 | measurement, analysis and evaluation | https://www.iso.org/standard/27001 | Functional | intersects with | Governing Body | GOV-01.2 | matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 9.1 | Monitoring, measurement, analysis and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Cybersecurity & Data Protection Assessments | CPL-03 | Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements. | 5 | |
| 9.1 | Monitoring, measurement, analysis and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Non-Compliance Oversight | CPL-01.1 | Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. | 5 | |
| 9.1 | Monitoring, measurement, analysis and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 10 | |
| 9.1 | Monitoring, measurement, analysis and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Cybersecurity & Data Protection Controls Oversight | CPL-02 | Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership. | 5 | |
| 9.1 | Monitoring, measurement, analysis and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Measures of Performance | GOV-05 | Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance. | 5 | |
| 9.1(a) | Monitoring, measurement, analysis and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Measures of Performance | GOV-05 | Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance. | 5 | |
| 9.1(a) | Monitoring, measurement, analysis and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 9.1(a) | Monitoring, measurement, analysis and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Cybersecurity & Data Protection Assessments | CPL-03 | Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements. | 5 | |
| 9.1(a) | Monitoring, measurement, analysis and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Non-Compliance Oversight | CPL-01.1 | Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. | 5 | |
| 9.1(b) | Monitoring, measurement, analysis and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 9.1(b) | Monitoring, measurement, analysis | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Measures of Performance | GOV-05 | Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance. | 5 | |
| 9.1(b) | and evaluation Monitoring, measurement, analysis | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Non-Compliance Oversight | CPL-01.1 | Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop | 5 | |
| 9.1(b) | and evaluation Monitoring, measurement, analysis and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Cybersecurity & Data Protection Assessments | CPL-03 | appropriate risk mitigation actions. Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements. | 5 | |
| 9.1(c) | Monitoring, measurement, analysis | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Measures of Performance | GOV-05 | Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance. | 5 | |
| 9.1(c) | and evaluation Monitoring, measurement, analysis | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Non-Compliance Oversight | CPL-01.1 | Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop | 5 | |
| 9.1(c) | and evaluation Monitoring, measurement, analysis and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Cybersecurity & Data Protection Assessments | CPL-03 | appropriate risk mitigation actions. Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements. | 5 | |
| 9.1(c) | Monitoring, measurement, analysis and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data | 5 | |
| 9.1(d) | Monitoring, measurement, analysis and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | protection program. Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data | 5 | |
| 9.1(d) | Monitoring, measurement, analysis | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Non-Compliance Oversight | CPL-01.1 | protection program. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. | 5 | |
| 9.1(d) | and evaluation Monitoring, measurement, analysis | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Cybersecurity & Data | CPL-03 | appropriate risk mitigation actions. Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements. | 5 | |
| | and evaluation Monitoring, | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | | | Protection Assessments Measures of | | data protection policies, standards and other applicable requirements. Mechanisms exist to develop, report and monitor cybersecurity and data | | |
| 9.1(d) | measurement, analysis and evaluation Monitoring, | https://www.iso.org/standard/27001 | Functional | intersects with | Performance | GOV-05 | protection program measures of performance. Mechanisms exist to develop, report and monitor cybersecurity and data | 5 | |
| 9.1(e) | measurement, analysis and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Measures of Performance | GOV-05 | protection program measures of performance. | 5 | |



| 9.1(e) meaa a a a a a a a a a a a a a a a a a | and evaluation Monitoring, easurement, analysis and evaluation Monitoring, easurement analysis | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Rationale | Relationship intersects with | | | Control Description Mechanisms exist to provide governance oversight reporting and | (optional) | |
|--|--|---|------------|------------------------------|---|----------|--|------------|---|
| 9.1(e) mean (1) 9.1(f) mean (2) 1.1(f) 1.1(| Monitoring, easurement, analysis and evaluation Monitoring, easurement, analysis | | | IIILEISECIS WILII | Status Reporting To Governing Body | GOV-01.2 | recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data | 5 | |
| 9.1(e) mean | and evaluation Monitoring, easurement, analysis | | Functional | | Cybersecurity & Data | CPL-03 | Protection program. Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and | 5 | |
| 9.1(f) meas | easurement, anatysis | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | | intersects with | Protection Assessments Non-Compliance | | data protection policies, standards and other applicable requirements. Mechanisms exist to document and review instances of non-compliance | | |
| 8 | Monitoring, | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Oversight | CPL-01.1 | with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to regularly review processes and documented | 5 | |
| 9.1(f) meas | and evaluation | https://www.iso.org/standard/27001 | Functional | intersects with | Cybersecurity & Data Protection Assessments | CPL-03 | procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements. Mechanisms exist to provide governance oversight reporting and | 5 | |
| , | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| | and evaluation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Measures of Performance | GOV-05 | Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance. | 5 | |
| | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Non-Compliance Oversight | CPL-01.1 | Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop | 5 | |
| | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | no relationship | N/A | N/A | appropriate risk mitigation actions. N/A | N/A | This is merely a section title without content. |
| 9.2.1 | | Buy a copy of ISO 27001 for control content: | Functional | subset of | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of | 10 | |
| 9.2.1 | Ganaral | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Internal Audit Function | CPL-02.1 | relevant statutory, regulatory and contractual controls. Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information | 5 | |
| 9.2.1(a)(1) | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Internal Audit Function | CPL-02.1 | governance processes. Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information | 5 | |
| 9.2.1(a)(2) | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Internal Audit Function | CPL-02.1 | sovernance processes. Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information | 5 | |
| 9.2.1(b) | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Internal Audit Function | CPL-02.1 | governance processes. Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information | 5 | |
| 9.2.2 Intern | | Buy a copy of ISO 27001 for control content: | Functional | subset of | Statutory, Regulatory & | CPL-01 | governance processes. Mechanisms exist to facilitate the identification and implementation of | 10 | |
| 9.2.2 Intern | rnal audit programme | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Contractual Compliance Monitor Controls | GOV-15.5 | relevant statutory, regulatory and contractual controls. Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications and/or Services (TAAS) under their control on an ongoing basis for applicable threats and risks, as well as to ensure oppersecurity and data protection controls are operating as intended. | 3 | |
| 9.2.2 Intern | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Internal Audit Function | CPL-02.1 | Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information | 5 | |
| 9.2.2(a) Intern | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Internal Audit Function | CPL-02.1 | governance processes. Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes. | 5 | |
| 9.2.2(b) Intern | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Internal Audit Function | CPL-02.1 | Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information | 5 | |
| 9.2.2(c) Intern | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Internal Audit Function | CPL-02.1 | governance processes. Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes. | 5 | |
| 9.3 Ma | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | no relationship | N/A | N/A | N/A | N/A | This is merely a section title without content. |
| 9.3.1 | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 9.3.1 | General | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data | 5 | |
| 9.3.2(a) | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | protection program. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 9.3.2(a) | danagement review inputs | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 9.3.2(b) Ma | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 9.3.2(b) | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 9.3.2(c) Ma | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 9.3.2(c) | Management review inputs | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 9.3.2(d) | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 9.3.2(d) Ma | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 9.3.2(d)(1) | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 9.3.2(d)(1) | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 9.3.2(d)(2) | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 9.3.2(d)(2) | | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |



| FDE# | FDE Name | FI D | STRM | STRM | SCF Control | SCF# | Secure Controls Framework (SCF) | Strength of | NI-1 (1) |
|---|---|---|--|---|---|--|--|--|---|
| FDE# | FDE Name | Focal Document Element (FDE) Description | Rationale | Relationship | SCF Control | SCF# | Control Description | Relationship (optional) | Notes (optional) |
| 9.3.2(d)(3) | Management review inputs | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 9.3.2(d)(3) | Management review inputs | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 9.3.2(d)(4) | Management review inputs | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 9.3.2(d)(4) | Management review inputs | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 9.3.2(e) | Management review inputs | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 9.3.2(e) | Management review inputs | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 9.3.2(f) | Management review inputs | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 9.3.2(f) | Management review inputs | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 9.3.2(g) | Management review inputs | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 9.3.2(g) | Management review inputs | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program. | 5 | |
| 9.3.3 | Management review results | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Steering Committee & Program Oversight | GOV-01.1 | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | |
| 9.3.3 | Management review results | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Status Reporting To Governing Body | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data | 5 | |
| I . | | | | | | | protection program. | | |
| 10.0 | Improvement | Buy a copy of ISO 27001 for control content: | Functional | no relationship | N/A | N/A | protection program. N/A | N/A | This is merely a section title without content. |
| 10.0 | Improvement Continual improvement | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | no relationship | N/A Cybersecurity & Data Protection Governance Program | N/A GOV-01 | | N/A 10 | This is merely a section title without content. |
| | | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | | | Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Controls | | N/A Mechanisms exist to facilitate the implementation of cybersecurity and | | This is merely a section title without content. |
| 10.1 | Continual improvement | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | subset of | Cybersecurity & Data Protection Governance Program Cybersecurity & Data | GOV-01 | N/A Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to provide a cybersecurity and data protection controls | 10 | This is merely a section title without content. |
| 10.1 | Continual improvement Continual improvement | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | subset of intersects with | Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Controls Oversight Steering Committee & | GOV-01 CPL-02 | N/A Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to provide a cybersecurity and data protection controls overlight function that reports to the organization's executive leadership. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key Cybersecurity, data privies and business executives. | 10 | This is merely a section title without content. |
| 10.1 | Continual improvement Continual improvement Continual improvement Nonconformity and | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional Functional Functional | subset of intersects with intersects with | Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Controls Oversight Steering Committee & Program Oversight Non-Compliance | GOV-01 CPL-02 GOV-01.1 | N/A Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop | 5 | This is merely a section title without content. |
| 10.1 | Continual improvement Continual improvement Continual improvement Nonconformity and corrective action Nonconformity and | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional Functional Functional | subset of intersects with intersects with intersects with | Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Controls Oversight Steering Committee & Program Oversight Non-Compliance Oversight Non-Compliance | GOV-01 CPL-02 GOV-01.1 | N/A Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis, which meets formally and on a regular basis. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate fast mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop | 10 5 5 | This is merely a section title without content. |
| 10.1 10.1 10.1 10.2 | Continual improvement Continual improvement Continual improvement Nonconformity and corrective action Nonconformity and corrective action Nonconformity and | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional Functional Functional Functional | subset of intersects with intersects with intersects with intersects with | Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Controls Oversight Steering Committee & Program Oversight Non-Compliance Oversight Non-Compliance Oversight Non-Compliance Oversight | GOV-01 CPL-02 GOV-01.1 CPL-01.1 | N/A Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. | 10 5 5 5 | This is merely a section title without content. |
| 10.1 10.1 10.1 10.2 10.2(a) | Continual improvement Continual improvement Continual improvement Nonconformity and corrective action Nonconformity and corrective action Nonconformity and corrective action | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional Functional Functional Functional Functional | subset of intersects with intersects with intersects with intersects with intersects with | Cybersecurity & Data Protection Governance Protestion Cybersecurity & Data Protection Controls Oversight Steering Committee & Program Oversight Non-Compliance Oversight Non-Compliance Oversight Non-Compliance Oversight Non-Compliance Oversight Non-Compliance | GOV-01 CPL-02 GOV-01.1 CPL-01.1 CPL-01.1 | N/A Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. | 10 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 | This is merely a section title without content. |
| 10.1 10.1 10.1 10.2 10.2(a) 10.2(a)(1) 10.2(a)(2) | Continual improvement Continual improvement Continual improvement Nonconformity and corrective action | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional Functional Functional Functional Functional Functional Functional | subset of intersects with intersects with intersects with intersects with intersects with intersects with | Cybersecurity & Data Protection Governance Profess Cybersecurity & Data Protection Controls Oversight Steering Committee & Program Oversight Non-Compliance Oversight | GOV-01 CPL-02 GOV-01.1 CPL-01.1 CPL-01.1 | N/A Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. | 10 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 | This is merely a section title without content. |
| 10.1 10.1 10.2 10.2(a) 10.2(a)(1) 10.2(a)(2) | Continual improvement Continual improvement Continual improvement Nonconformity and corrective action | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional Functional Functional Functional Functional Functional Functional Functional | subset of intersects with | Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Controls Oversight Steering Committee & Program Oversight Non-Compliance Oversight | GOV-011 CPL-02 GOV-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 | N/A Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which mests formally and on a regulate hasis. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. | 10 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 | This is merely a section title without content. |
| 10.1 10.1 10.1 10.2 10.2(a) 10.2(a)(1) 10.2(a)(2) 10.2(b)(1) | Continual improvement Continual improvement Continual improvement Nonconformity and corrective action | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional Functional Functional Functional Functional Functional Functional Functional Functional | subset of intersects with | Cybersecurity & Data Protection Governance Profess Cybersecurity & Data Protection Controls Oversight Steering Committee & Program Oversight Non-Compliance Oversight | GOV-01 CPL-02 GOV-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop a | 10 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 | This is merely a section title without content. |
| 10.1 10.1 10.1 10.2 10.2(a)(1) 10.2(a)(2) 10.2(b)(1) 10.2(b)(1) | Continual improvement Continual improvement Continual improvement Nonconformity and corrective action | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of intersects with | Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Controls Oversight Steering Committee & Program Oversight Non-Compliance | GOV-01 CPL-02 GOV-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a testing committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which mests formally and on a regular basis. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop sopropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop sopropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop ap | 10 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 | This is merely a section title without content. |
| 10.1 10.1 10.1 10.2 10.2(a) 10.2(a)(1) 10.2(a)(2) 10.2(b)(1) 10.2(b)(1) 10.2(b)(3) | Continual improvement Continual improvement Continual improvement Nonconformity and corrective action | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of intersects with | Cybersecurity & Data Protection Governance Profess Cybersecurity & Data Protection Governance Profess Cybersecurity & Data Protection Controls Oversight Non-Compliance Oversight | GOV-01 CPL-02 GOV-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop a | 10 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 | This is merely a section title without content. |
| 10.1 10.1 10.1 10.2 10.2(a)(1) 10.2(a)(2) 10.2(b)(1) 10.2(b)(1) 10.2(b)(3) 10.2(c) | Continual improvement Continual improvement Continual improvement Nonconformity and corrective action | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of intersects with | Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Controls Oversight Steering Committee & Program Oversight Non-Compliance | GOV-01 CPL-02 GOV-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, whilch mests formally and on a regular basis. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop | 10 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 | This is merely a section title without content. |
| 10.1 10.1 10.1 10.2 10.2(a) 10.2(a)(1) 10.2(b)(1) 10.2(b)(1) 10.2(b)(2) 10.2(b)(3) 10.2(c) 10.2(d) | Continual improvement Continual improvement Continual improvement Nonconformity and corrective action | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional Functional | subset of intersects with | Cybersecurity & Data Protection Governance Protestan Cybersecurity & Data Protection Controls Coversight Steering Committee & Program Oversight Non-Compliance Oversight | GOV-01 CPL-02 GOV-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 CPL-01.1 | Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls. Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop a | 10 | This is merely a section title without content. |

ISO 27001:2022

