Set Theory Relationship Mapping (STRM)



Reference Document: Secure Controls Framework (SCF) version 2024.1

Focal Document: ISO 27001:2022

STRM URL: https://content.securecontrolsframework.com/strm/scf-2024-1-iso-27001-2022.pdf

Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two concepts are related:

- 1. Syntactic: How similar is the wording that expresses the two concepts? This is a word-for-word analysis of the relationship, not an interpretation of the language.
- 2. Semantic: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
- 3. Functional: How similar are the <u>results</u> of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed.

Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two distinct concepts:

- 1. Subset Of
- 2. Intersects With
- 3. Equal
- 4. Superset Of
- 5. No Relationship



Relationship Type #1:

Focal Document Element is a subset of SCF control. In other words, SCF control contains everything that Focal Document Element does and more.

Relationship Type #2: INTERSECTS WITH

SCF control has some overlap with Focal Document Element, but each includes content that the other does not.

Relationship Type #3: EQUAL

SCF control and Focal Document Element are the same, although not necessarily identical.

Relationship Type #4: SUPERSET OF

Focal Document Element is a superset of SCF control. In other words, Focal Document Element contains everything that SCF control does and more.

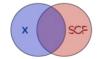
Relationship Type #5: NO RELATIONSHIP

SCF control and Focal Document Element are unrelated; their content does not overlap.



SUBSET OF

Relative Relationship Strength (control versus control)



INTERSECTS WITH

Relative Relationship Strength (control versus control)



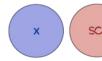
EQUAL

Relative Relationship Strength (control versus control)



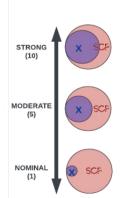
SUPERSET OF

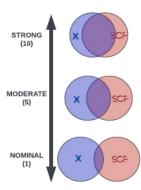
Relative Relationship Strength (control versus control)

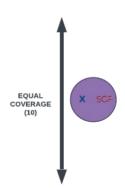


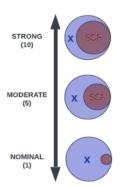
NO RELATIONSHIP

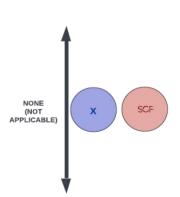
Relative Relationship Strength (control versus control)













FDE#	FDE Name	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF#	Secure Controls Framework (SCF)	Strength of Relationship	Notes (optional)
		Buy a copy of ISO 27001 for control content:	Rationale	Relationship			Control Description	(optional)	
2.0	Scope Normative references	https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content:	Functional	no relationship	N/A N/A	N/A N/A	N/A	N/A N/A	No requirements to map to.
3.0	Terms and definitions	https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content:	Functional	intersects with	Standardized Terminology	SEA-02.1	N/A Mechanisms exist to standardize technology and process terminology to	N/A	No requirements to map to.
	Context of the	https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content:					reduce confusion amongst groups and departments.	21/2	N
4.0	organization	https://www.iso.org/standard/27001	Functional	no relationship	N/A	N/A	N/A Mechanisms exist to establish control objectives as the basis for the	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	Define Control Objectives Statutory, Regulatory & Contractual Compliance	GOV-09	selection, implementation and management of the organization's internal control system. 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.
	Understanding the	Buy a copy of ISO 27001 for control content:	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	needs and expectations of interested parties	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	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 interested parties	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5	
4.2(c)	Understanding the needs and expectations of interested parties	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5	
	Determining the scope of the information	Buy a copy of ISO 27001 for control content:	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	security management system	https://www.iso.org/standard/27001	Functional	intersects with	Asset Scope Classification	AST-04.1	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 personnel (internal and third-parties).	5	
4.3(a)	Determining the scope of the information security management system	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & 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	
	Determining the scope		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 (ESPs).	5	
4.3(c)	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	
			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	
	Information security	Buy a copy of ISO 27001 for control content:	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	management system	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	$\label{lem:mechanisms} \begin{tabular}{ll} Mechanisms exist to facilitate the implementation of cybersecurity \& data protection governance controls. \end{tabular}$	10	
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 Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
		, , , , , , , , , , , , , , , , , , ,	Functional	subset of	Cybersecurity & Data Protection Governance	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	Program 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	Buy a copy of ISO 27001 for control content:	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	
	commitment	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	
	Leadership and	Buy a copy of ISO 27001 for control content:	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)	commitment	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	
			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(g)	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(h)	Leadership and	Buy a copy of ISO 27001 for control content:	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls. Mechanisms exist to assign one or more qualified individuals with the	10	
	commitment	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	
5.2	Policy	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	



3 of 11

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)
5.2(a)	Policy	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
		Buy a copy of ISO 27001 for control content:	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(b)	Policy	https://www.iso.org/standard/27001	Functional	intersects with	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5	
5.2(c)	Policy	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & 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	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. Mechanisms exist to assign one or more qualified individuals with the	5	
	authorities	intps://www.isu.org/statustu/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(a)	Organizational roles, responsibilities and	Buy a copy of ISO 27001 for control content:	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	
	authorities	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	
5.3(b)	Organizational roles, responsibilities and	Buy a copy of ISO 27001 for control content:	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	
535(5)	authorities	https://www.iso.org/standard/27001	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
6.0	Planning	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	no relationship	N/A	N/A	N/A	N/A	This is merely a section title without content.
6.1	Actions to address risks and opportunities	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	no relationship	N/A	N/A	N/A	N/A	This is merely a section title without content.
6.1.1	Actions to address risks and opportunities	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	subset of	Risk Management Program Cybersecurity & Data Protection Governance	RSK-01 GOV-01	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.	10	
6.1.1(a)	Actions to address risks and opportunities	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	subset of	Program Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
	and opportunities	nttps.//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	
6.1.1(b)		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. Mechanisms exist to facilitate the implementation of strategic,	10	
			Functional	subset of	Risk Management Program Cybersecurity & Data	RSK-01	operational and tactical risk management controls.	10	
6.1.1(c)		Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	subset of	Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
			Functional	subset of	Risk Management Program Cybersecurity & Data	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
6.1.1(d)	Actions to address risks and opportunities	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	subset of	Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
	and opportunities		Functional			_		_	
				subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
6.1.1(e)(1)		Buy a copy of ISO 27001 for control content:	Functional	subset of	Risk Management Program Cybersecurity & Data Protection Governance Program	RSK-01 GOV-01	operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
6.1.1(e)(1)	Actions to address risks and opportunities	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional		Cybersecurity & Data Protection Governance Program Risk Management Program		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.		
6.1.1(e)(1) 6.1.1(e)(2)	and opportunities Actions to address risks	https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content:		subset of	Cybersecurity & Data Protection Governance Program	GOV-01	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,	10	
	and opportunities	https://www.iso.org/standard/27001	Functional	subset of	Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance	GOV-01 RSK-01	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 cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
	and opportunities Actions to address risks and opportunities Information security	https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content:	Functional	subset of subset of	Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program	GOV-01 RSK-01 GOV-01	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 cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to identify: - Assumptions affecting risk assessments, risk response and risk monitoring; - Constraints affecting risk assessments, risk response and risk monitoring: - The organizational risk tolerance; and - Priorities, benefits and trade-offs considered by the organization for	10 10 10	
6.1.1(e)(2)	and opportunities Actions to address risks and opportunities Information security	https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content:	Functional Functional Functional	subset of subset of subset of subset of	Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program	GOV-01 RSK-01 GOV-01 RSK-01	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 cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to identify: *Assumptions affecting risk assessments, risk response and risk monitoring: *Constraints affecting risk assessments, risk response and risk monitoring: *The organizational risk tolerance; and *Priorities, benefits and trade-offs considered by the organization for managing risk. Mechanisms exist to facilitate the implementation of strategic,	10 10 10	
6.1.1(e)(2)	and opportunities Actions to address risks and opportunities Information security risk assessment	https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content:	Functional Functional Functional	subset of subset of subset of subset of intersects with	Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Protection Governance Program Risk Management Program Risk Framing	GOV-01 RSK-01 GOV-01 RSK-01	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 cybersecurity & data protection governance controls. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to identify: **Assumptions affecting risk assessments, risk response and risk monitoring: **Constraints affecting risk assessments, risk response and risk monitoring: **The organizational risk tolerance; and **Priorities, benefits and trade-offs considered by the organization for managing risk.	10 10 10 10	
6.1.1(e)(2) 6.1.2	and opportunities Actions to address risks and opportunities Information security risk assessment	https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content:	Functional Functional Functional Functional	subset of subset of subset of subset of subset of subset of	Cybersecurity & Data Protection Governance Program Risk Management Program Cybersecurity & Data Protection Governance Program Risk Management Program Risk Framing	GOV-01 RSK-01 GOV-01 RSK-01 RSK-01.1	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 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 identify: *Assumptions affecting risk assessments, risk response and risk monitoring: *The organizational risk tolerance; and *Priorities, benefits and trade-offs considered by the organization for managing risk. Mechanisms exist to facilitate the implementation of strategic, operational and atticial risk management controls. Mechanisms exist to identify: *Assumptions affecting risk assessments, risk response and risk monitoring; *Constraints affecting risk assessments, risk response and risk monitoring; *Constraints affecting risk assessments, risk response and risk monitoring; *Constraints affecting risk assessments, risk response and risk monitoring; **Constraints affecting risk assessments, risk response and risk monitoring; **Priorities, benefits and trade-offs considered by the organization for	10 10 10 10 10 5 10 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 (optional)	Notes (optional)
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	Mechanisms exist to identify: - Assumptions affecting risk assessments, risk response and risk monitoring; - Constraints affecting risk assessments, risk response and risk monitoring; - The organizational risk tolerance; and - Priorities, benefits and trade-offs considered by the organization for	5	
			Functional	subset of	Risk Management Program	RSK-01	managing risk. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
6.1.2(a)(2)	Information security risk assessment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: - Assumptions affecting risk assessments, risk response and risk monitoring; - Constraints affecting risk assessments, risk response and risk monitoring; - The organizational risk tolerance; and - Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
6.1.2(b)	Information security risk assessment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: - Assumptions affecting risk assessments, risk response and risk monitoring: - Constraints affecting risk assessments, risk response and risk monitoring: - The organizational risk tolerance; and - Priorities, benefits and trade-offs considered by the organization for managing risk. Mechanisms exist to facilitate the implementation of strategic,	5	
6.1.2(c)	Information security risk assessment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional Functional	subset of	Risk Management Program Risk Framing	RSK-01.1	preciationals acts to inclinate the imprementation of strategic, operational and tactical risk management controls. Mechanisms exist to identify: - Assumptions affecting risk assessments, risk response and risk monitoring: - Constraints affecting risk assessments, risk response and risk monitoring: - The organizational risk tolerance; and - Priorities, benefits and trade-offs considered by the organization for	5	
			Functional	subset of	Risk Management Program	RSK-01	managing risk. Mechanisms exist to facilitate the implementation of strategic,	10	
			Functional	intersects with	Risk Identification	RSK-03	operational and tactical risk management controls. Mechanisms exist to identify and document risks, both internal and external.	5	
6.1.2(c)(1)	Information security risk assessment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: - Assumptions affecting risk assessments, risk response and risk monitoring; - Constraints affecting risk assessments, risk response and risk monitoring; - The organizational risk tolerance; and - Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
			Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
			Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external. Mechanisms exist to facilitate the implementation of strategic,	5	
			Functional	subset of	Risk Management Program	RSK-01	operational and tactical risk management controls. Mechanisms exist to identify and document risks, both internal and	10	
6.1.2(c)(2)	Information security risk assessment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Identification Risk Framing	RSK-01.1	external. Mechanisms exist to identify: *Assumptions affecting risk assessments, risk response and risk monitoring; *Constraints affecting risk assessments, risk response and risk monitoring; *The organizational risk tolerance; and *Priorities, benefits and trade-offs considered by the organization for	5	
			Functional	subset of	Risk Management Program	RSK-01	managing risk. Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
			Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's	5	
6.1.2(d)	Information security risk assessment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Framing	RSK-01.1	systems and data. Mechanisms exist in identify: - Assumptions affecting risk assessments, risk response and risk monitoring; - Constraints affecting risk assessments, risk response and risk monitoring; - The organizational risk tolerance; and - Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
			Functional	intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
6.1.2(d)(1)	Information security risk assessment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	subset of	Risk Framing	RSK-01.1	Mechanisms exist to identify: - Assumptions affecting risk assessments, risk response and risk monitoring; - Constraints affecting risk assessments, risk response and risk monitoring; - The organizational risk tolerance; and - Priorities, benefits and trade-offs considered by the organization for managing risk.	10	
			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(d)(2)	Information security	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: * Assumptions affecting risk assessments, risk response and risk monitoring; * Constraints affecting risk assessments, risk response and risk monitoring; * The organizational risk tolerance; and * Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
		2	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
			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	
			Functional	intersects with	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize systems and data in accordance with applicable local, state and Federal laws that: - Document the security categorization results (including supporting rationale) in the security plan for systems; and - Ensure the security categorization decision is reviewed and approved by the asset owner. Mechanisms exist to identify:	5	
6.1.2(d)(3)	Information security risk assessment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Framing Risk Management Program	RSK-01.1	Assumptions affecting risk assessments, risk response and risk monitoring; Constraints affecting risk assessments, risk response and risk monitoring; The organizational risk tolerance; and Priorities, benefits and trade-offs considered by the organization for managing risk. Mechanisms exist to facilitate the implementation of strategic,	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
			Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's	5	
6.1.2(e)	Information security risk assessment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Framing	RSK-01.1	systems and data. Mechanisms exit to identify: - Assumptions affecting risk assessments, risk response and risk monitoring: - Constraints affecting risk assessments, risk response and risk monitoring: - The organizational risk tolerance; and - Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
			Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
			Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes Mechanisms exist to conduct recurring assessments of risk that includes	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	the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
	risk discussification	map.y/www.so.org/standard/27001	Functional	intersects with	Risk Framing		Mechanisms exist to identify: Mechanisms exist to facilitate the implementation of strategic,	5	
			Functional	subset of	Risk Management Program	RSK-01	operational and tactical risk management controls. Mechanisms exist to identify:	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	Assumptions affecting risk assessments, risk response and risk monitoring; Constraints affecting risk assessments, risk response and risk monitoring; The organizational risk tolerance; and Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
			Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
			Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's	5	
							systems and data. Mechanisms exist to respond to findings from cybersecurity & data		
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		privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	
			Functional	intersects with	Risk Remediation		Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to respond to findings from cybersecurity & data	5	
6.1.3(a)	Information security risk treatment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Response		privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	
			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(b)	Information security risk treatment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Response	RSK-06.1	privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	
			Functional Functional	intersects with intersects with	Risk Remediation Risk Remediation		Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to remediate risks to an acceptable level.	5 5	
6.1.3(c)	Information security risk treatment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Response		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	
			Functional Functional	intersects with intersects with	Risk Remediation Risk Remediation		Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to remediate risks to an acceptable level.	5	
6.1.3(e)	Information security risk treatment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Response		Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation	5	
			Functional	intersects with	Risk Remediation		has been performed. Mechanisms exist to remediate risks to an acceptable level.	5	
6.1.3(f)	Information security risk treatment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Response		Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	
6.2	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(a)	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(b)	Information security objectives and planning to achieve them	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5	
6.2(c)	Information security objectives and planning 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(d)	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(e)	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(f)	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(g)	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(h)	Information security objectives and planning to achieve them	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5	
6.2(i)	Information security objectives and planning 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(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(I)	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	(optional) 5	
7.2	Competence	Buy a copy of ISO 27001 for control content: https://www.iso.ore/standard/27001	Functional	intersects with	Management Competency Requirements for Security-Related	HRS-03.2	privacy programs and document all exceptions to this requirement. Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
		nttps://www.iso.org/standatu/27001	Functional	intersects with	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-Related	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	
			Functional	intersects with	Positions Competency Requirements	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed	5	
7.2(b)	Competence	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	for Security-Related Positions Personnel Screening	HRS-03.2	by qualified individuals who have the necessary skill set. Mechanisms exist to manage personnel security risk by screening	5	
			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	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	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	
			Functional	subset of	Human Resources Security	HRS-01	Mechanisms exist to facilitate the implementation of personnel security	10	
7.2(d)	Competence	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Management Competency Requirements for Security-Related	HRS-03.2	controls. Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
			Functional	intersects with	Positions Social Media & Social	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit	5	
			Tunctional	intersects with	Networking Restrictions	11113-03.2	information on commercial websites and sharing account information. Mechanisms exist to verify that individuals accessing a system processing,	,	
			Functional	intersects with	Formal Indoctrination	HRS-04.2	storing, or transmitting sensitive information are formally indoctrinated for all the relevant types of information to which they have access on the system.	5	
			Functional	intersects with	User Awareness Use of Communications	HRS-03.1	Mechanisms exist to establish usage restrictions and implementation	5	
			Functional	intersects with	Technology	HRS-05.3	cause damage to systems, if used maliciously.	5	
7.3	Awareness	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
			Functional	intersects with	Use of Critical Technologies	HRS-05.4		5	
			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	
			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	
			Functional	intersects with	Rules of Behavior	HRS-05.1	behavior.	5	
			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	
			Functional	intersects with	Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.	5	
			Functional	intersects with	Formal Indoctrination	HRS-04.2	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information are formally indoctrinated for all the relevant types of information to which they have access on the system.	5	
			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	
			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. Mechanisms exist to establish usage restrictions and implementation	5	
			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	
			Functional	intersects with	Use of Critical Technologies	HRS-05.4		5	
			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	
			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	
			Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
			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	
			Functional	intersects with	Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.	5	
			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	
			Functional	intersects with	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit	5	
7.3(b)	Awareness	Buy a copy of ISO 27001 for control content:	Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation	5	
		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	
			Functional	intersects with	Use of Critical Technologies	HRS-05.4		5	
			Functional	intersects with	Formal Indoctrination	HRS-04.2	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information are formally indoctrinated for all the relevant types of information to which they have access on the	5	
			Functional	intersects with	Rules of Behavior	HRS-05.1	system. Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
			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	
			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	
			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	
	l						milioniation on commercial websites and snaring account information.		



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)
			Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
			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(c)	Awareness	Buy a copy of ISO 27001 for control content:	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	
7.5(c)	Awareness	https://www.iso.org/standard/27001	Functional	intersects with	Formal Indoctrination	HRS-04.2	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information are formally indoctrinated for all the relevant types of information to which they have access on the system.	5	
			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	
			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	
			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	
			Functional	intersects with	Use of Critical Technologies	HRS-05.4	Mechanisms exist to govern usage policies for critical technologies.	5	
			Functional	intersects with	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
7.4	Communication	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
		IIILps://www.isu.org/stanuaru/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	
			Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
			Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function. Mechanisms exist to provide governance oversight reporting and	5	
7.4(a)	Communication	Buy a copy of ISO 27001 for control content:	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	
7.4(a)	Communication	https://www.iso.org/standard/27001	Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
			Functional	intersects with	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
			Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
		Dura seaso of ISO 37003 for control contents	Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
7.4(b)	Communication	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
			Functional	intersects with	Threat Intelligence Feeds	THR-03	Mechanism exist to maintain situational awareness of evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
			Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
			Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
7.4(c)	Communication	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
			Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and	5	
			Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
		Buy a copy of ISO 27001 for control content:	Functional	intersects with	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and	5	
7.4(d)	Communication	https://www.iso.org/standard/27001	Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	compensating controls. Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
			Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	matters considered material to the organization's cybersecurity & data	5	
7.5	Documented information	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	no relationship	N/A	N/A	protection program. N/A	N/A	This is merely a section title without content.
7.5.1	General	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
7.5.1(a)	General	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
7.5.1(b)	General	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
		Buy a copy of ISO 27001 for control content:	Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy	5	
7.5.2	Creating and updating	https://www.iso.org/standard/27001	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	and effectiveness. Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
		Buy a copy of ISO 27003 for control	Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy	5	
7.5.2(a)	Creating and updating	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	and effectiveness. Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
			Functional	intersects with	Periodic Review & Update of Cybersecurity & Data	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy	(optional)	
7.5.2(b)	Creating and updating	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Protection Program Publishing Cybersecurity & Data Protection Documentation	GOV-02	and effectiveness. Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
7.5.2(c)	Creating and updating	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
7.5.3	Control of documented information	Buy a copy of ISO 27001 for control content:	Functional	intersects with	Periodic Review & Update Publishing Cybersecurity & Data Protection	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, Mechanisms exist to restablish, maintain and disseminate cybersecurity &	5	
7.5.3(a)	Control of documented		Functional	intersects with	Documentation Publishing Cybersecurity & Data Protection	GOV-02	data protection policies, standards and procedures. Mechanisms exist to establish, maintain and disseminate cybersecurity &	5	
7.5.3(b)		https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content:	Functional	intersects with	Documentation Publishing Cybersecurity & Data Protection	GOV-02	data protection policies, standards and procedures. Mechanisms exist to establish, maintain and disseminate cybersecurity &	5	
	information Control of documented	https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content:	Functional	intersects with	Documentation Publishing Cybersecurity & Data Protection	GOV-02	data protection policies, standards and procedures. Mechanisms exist to establish, maintain and disseminate cybersecurity &	5	
7.5.3(c)	information Control of documented	https://www.iso.org/standard/27001 Buy a copy of ISO 27001 for control content:			Documentation Publishing Cybersecurity &		data protection policies, standards and procedures. Mechanisms exist to establish, maintain and disseminate cybersecurity &	-	
7.5.3(d)	information	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	
7.5.3(e)	Control of documented information	https://www.iso.org/standard/27001	Functional	intersects with	Data Protection Documentation Publishing Cybersecurity &	GOV-02	data protection policies, standards and procedures.	5	
7.5.3(f)	information	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	Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5 N/A	This is marchy a specific title with
8.0	Operation	https://www.iso.org/standard/27001	Functional	no relationship	N/A	N/A	N/A Mechanisms exist to facilitate the implementation of operational security	N/A	This is merely a section title without content.
			Functional	subset of	Operations Security Cybersecurity & Data Protection Governance Program	OPS-01 GOV-01	controls. Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
			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	
	Operational planning	Buy a copy of ISO 27001 for control content:	Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
8.1	and control	https://www.iso.org/standard/27001	Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	5	
			Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
8.2	Information security risk assessment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
			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	risk treatment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Remediation Risk Response	RSK-06.1	Mechanisms exist to remediate risks to an acceptable level. 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.
			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. Mechanisms exist to ensure managers regularly review the processes and	5	
9.1	Monitoring, measurement, analysis	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements. Mechanisms exist to document and review instances of non-compliance	5	
	and evaluation		Functional	intersects with	Non-Compliance Oversight Statutory, Regulatory &	CPL-01.1	with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to facilitate the identification and implementation of	5	
			Functional	subset of	Contractual Compliance	CPL-01	relevant statutory, regulatory and contractual controls.	10	
			Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance. Mechanisms exist to develop, report and monitor cybersecurity & data	5	
			Functional	intersects with	Measures of Performance Status Reporting To	GOV-05	privacy program measures of performance. Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about	5	
9.1(a)	Monitoring, measurement, analysis and evaluation	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001			Governing Body Cybersecurity & Data		matters considered material to the organization's cybersecurity & data protection program. Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to		
			Functional	intersects with	Protection Assessments	CPL-03	appropriate cybersecurity & data protection policies, standards and other applicable requirements. Mechanisms exist to document and review instances of non-compliance	5	
			Functional	intersects with	Non-Compliance Oversight Status Reporting To		with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions. Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about	5	
	Monitoring,		Functional	intersects with	Governing Body Measures of Performance	GOV-01.2	matters considered material to the organization's cybersecurity & data protection program. Mechanisms exist to develop, report and monitor cybersecurity & data	5	
9.1(b)	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	privacy program measures of performance. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
			Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	5	
			Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
			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 ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	5	
			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	
			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	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 ensure managers regularly review the processes and	5	
	und evaluation		Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	5	
			Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
			Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
	Monitoring,	Buy a copy of ISO 27001 for control content:	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)	measurement, analysis and evaluation	https://www.iso.org/standard/27001	Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity & data protection policies, standards and other applicable requirements.	5	
			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	
			Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate 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	
			Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
			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	N/A	N/A	This is merely a section title without content.
			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	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	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	
			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	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)	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	governance processes. Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
9.2.2(b)	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	Revenience processes: Mechanisms exists 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)	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:	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	
3.3.1	General	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(a)	Management review	Buy a copy of ISO 27001 for control content:	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	
	inputs	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	Buy a copy of ISO 27001 for control content:	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	
	inputs	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(e)	Management review	Buy a copy of ISO 27001 for control content:	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 #	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)
3.3.2(c)	inputs	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	
	Management review	Buy a copy of ISO 27001 for control content:	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(d)	inputs	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(d)(1)	Management review	Buy a copy of ISO 27001 for control content:	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	matters considered material to the organization's cybersecurity & data protection program.	5	
	inputs	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. Mechanisms exist to coordinate cybersecurity, data protection and	5	
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	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.	5	
	iliputs	mttps://www.bo.urg/standaru/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. Mechanisms exist to provide governance oversight reporting and	5	
9.3.2(d)(3)	Management review	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	commandations to those entrusted to make executive decisions about	5	
	mpacs	magory www.socory standardy 27 002	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 provide governance oversight reporting and	5	
9.3.2(d)(4)	Management review	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 coordinate cybersecurity, data protection and	5	
			Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	husiness alignment through a steering committee or advisory heard	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	husiness alignment through a steering committee or advisory heard	5	
	inputs	The state of the s	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	recommendations to those entrusted to make executive decisions about	5	
9.3.2(f)	Management review	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 coordinate cybersecurity, data protection and	5	
	inputs	The state of the s	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	business alignment through a steering committee or advisory board	5	
9.3.2(g)	Management review	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	husiness alignment through a steering committee or advisory heard	5	
			Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	recommendations to those entrusted to make executive decisions about	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	husiness alignment through a steering committee or advisory heard	5	
		Buy a copy of ISO 27001 for control content:	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	
10.0	Improvement	https://www.iso.org/standard/27001	Functional	no relationship	N/A Cybersecurity & Data	N/A	N/A Mechanisms exist to facilitate the implementation of cybersecurity & data	N/A	This is merely a section title without content.
10.1		Buy a copy of ISO 27001 for control content:	Functional	subset of intersects with	Protection Governance Program Cybersecurity & Data Protection Controls	GOV-01 CPL-02	protection governance controls. Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	10	
10.1	Continual improvement	https://www.iso.org/standard/27001	Functional	intersects with	Oversight 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	
10.2	Nonconformity and	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Non-Compliance Oversight	CPL-01.1	which meets formally and on a regular basis. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop	5	
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	appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	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	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	appropriate risk mitigation actions. Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	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.	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	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)(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)(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.	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	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(e)	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	



ISO 27001:2022

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)
10.2(f)		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(g)		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	

