version 2025.2 6/26/2025

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2025.2
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm

Focal Document: ISO 27001:2022
Focal Document URL: https://www.iso.org/standard/27001
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-general-iso-27001-2022.pdf

| 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) |
|--------|--|--|-------------------|----------------------|--|----------|--|---|--|
| 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 | 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 push 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 systems, applications and services 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 systems, applications and services to support the ongoing secure management of those assets. | 5 | |
| 4.2(b) | Understanding the needs and expectations of | 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 | 5 | |
| 4.2(c) | interested parties 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 | internal control system. 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 | Internal control system. 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 | 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 & data privacy controls that are determined to meet statutory, regulatory | 5 | |
| 4.3 | management system 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 | and/or contractual compliance obligations. Mechanisms exist to determine cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and | 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 | personnel (Internal and third-parties). Mechanisms exist to document and validate the scope of cybersecurity & data privacy 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 & data privacy 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 & data privacy controls between internal stakeholders and External Service Providers (ESP). | 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 & data privacy 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 & 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 Program | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity & 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 | 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. | 10 | |
| 5.1 | Leadership and commitment | 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 | |
| 5.1(a) | Leadership and commitment | 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 & data protection policies, standards and procedures. | 5 | |
| 5.1(a) | Leadership and commitment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Documentation Cybersecurity & Data Protection Governance Program | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. | 10 | |
| 5.1(b) | 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 Program | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. | 10 | |
| 5.1(c) | Leadership and commitment | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Cybersecurity & Data Privacy Resource Management | PRM-02 | Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity & data privacy 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 | Cybersecurity & Data Protection Governance Program | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity & 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 | Cybersecurity & Data Protection Governance Program | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity & 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 | Cybersecurity & Data Protection Governance Program | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity & 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 | Cybersecurity & Data Privacy Portfolio Management | PRM-01 | Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives. | 10 | |
| 5.1(f) | Leadership and commitment | 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 & data protection program. | 5 | |
| 5.1(f) | 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 Program | GOV-01 | Mechanisms exist to facilitate the implementation of cybersecurity & 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) |
|--|---|---|--|---|---|--|--|--|--|
| 5440 | Leadership and | Buy a copy of ISO 27001 for control content: | | | Cybersecurity & Data | 001104 | Mechanisms exist to facilitate the implementation of cybersecurity & | (optional) | |
| 5.1(g) 5.1(h) | commitment Leadership and | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional Functional | subset of | Protection Governance Program Cybersecurity & Data Protection Governance | GOV-01 | data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. | 10 | |
| 5.1(h) | commitment Leadership and | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Program Assigned Cybersecurity & Data Protection | GOV-04 | Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, | 5 | |
| | commitment | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | | | Responsibilities Publishing Cybersecurity | | implement and maintain an enterprise-wide cybersecurity & data protection program. Mechanisms exist to establish, maintain and disseminate cybersecurity | | |
| 5.2 | Policy | https://www.iso.org/standard/27001 | Functional | intersects with | & Data Protection Documentation Publishing Cybersecurity | GOV-02 | & data protection policies, standards and procedures. Mechanisms exist to establish, maintain and disseminate cybersecurity | 5 | |
| 5.2(a) | Policy | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | & Data Protection Documentation | GOV-02 | & 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 & data protection policies, standards and procedures. Mechanisms exist to establish control objectives as the basis for the | 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 Publishing Cybersecurity | GOV-09 | Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system. Mechanisms exist to establish, maintain and disseminate cybersecurity | 5 | |
| 5.2(c) | Policy | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | & Data Protection Documentation | GOV-02 | & 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 & 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 & 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 & 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 & 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, | 5 | |
| 5.3 | Organizational roles, responsibilities and | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Assigned Cybersecurity & Data Protection | GOV-04 | which meets formally and on a regular basis. 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 & data | 5 | |
| 5.3 | authorities Organizational roles, responsibilities and | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Responsibilities Defined Roles & Responsibilities | HRS-03 | protection program. Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 5 | |
| | authorities Organizational roles, | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | | | Steering Committee & | | Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, | | |
| 5.3(a) | responsibilities and authorities | https://www.iso.org/standard/27001 | Functional | intersects with | Program Oversight | GOV-01.1 | comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. Mechanisms exist to assign one or more qualified individuals with the | 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 | mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program. | 5 | |
| 5.3(b) | Organizational roles, responsibilities and | Buy a copy of ISO 27001 for control content: | F | | Assigned Cybersecurity & | 001104 | Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, | - | |
| 0.0(0) | authorities | https://www.iso.org/standard/27001 | Functional | intersects with | Data Protection Responsibilities | GOV-04 | implement and maintain an enterprise-wide cybersecurity & data | 5 | |
| 5.3(b) | | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | | GOV-04 | 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, | 5 | |
| | authorities Organizational roles, responsibilities and | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | | | Responsibilities Steering Committee & | | protection program. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, | | This is merely a section title without content. |
| 5.3(b) | authorities Organizational roles, responsibilities and authorities Planning Actions to address risks | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 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 | Responsibilities 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 opbersecurity, data privacy and business executives, which meets formally and on a regular basis. | 5 | This is merely a section title without content. This is merely a section title without content. |
| 5.3(b) 6.0 | authorities Organizational roles, responsibilities and authorities Planning | Buy a copy of ISO 27001 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 | intersects with | Responsibilities Steering Committee & Program Oversight N/A N/A Risk Management Program | GOV-01.1 N/A | protection program. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key opbersecurity, data privacy and business executives, which meets formally and on a regular basis. N/A N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | 5 N/A | |
| 5.3(b) 6.0 6.1 | authorities Organizational roles, responsibilities and authorities Planning Actions to address risks and opportunities Actions to address risks | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy 150 27001 for control content: | Functional Functional | intersects with no relationship no relationship | Responsibilities Steering Committee & Program Oversight N/A N/A Risk Management Program Cybersecurity & Data Protection Governance Program | GOV-01.1 N/A N/A | 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. N/A N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. | 5 N/A N/A | |
| 5.3(b) 6.0 6.1 6.1.1 | authorities Organizational roles, responsibilities and authorities Planning 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 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 | intersects with no relationship no relationship subset of | Responsibilities Steering Committee & Program Oversight N/A N/A N/A Risk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Protection Governance | GOV-01.1 N/A N/A RSK-01 | 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. N/A N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | 5 N/A N/A 10 | |
| 5.3(b) 6.0 6.1 6.1.1 | authorities Organizational roles, responsibilities and authorities Planning 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: | Functional Functional Functional Functional | intersects with no relationship no relationship subset of | Responsibilities Steering Committee & Program Oversight N/A N/A Risk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Risk Management Program | GOV-01.1 N/A N/A RSK-01 GOV-01 | protection program. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key (operacurity, data privacy and business executives, which meets formally and on a regular basis. N/A N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Machanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of sybersecurity & data protection governance controls. | 5 N/A N/A 10 | |
| 5.3(b) 6.0 6.1 6.1.1 6.1.1 | authorities Organizational roles, responsibilities and authorities Planning 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: | Functional Functional Functional Functional Functional | intersects with no relationship no relationship subset of subset of | Responsibilities Steering Committee & Program Oversight N/A N/A N/A N/A N/A Risk Management Program Cybersecurity & Data Protection Governance Program Protes Governance Program Risk Management | GOV-01.1 N/A N/A RSK-01 GOV-01 | 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. N/A N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. | 5 N/A N/A 10 10 | |
| 5.3(b) 6.0 6.1 6.1.1 6.1.1 6.1.1 6.1.1(a) | authorities Organizational roles, responsibilities and authorities Planning 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: | Functional Functional Functional Functional Functional Functional | intersects with no relationship no relationship subset of subset of | Responsibilities Steering Committee & Program Oversight N/A N/A Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Profesen Risk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Risk Management Program Risk Management Program Risk Management Program | GOV-01.1 N/A N/A RSK-01 GOV-01 RSK-01 | protection program. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key Opersecurity, data privacy and business executives, which meets formally and on a regular basis. N/A N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Machanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Machanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Machanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operations and tactical risk management controls. | 5 N/A N/A 10 10 | |
| 5.3(b) 6.0 6.1 6.1.1 6.1.1 6.1.1 6.1.1(a) 6.1.1(a) | authorities Organizational roles, responsibilities and authorities Planning 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: | Functional Functional Functional Functional Functional Functional Functional | intersects with no relationship no relationship subset of subset of subset of subset of | Responsibilities Steering Committee & Program Oversight N/A N/A Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Risk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Risk Management Program Risk Management Program Risk Management Program | GOV-01.1 N/A N/A RSK-01 GOV-01 RSK-01 GOV-01 | 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. N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & 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 & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. | 5 N/A N/A 10 10 10 10 10 10 10 | |
| 5.3(b) 6.0 6.1 6.1.1 6.1.1 6.1.1(a) 6.1.1(b) | authorities Organizational roles, responsibilities and authorities Planning Actions to address risks and opportunities | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 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 | intersects with no relationship no relationship subset of subset of subset of subset of subset of | Responsibilities Steering Committee & Program Oversight N/A N/A Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Protection Governance Program Risk Management Program Risk Management Program Risk Management Program Risk Management Program Risk Management Program Risk Management Program Risk Management Program Risk Management Program Risk Management Program Risk Management Program Risk Management Program Risk Management Program | GOV-01.1 N/A N/A RSK-01 GOV-01 GOV-01 RSK-01 GOV-01 | 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. N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & 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 sybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of sybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of sybersecurity & data protection governance controls. | 5 N/A N/A 10 10 10 10 10 10 10 10 10 10 | |
| 5.3(b) 6.0 6.1 6.1.1 6.1.1 6.1.1(a) 6.1.1(a) 6.1.1(b) 6.1.1(b) | authorities Organizational roles, responsibilities and authorities Planning 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: | Functional | intersects with no relationship no relationship subset of subset of subset of subset of subset of subset of | Responsibilities Steering Committee & Program Oversight N/A Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Risk Management Program Gybersecurity & Data Protection Governance Program Risk Management Program Gybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Risk Management | GOV-01.1 N/A N/A RSK-01 GOV-01 RSK-01 GOV-01 GOV-01 | protection program. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key opbersecurity, data privacy and business executives, which meets formally and on a regular basis. N/A N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Machanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & 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 & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & 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 & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. | 5 N/A N/A 10 10 10 10 10 10 10 10 10 10 10 10 10 | |
| 5.3(b) 6.0 6.1 6.1.1 6.1.1 6.1.1(a) 6.1.1(b) 6.1.1(b) 6.1.1(c) | authorities Organizational roles, responsibilities and authorities Planning 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 | Functional | intersects with no relationship no relationship subset of | Responsibilities Steering Committee & Program Oversight N/A N/A Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Frogram Risk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Risk Management Program Risk Management Protection Governance Program Risk Management Protection Governance Program Risk Management Protection Governance Risk Management Program Cybersecurity & Data | GOV-01.1 N/A N/A RSK-01 GOV-01 GOV-01 RSK-01 GOV-01 RSK-01 RSK-01 RSK-01 | protection program. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key (potenscurity, data privacy and business executives, which meets formally and on a regular basis. N/A N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & 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 & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. | 5 N/A N/A 10 10 10 10 10 10 10 10 10 10 10 10 10 | |
| 5.3(b) 6.0 6.1 6.1.1 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) | authorities Organizational roles, responsibilities and authorities Planning Actions to address risks and opportunities | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 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 | intersects with no relationship no relationship subset of | Responsibilities Steering Committee & Program Oversight N/A N/A N/A N/A N/A N/A Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Risk Management Program Gybersecurity & Data Protection Governance Program Risk Management | GOV-01.1 N/A N/A RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 | 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. N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & 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, operations and ractical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operations and ractical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operations and soperance controls. | 5 N/A N/A 10 10 10 10 10 10 10 10 10 10 10 10 10 | |
| 5.3(b) 6.0 6.1 6.1.1 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) | authorities Organizational roles, responsibilities and authorities Planning 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 | intersects with no relationship no relationship subset of | Responsibilities Steering Committee & Program Oversight N/A N/A Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Risk Management Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program | GOV-01.1 N/A | 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. N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of sybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of sybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of sybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of sybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. | 5 N/A N/A 10 10 10 10 10 10 10 10 10 10 10 10 10 | |
| 5.3(b) 6.0 6.1 6.1.1 6.1.1 6.1.1(a) 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) | authorities Organizational rolea, responsibilities and authorities Planning 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 | intersects with no relationship no relationship subset of | Responsibilities Steering Committee & Program Oversight N/A N/A Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data | GOV-01.1 N/A N/A RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 | protection program. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key (operacurity, data privacy and business executives, which meets formally and on a regular basis. N/A N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & 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 & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. | 5 N/A N/A 10 10 10 10 10 10 10 10 10 10 10 10 10 | |
| 5.3(b) 6.0 6.1 6.1.1 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) | authorities Organizational roles, responsibilities and authorities Planning 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 | intersects with no relationship no relationship subset of | Responsibilities Steering Committee & Program Oversight N/A N/A Risk Management Program Cybersecurity & Data Protection Governance Program Gish Management Program Gish Management Program Gish Management Program Risk Management Protection Governance Program Risk Management Program Gybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management | GOV-01.1 N/A N/A RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 RSK-01 RSK-01 RSK-01 RSK-01 | 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. N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & 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, operations all actical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operations and actical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operations and actical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operations and and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. | 5 NVA NVA 10 10 10 10 10 10 10 10 10 10 10 10 10 | |
| 5.3(b) 6.0 6.1 6.1.1 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) | authorities Organizational roles, responsibilities and authorities Planning Actions to address risks and opportunities | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 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 | intersects with no relationship no relationship subset of | Responsibilities Steering Committee & Program Oversight N/A N/A Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Risk Management Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Risk Management Risk Management Risk Management Risk Management Risk Management | GOV-01.1 N/A N/A RSK-01 GOV-01 RSK-01 GOV-01 | protection program. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key (potenscurity, data privacy and business executives, which meets formally and on a regular basis. N/A N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of sybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of sybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of sybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of sybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementa | 5 N/A N/A 10 10 10 10 10 10 10 10 10 10 10 10 10 | |
| 5.3(b) 6.0 6.1 6.1.1 6.1.1 6.1.1(a) 6.1.1(b) 6.1.1(b) 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) 6.1.1(e)(1) | authorities Organizational roles, responsibilities and authorities Planning 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 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 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 | intersects with no relationship no relationship subset of | Responsibilities Steering Committee & Program Oversight N/A N/A Risk Management Program Cybersecurity & Data Protection Governance Program Gybersecurity & Data Protection Governance Program Gybersecurity & Data Protection Governance Program Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program | GOV-01.1 N/A N/A RSK-01 GOV-01 GOV-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 GOV-01 RSK-01 RSK-01 | 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. N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & 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 & 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, operations and actical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operations and actical 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 & data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and actical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and actical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and actical risk management controls. Mechanisms exist to facilitate the implementation of strategic, operational and act | 5 N/A N/A 10 10 10 10 10 10 10 10 10 10 10 10 10 | |
| 5.3(b) 6.0 6.1 6.1.1 6.1.1 6.1.1(a) 6.1.1(a) 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)(1) 6.1.1(e)(2) 6.1.1(e)(2) | authorities Organizational roles, responsibilities and authorities Planning 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 Functional | intersects with no relationship no relationship subset of | Responsibilities Steering Committee & Program Oversight N/A N/A Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Risk Management | GOV-01.1 N/A N/A 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 | protection program. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key (potenscurity, data privacy and business executives, which meets formally and on a regular basis. N/A N/A Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of sybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of sybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of sybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & 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 & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to facilit | 5 N/A N/A 10 10 10 10 10 10 10 10 10 10 10 10 10 | |



| FDE# | FDE Name | Focal Document Element (FDE) Description | STRM | STRM Relationship | SCF Control | SCF# | Secure Controls Framework (SCF) | Strength of Relationship | Notes (optional) |
|-------------|---|---|------------|----------------------|---------------------------------------|----------|---|-----------------------------|------------------|
| 0.4.0(1)(4) | Information security risk | | Rationale | | Risk Management | DOM 04 | Control Description Mechanisms exist to facilitate the implementation of strategic, | (optional) | |
| 6.1.2(a)(1) | assessment | https://www.iso.org/standard/27001 | Functional | subset of | Program | RSK-01 | operational and tactical risk management controls. Mechanisms exist to identify: | 10 | |
| | | | | | | | (1) Assumptions affecting risk assessments, risk response and risk monitoring: | | |
| 6.1.2(a)(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 | |
| | assessificit | Inteps.//www.iso.org/standard/27001 | | | | | (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 tactical risk management controls. | 10 | |
| | | | | | | | Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk | | |
| | Information security risk | Buy a copy of ISO 27001 for control content: | | | | | monitoring; (2) Constraints affecting risk assessments, risk response and risk | _ | |
| 6.1.2(a)(2) | assessment | https://www.iso.org/standard/27001 | Functional | intersects with | Risk Framing | RSK-01.1 | monitoring; (3) The organizational risk tolerance; and | 5 | |
| | | | | | | | (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | | |
| | | | | | | | Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk | | |
| | Information enqurity rick | Buy a copy of ISO 27001 for control content: | | | | | monitoring; (2) Constraints affecting risk assessments, risk response and risk | | |
| 6.1.2(b) | assessment | https://www.iso.org/standard/27001 | Functional | intersects with | Risk Framing | RSK-01.1 | monitoring; | 5 | |
| | | | | | | | (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for | | |
| 6.1.2(b) | | Buy a copy of ISO 27001 for control content: | Functional | subset of | Risk Management | RSK-01 | managing risk. Mechanisms exist to facilitate the implementation of strategic, | 10 | |
| | assessment | https://www.iso.org/standard/27001 | | | Program | | operational and tactical risk management controls. Mechanisms exist to identify: | | |
| | | | | | | | (1) Assumptions affecting risk assessments, risk response and risk monitoring; | | |
| 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 | (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 | | |
| | Information security risk | Buy a copy of ISO 27001 for control content: | | | Risk Management | | managing risk. Mechanisms exist to facilitate the implementation of strategic, | | |
| 6.1.2(c) | assessment | https://www.iso.org/standard/27001 | Functional | subset of | Program | RSK-01 | operational and tactical risk management controls. Mechanisms exist to identify and document risks, both internal and | 10 | |
| 6.1.2(c) | Information security risk assessment | https://www.iso.org/standard/27001 | Functional | intersects with | Risk Identification | RSK-03 | external. | 5 | |
| | | | | | | | Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk | | |
| 6.1.2(c)(1) | Information security risk | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Risk Framing | RSK-01.1 | monitoring; (2) Constraints affecting risk assessments, risk response and risk | 5 | |
| 0.1.2(0)(1) | assessment | https://www.iso.org/standard/27001 | Tunctionat | IIIteraecta With | Noctraning | NOK-01.1 | monitoring; (3) The organizational risk tolerance; and | 5 | |
| | | | | | | | (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | | |
| 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 | Mechanisms exist to facilitate the implementation of strategic, | 10 | |
| 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 | intersects with | Risk Identification | RSK-03 | Mechanisms exist to identify and document risks, both internal and external. | 5 | |
| 6.1.2(c)(2) | Information security risk | Buy a copy of ISO 27001 for control content: | Functional | subset of | Risk Management | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, | 10 | |
| 6.1.2(c)(2) | assessment Information security risk | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Program Risk Identification | RSK-03 | operational and tactical risk management controls. Mechanisms exist to identify and document risks, both internal and | 5 | |
| | assessment | https://www.iso.org/standard/27001 | | | | | external. Mechanisms exist to identify: | | |
| | | | | | | | (1) Assumptions affecting risk assessments, risk response and risk monitoring; | | |
| 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 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 | | |
| | Information security risk | Buy a copy of ISO 27001 for control content: | | | Risk Management | | managing risk. Mechanisms exist to facilitate the implementation of strategic, | | |
| 6.1.2(d) | assessment | https://www.iso.org/standard/27001 | Functional | subset of | Program | RSK-01 | operational and tactical risk management controls. Mechanisms exist to conduct recurring assessments of risk that includes | 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 | the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's | 5 | |
| | docominic | The part will be to be a part of the part | | | | | systems and data. Mechanisms exist to identify: | | |
| | | | | | | | (1) Assumptions affecting risk assessments, risk response and risk | | |
| 6.1.2(d) | | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Risk Framing | RSK-01.1 | monitoring; (2) Constraints affecting risk assessments, risk response and risk | 5 | |
| | assessment | https://www.iso.org/standard/27001 | | | | | monitoring; (3) The organizational risk tolerance; and | | |
| | | | | | | | (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | | |
| 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 | |
| | | | - | | | | Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk | | |
| | Information security risk | Buy a copy of ISO 27001 for control content: | F | | B | no:: : | monitoring; (2) Constraints affecting risk assessments, risk response and risk | | |
| 6.1.2(d)(1) | assessment | https://www.iso.org/standard/27001 | Functional | subset of | Risk Framing | RSK-01.1 | monitoring; (3) The organizational risk tolerance; and | 10 | |
| | | | | | | | (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | | |
| | Information security risk | Buy a copy of ISO 27001 for control content: | | | | | managing risk. Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, | | |
| 6.1.2(d)(1) | assessment | https://www.iso.org/standard/27001 | Functional | intersects with | Risk Assessment | RSK-04 | disclosure, disruption, modification or destruction of the organization's | 5 | |
| | | | | | | | systems and data. Mechanisms exist to identify: | | |
| | | | | | | | (1) Assumptions affecting risk assessments, risk response and risk monitoring; | | |
| 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 | (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 | | |
| 6 4 0/40/00 | Information security risk | Buy a copy of ISO 27001 for control content: | Functional | purhant : | Risk Management | RSK-01 | managing risk. Mechanisms exist to facilitate the implementation of strategic, | 10 | |
| 6.1.2(d)(2) | assessment | https://www.iso.org/standard/27001 | ranctional | subset of | Program | 10-ACH | operational and tactical risk management controls. Mechanisms exist to conduct recurring assessments of risk that includes | 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 | the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's | 5 | |
| | | <u> </u> | | | | | systems and data. Mechanisms exist to categorize systems and data in accordance with | | |
| | Information requirity deli- | Buy a copy of ISO 27001 for control content: | | | Risk-Based Security | | applicable laws, regulations and contractual obligations that: | | |
| 6.1.2(d)(3) | Information security risk assessment | https://www.iso.org/standard/27001 | Functional | intersects with | Risk-Based Security Categorization | RSK-02 | Document the security categorization results (including supporting rationale) in the security plan for systems; and | 5 | |
| | | | | | | | (2) Ensure the security categorization decision is reviewed and approved by the asset owner. | | |
| | | | | | | | Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk | | |
| 6.1.2(d)(3) | | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Risk Framing | RSK-01.1 | monitoring; (2) Constraints affecting risk assessments, risk response and risk | 5 | |
| 0.1.2(0)(3) | assessment | https://www.iso.org/standard/27001 | runctionat | intersects with | nisk r/aming | nan-U1.1 | monitoring; (3) The organizational risk tolerance; and | 5 | |
| | | | | | | | (4) Priorities, benefits and trade-offs considered by the organization for managing risk. | | |
| 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 | subset of | Risk Management Program | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | 10 | |
| H | - GOODOOIIIBIIL | | | | riograill | | | | |



| 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(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 | 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 systems and data. | 5 | |
| 6.1.2(e) | | Buy a copy of ISO 27001 for control content: | 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 | 5 | |
| | assessment | https://www.iso.org/standard/27001 | | | | | monitoring; (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) | 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 systems and data. | 5 | |
| 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 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 systems and data. Mechanisms exist to identify: | 5 | |
| 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 | (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(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. | 10 | |
| 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 | Mechanisma exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; | 5 | |
| | Information security risk | Buy a copy of ISO 27001 for control content: | | | Risk Management | | (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk. Mechanisms exist to facilitate the implementation of strategic, | | |
| 6.1.2(e)(2) | assessment | https://www.iso.org/standard/27001 | Functional | subset of | Program | RSK-01 | operational and tactical risk management controls. Mechanisms exist to conduct recurring assessments of risk that includes | 10 | |
| 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 Assessment | RSK-04 | the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data. Mechanisms exist to respond to findings from cybersecurity & data | 5 | |
| 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 | privacy assessments, incidents and audits to ensure proper remediation has been performed. | 5 | |
| 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 Remediation | RSK-06 | Mechanisms exist to remediate risks to an acceptable level. | 5 | |
| 6.1.3(a) | 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 Response | RSK-06.1 | Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed. Mechanisms exist to remediate risks to an acceptable level. | 5 | |
| 6.1.3(a) | treatment | https://www.iso.org/standard/27001 | Functional | intersects with | Risk Remediation | RSK-06 | Mechanisms exist to respond to findings from cybersecurity & data | 5 | |
| 6.1.3(b) | | 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 | intersects with | Risk Response | RSK-06.1 RSK-06 | privacy assessments, incidents and audits to ensure proper remediation has been performed. Mechanisms exist to remediate risks to an acceptable level. | 5 | |
| 6.1.3(c) | Information security risk 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 remediate risks to an acceptable level. | 5 | |
| 6.1.3(c) | Information security risk treatment | https://www.iso.org/standard/27001 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 & data privacy assessments, incidents and audits to ensure proper remediation has been performed. | 5 | |
| 6.1.3(d) | 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 & data privacy assessments, incidents and audits to ensure proper remediation has been performed. | 5 | |
| 6.1.3(d) | 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(e) | 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. Mechanisms exist to respond to findings from cybersecurity & data | 5 | |
| 6.1.3(e) | Information security risk treatment | 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 Response | RSK-06.1 | privacy 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 | https://www.iso.org/standard/27001 | Functional | intersects with | Risk Remediation | RSK-06 | Mechanisms exist to respond to findings from cybersecurity & data | 5 | |
| 6.1.3(f) | treatment Information security | 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 Response | RSK-06.1 | privacy 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 | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects 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 | 5 | |
| 6.2(a) | 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(b) | 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(c) | 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 | | 5 | |
| 6.2(d) | 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(e) | 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(f) | objectives and planning to achieve them Information security | 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 | 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 | 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 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 | Mechanisms exist to establish control objectives as the basis for the 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(i) | 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(j) | 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(k) | 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(l) | 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 | |
| 6.3 | Planning of changes | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Change Management Program | CHG-01 | Mechanisms exist to facilitate the implementation of a change management program. | 10 | |
| 7.0 | Support | 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. |



| 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: https://www.iso.org/standard/27001 | Functional | intersects with | Cybersecurity & Data Privacy Resource | PRM-02 | Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity & data privacy programs and document all exceptions to this | (optional) 5 | |
| 7.2 | Competence | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Management Competency Requirements for Security | HRS-03.2 | requirement. 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 | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Related Positions Position Categorization | HRS-02 | Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for | 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 | HRS-03.2 | individuals filling those positions. Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set. | 5 | |
| 700 | 0 | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Related Positions Competency Requirements for Security | | Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set. | 5 | |
| 7.2(b) 7.2(b) | Competence | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Related Positions Personnel Screening | HRS-03.2 | Mechanisms exist to manage personnel security risk by screening | 5 | |
| 7.2(c) | Competence | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | Functional | intersects with | Personnel Screening | HRS-04 | individuals prior to authorizing access. Mechanisms exist to manage personnel security risk by screening | 5 | |
| 7.2(c) | Competence | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Competency Requirements for Security | HRS-03.2 | individuals prior to authorizing access. 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 | Related Positions 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: | Functional | intersects with | Use of Communications | HRS-05.3 | Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to | 5 | |
| 7.3 | Awareness | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Technology Human Resources Security Management | HRS-01 | Cause damage to systems, if used maliciously. 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 & data privacy policies and provide acknowledgement. | 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 | Mechanisms exist to define acceptable and unacceptable rules of behavior 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 | Functional | intersects with | Terms of Employment | HRS-05 | Mechanisms exist to require all employees and contractors to apply cybersecurity & data privacy principles in their daily work. | 5 | |
| 7.3 | Awareness | 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 | |
| 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 | 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(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 & data privacy principles in their daily work. | 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 | 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(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. | 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 | 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(a) | 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(a) | 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(a) | 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(a) | 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(b) | 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(b) | Awareness | 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 | |
| 7.3(b) | 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 & data privacy principles in their daily work. | 5 | |
| 7.3(b) | 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(b) | 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(b) | 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(b) | 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(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 Buy a copy of ISO 27001 for control content: | Functional Functional | intersects with | User Awareness Social Media & Social | 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 define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting | 5 | |
| 7.3(c) | | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: | | | Networking Restrictions Human Resources | | information on commercial websites and sharing account information. Mechanisms exist to facilitate the implementation of personnel security | | |
| 7.3(c) 7.3(c) | Awareness | 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 | Security Management Terms of Employment | HRS-01 HRS-05 | controls. Mechanisms exist to require all employees and contractors to apply cybersecurity & data privacy principles in their daily work. | 10 | |
| 7.3(c) | Awareness | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Policy Familiarization & | HRS-05.7 | Mechanisms exist to ensure personnel receive recurring familiarization | 5 | |
| ,.5(0) | | https://www.iso.org/standard/27001 | onolidi | Soots With | Acknowledgement | 33.7 | with the organization's cybersecurity & data privacy policies and provide acknowledgement. | | |



| 1 | 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) |
|--|----------|--------------------------|--|-------------------|----------------------|--|----------|--|-----------------------------|---|
| 1906 | 7.3(c) | Awareness | | | | Formal Indoctrination | HRS-04.2 | | (optional) | |
| | 7.3(c) | Awareness | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Use of Mobile Devices | HRS-05.5 | Mechanisms exist to manage business risks associated with permitting | 5 | |
| Part | 7.3(c) | Awareness | Buy a copy of ISO 27001 for control content: | Functional | intersects with | | HRS-05.3 | Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to | 5 | |
| Column | 7.3(c) | Awareness | Buy a copy of ISO 27001 for control content: | Functional | intersects with | | HRS-05 1 | Mechanisms exist to define acceptable and unacceptable rules of | 5 | |
| | | | , | | | | | unacceptable behavior. | | |
| 1 | | | | | | | | | | |
| 1 | 7.4 | Communication | | Functional | intersects with | Feeds | THR-03 | techniques and procedures to facilitate the implementation of preventative and compensating controls. | 5 | |
| Part | 7.4 | Communication | | Functional | subset of | Privacy-Minded | SAT-01 | | 10 | |
| Part | 7.4 | Communication | | Functional | intersects with | Status Reporting To | GOV-01.2 | recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data | 5 | |
| | 7.4 | Communication | | Functional | intersects with | Privacy Awareness | SAT-02 | Mechanisms exist to provide all employees and contractors appropriate | 5 | |
| Page Communication Commu | 7.4(a) | Communication | | Functional | intersects with | Cybersecurity & Data | SAT-02 | | 5 | |
| Part | | | | | | _ | | recommendations to those entrusted to make executive decisions about | | |
| 1.4 1.5 | 7.4(a) | Communication | | Functional | intersects with | Governing Body | GOV-01.2 | matters considered material to the organization's cybersecurity & data protection program. | 5 | |
| Part | 7.4(a) | Communication | | Functional | subset of | Privacy-Minded | SAT-01 | development and awareness controls. | 10 | |
| Antique | 7.4(a) | Communication | | Functional | intersects with | | THR-03 | and evolving threats by leveraging the knowledge of attacker tactics, | 5 | |
| | 7.4(b) | Communication | | Functional | subset of | | SAT-01 | Mechanisms exist to facilitate the implementation of security workforce | 10 | |
| Antique | | | | | | Workforce Cybersecurity & Data | | Mechanisms exist to provide all employees and contractors appropriate | | |
| | 7.4(b) | Communication | | Functional | intersects with | | SAT-02 | | 5 | |
| Community Comm | 7.4(b) | Communication | | Functional | intersects with | | GOV-01.2 | recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program. | 5 | |
| | 7.4(b) | Communication | | Functional | intersects with | | THR-03 | and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of | 5 | |
| Part | 7.4(c) | Communication | | Functional | intersects with | Privacy Awareness | SAT-02 | | 5 | |
| Professional Communication Professional C | 7.4(c) | Communication | | Functional | subset of | Cybersecurity & Data Privacy-Minded | SAT-01 | | 10 | |
| Part | 7.4(c) | Communication | | Functional | intersects with | | THR-03 | and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of | 5 | |
| Process of the Communication | 7.4(c) | Communication | | Functional | intersects with | | GOV-01.2 | recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data | 5 | |
| Part | 7.4(d) | Communication | | Functional | intersects with | Privacy Awareness | SAT-02 | | 5 | |
| Processing and special content conte | 7.4(d) | Communication | | Functional | intersects with | Threat Intelligence Feeds | THR-03 | and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of | 5 | |
| Part Communication Buy a copy of ISO 27000 for common centers: https://www.ba.org/standard/27001 Functional Interacts with State Reporting To Governing Body COV-41 A Data Protection Coverning Body CoV-42 A Data Protection Coverning Body Coverning Body CoV-42 A Data Protection Coverning Body Coverning Body CoV-42 A Data Protection Coverning Body | 7.4(d) | Communication | | Functional | subset of | Privacy-Minded | SAT-01 | Mechanisms exist to facilitate the implementation of security workforce | 10 | |
| Part | 7.4(d) | Communication | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Status Reporting To | GOV-01.2 | recommendations to those entrusted to make executive decisions about | 5 | |
| Principle Prin | 7.5 | Documented information | | Functional | no relationship | N/A | N/A | | N/A | This is merely a section title without content. |
| Process Proc | 7.5.1 | General | Buy a copy of ISO 27001 for control content: | Functional | intersects with | & Data Protection | GOV-02 | | 5 | |
| Policining Cybersecurity 2 December 18 By a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Functional intersects with Policining Cybersecurity 2 December 18 By a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Functional intersects with Policining Cybersecurity 2 December 2 De | 7.5.1(a) | General | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Publishing Cybersecurity & Data Protection | GOV-02 | | 5 | |
| Process Proc | 7.5.1(b) | General | | Functional | intersects with | Publishing Cybersecurity & Data Protection | GOV-02 | | 5 | |
| 7.5.2(a) Creating and updating Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | 7.5.2 | Creating and updating | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Periodic Review & Update of Cybersecurity & Data | GOV-03 | including policies, standards and procedures, at planned intervals or if | 5 | |
| 7.5.2(a) Creating and updating 1 | 7.5.2 | Creating and updating | | Functional | intersects with | Publishing Cybersecurity & Data Protection | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity | 5 | |
| 1.5.2(a) Creating and updating | 7500 | Constitute and the state | Buy a copy of ISO 27001 for control content: | Funetic 1 | 5-14 | Periodic Review & Update | 00110- | | | |
| 7.5.2(a) Creating and updating https://www.iso.org/standar/d27001 Functional intersects with Documentation Docum | 7.5.2(a) | Greating and updating | https://www.iso.org/standard/27001 | Functional | intersects with | Protection Program | GOV-03 | significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | 5 | |
| 7.5.2(b) Creating and updating The production of the production o | 7.5.2(a) | Creating and updating | | Functional | intersects with | & Data Protection Documentation | GOV-02 | & data protection policies, standards and procedures. | 5 | |
| Publishing Operatorial | 7.5.2(b) | Creating and updating | | Functional | intersects with | 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(c) Creating and updating The proof is 27001 for control content: https://www.iso.org/standard/27001 The proof is 27001 for control content: https://www.iso.org/stand | 7.5.2(b) | Creating and updating | | Functional | intersects with | & Data Protection | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity | 5 | |
| 7.5.2(c) Creating and updating Creating and updating https://www.iso.org/standard/27001 Functional intersects with https://www.iso.org/standard/27001 Functional intersects with intersects with intersects with procedure of Cybersecurity & Data procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policies, standards and procedures, at planned intervals or including policie | 7.5.2(c) | Creating and updating | | Functional | intersects with | Publishing Cybersecurity & Data Protection | GOV-02 | | 5 | |
| riotection riogram and effectiveness. | 7.5.2(c) | Creating and updating | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Periodic Review & Update | GOV-03 | including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy | 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 | 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 & data protection policies, standards and procedures. | (optional) 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 | Documentation Publishing Cybersecurity & Data Protection | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity & 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 | Documentation Publishing Cybersecurity & Data Protection | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity & 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 | Documentation Publishing Cybersecurity & Data Protection | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures. | 5 | |
| 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 | Documentation Publishing Cybersecurity & Data Protection | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures. | 5 | |
| 7.5.3(e) | Control of documented information | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Documentation Publishing Cybersecurity & Data Protection | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures. | 5 | |
| 7.5.3(f) | Control of documented information | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Documentation Publishing Cybersecurity & Data Protection | GOV-02 | Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures. | 5 | |
| 8.0 | Operation | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | no relationship | Documentation N/A | N/A | N/A | N/A | This is merely a section title without content. |
| 8.1 | | Buy a copy of ISO 27001 for control content: | Functional | subset of | Operations Security | OPS-01 | Mechanisms exist to facilitate the implementation of operational | 10 | |
| 8.1 | control Operational planning and control | https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | subset of | Cybersecurity & Data Protection Governance | GOV-01 | security controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. | 10 | |
| 8.1 | Operational planning and control | Buy a copy of ISO 27001 for control content: https://www.iso.org/stenderd/27001 | Functional | intersects with | Program Cybersecurity & Data Protection Controls | CPL-02 | Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership. | 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 | Oversight Standardized Operating Procedures (SOP) | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper | 5 | |
| 8.1 | | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Cybersecurity & Data Protection Assessments | CPL-03 | execution of day-to-day/ assigned tasks. Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity & data protection policies, standards and other applicable requirements. | 5 | |
| | Control | nttps://www.iso.org/standard/27001 | | | | | Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure | | |
| 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 | appropriate jackments on service images in to essain 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. Mechanisms exist to conduct recurring assessments of risk that includes | 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 | recnainsms exist to conduct recurring assessments or risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data. | 5 | |
| 8.2 | 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 | |
| 8.3 | 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 | |
| 8.3 | 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 & data privacy assessments, incidents and audits to ensure proper remediation has been performed. | 5 | |
| 9.0 | Performance evaluation | 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. |
| 9.1 | 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 & 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 & 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 & 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 & data privacy 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 & data privacy 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 | matters considered material to the organization's cybersecurity & data | 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 | protection program. Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity & 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 | 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 | Measures of Performance | GOV-05 | Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance. | 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 | 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 | Cybersecurity & Data Protection Assessments | CPL-03 | Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity & 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 | Measures of Performance | GOV-05 | Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance. | 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 | 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(c) | 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 & 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 & data protection program. | 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 | 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 & data protection program. | 5 | |



| | 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) |
|-------------|--|--|-------------------|----------------------|---|----------|---|-----------------------------|---|
| 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 | Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop | (optional) 5 | |
| 9.1(d) | 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 & data protection policies, standards and other applicable requirements. | 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 | Measures of Performance | GOV-05 | Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance. | 5 | |
| 9.1(e) | 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 & data privacy program measures of performance. | 5 | |
| 9.1(e) | 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 & data protection program. | 5 | |
| 9.1(e) | 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 & data protection policies, standards and other applicable requirements. | 5 | |
| 9.1(e) | 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(f) | 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 & data protection policies, standards and other applicable requirements. | 5 | |
| 9.1(f) | 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 & data protection program. | 5 | |
| 9.1(f) | 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 & data privacy program measures of performance. | 5 | |
| 9.1(f) | 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 appropriate risk mitigation actions. | 5 | |
| 9.2 | Internal audit | 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 | General | 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 | |
| 9.2.1 | General | 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 governance processes. | 5 | |
| 9.2.1(a)(1) | General | 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 governance processes. | 5 | |
| 9.2.1(a)(2) | General | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Internal Audit Function | CPL-02.1 | Revenience 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 | |
| 9.2.1(b) | General | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Internal Audit Function | CPL-02.1 | Recentine 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 In | Internal audit programme | 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 | |
| 9.2.2 In | Internal audit programme | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Monitor Controls | GOV-15.5 | Mechanisms exist to compel data and/or process owners to monitor systems, applications and/or services under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity & data privacy controls are operating as intended. | 3 | |
| 9.2.2 In | Internal audit programme | 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 governance processes. | 5 | |
| 9.2.2(a) In | Internal audit programme | 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 governance processes. | 5 | |
| 9.2.2(b) In | Internal audit programme | 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 governance processes. | 5 | |
| 9.2.2(c) In | Internal audit programme | 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 governance processes. | 5 | |
| 9.3 | Management review | 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 | General | 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 | matters considered material to the organization's cybersecurity & data protection program. | 5 | |
| 9.3.2(a) | 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(a) | 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 & data protection program. | 5 | |
| 9.3.2(b) | 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(b) | 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 | 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 | 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 & 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) | 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) | 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 | 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) |
|-------------|--|--|-------------------|----------------------|--|----------|---|-----------------------------|---|
| 9.3.2(d)(1) | 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 | matters considered material to the organization's cybersecurity & data | 5 | |
| 9.3.2(d)(1) | 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 | 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, | 5 | |
| 9.3.2(d)(2) | Management review | Buy a copy of ISO 27001 for control content: | Functional | intersects with | Steering Committee & | GOV-01.1 | which meets formally and on a regular basis. Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, | 5 | |
| 9.3.2(U)(2) | inputs | https://www.iso.org/standard/27001 | Functional | intersects with | Program Oversight | GOV-01.1 | comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. Mechanisms exist to provide governance oversight reporting and | 3 | |
| 9.3.2(d)(2) | 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 | recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program. Mechanisms exist to provide governance oversight reporting and | 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 | 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 & 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 | 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 | 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 | matters considered material to the organization's cybersecurity & data | 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 | 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, | 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 | which meets formally and on a regular basis. 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 | 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 & data protection program. | 5 | |
| 10.0 | Improvement | 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. |
| 10.1 | Continual improvement | 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 & data protection governance controls. | 10 | |
| 10.1 | Continual improvement | 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 & data protection controls oversight function that reports to the organization's executive leadership. Mechanisms exist to coordinate cybersecurity, data protection and | 5 | |
| 10.1 | Continual improvement | 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 | 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 | 5 | |
| 10.2 | Nonconformity and corrective action | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Non-Compliance Oversight | CPL-01.1 | with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. | 5 | |
| 10.2(a) | Nonconformity and corrective action | 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 | |
| 10.2(a)(1) | Nonconformity and corrective action | 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 | |
| 10.2(a)(2) | Nonconformity and corrective action | 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 | |
| 10.2(b) | Nonconformity and corrective action | 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. Mechanisms exist to document and review instances of non-compliance | 5 | |
| 10.2(b)(1) | Nonconformity and corrective action | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Non-Compliance Oversight | CPL-01.1 | with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. | 5 | |
| 10.2(b)(2) | Nonconformity and corrective action | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Non-Compliance Oversight | CPL-01.1 | appropriate risk mitigation actions. | 5 | |
| 10.2(b)(3) | Nonconformity and corrective action | 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. Mechanisms exist to document and review instances of non-compliance | 5 | |
| 10.2(c) | Nonconformity and corrective action | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Non-Compliance Oversight | CPL-01.1 | with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance | 5 | |
| 10.2(d) | Nonconformity and corrective action | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Non-Compliance Oversight Non-Compliance | CPL-01.1 | | 5 | |
| 10.2(e) | Nonconformity and corrective action Nonconformity and | 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 | Non-Compliance Oversight Non-Compliance | CPL-01.1 | with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance | 5 | |
| 10.2(f) | corrective action | https://www.iso.org/standard/27001 | Functional | intersects with | Oversight | | with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance | 5 | |
| 10.2(g) | Nonconformity and corrective action | Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 | Functional | intersects with | Non-Compliance Oversight | CPL-01.1 | with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. | 5 | |

