### **Set Theory Relationship Mapping (STRM)**



Reference Document: Secure Controls Framework (SCF) version 2024.4

Focal Document: ISO 27001:2022

Focal Document URL: https://www.iso.org/standard/27001

STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-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 results of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise

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

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



#### Relationship Type #1: SUBSET OF

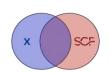
Focal Document Element is a subset of SCF control. In other words, SCF control contains everything that Focal Document Element does and more.



SUBSET OF Relative Relationship Strength (control versus

### Relationship Type #2: INTERSECTS WITH

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



INTERSECTS WITH Relative Relationship Strength (control versus

## Relationship Type #3:

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



Relative Relationship Strength (control versus control)

# Relationship Type #4:

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

### SCF control and Focal Document Element are

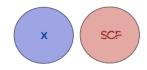
unrelated; their content does not overlap.

Relationship Type #5:

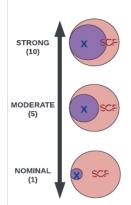
NO RELATIONSHIP

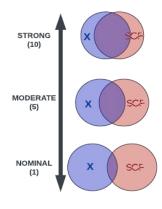


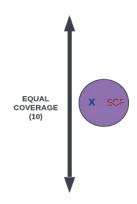
Relative Relationship Strength (control versus control)

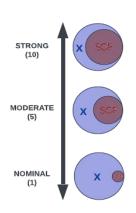


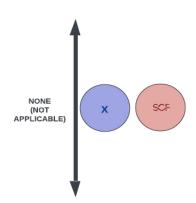
NO RELATIONSHIP Relative Relationship Strength (control versus control)













FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
1.0	\cone	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2.0		Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.0	Terms and definitions	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.		
4.0		Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
	Organization	Tittps://www.iso.org/standard/27001	Functional	intersects with	Defining Business Context	GOV-08	Mechanisms exist to define the context of its business model and document the mission of the organization.	5	
					& Mission		Mechanisms exist to establish control objectives as the basis for the		
	Understanding the	Buy a copy of ISO 27001 for control content:	Functional	intersects with	Define Control Objectives	GOV-09	selection, implementation and management of the organization's internal control system.	5	
4.1	organization and its context	https://www.iso.org/standard/27001	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	ISO 27001:2022 Amendment 1 adds "climate action changes" that a reasonable person would conclude has nothing to do with cybersecurity and is merely a inclusion for Environmental, Social & Governance (ESG) compliance to push a political agenda.
4.2	Understanding the needs and expectations	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	
7.2	of interested parties	https://www.iso.org/standard/27001	Functional	intersects with	Stakeholder Identification & Involvement	AST-01.2	management of those assets.	5	
	Understanding the	Buy a copy of ISO 27001 for control content:	Functional	intersects with	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the mission of the organization.	5	
4.2(a)	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(b)	Inded and evnectations	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	
	Crimer server parases		Functional	intersects with	Defining Business Context	GOV-08	Mechanisms exist to define the context of its business model and document the mission of the organization.	5	
4.3	Determining the scope of the information	Buy a copy of ISO 27001 for control content:	Functional	intorrocts with	& Mission	CDI 01.2	Mechanisms exist to document and validate the scope of cybersecurity &	5	
4.3	security management system	https://www.iso.org/standard/27001	Functional	intersects with	Compliance Scope		data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.  Mechanisms exist to determine cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate	5	
	Determining the scope		Functional	intersects with	Asset Scope Classification	AST-04.1	asset scope categorization for all systems, applications, services and personnel (internal and third-parties).  Mechanisms exist to document and validate the scope of cybersecurity &	5	
4.3(a)		Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Compliance Scope	CPL-01.2	data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
4.3(b)	of the information	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 of the information	Buy a copy of ISO 27001 for control content:	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)		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)  Cybersecurity & Data	CLD-06.1	Cloud Service Provider (CSP) and its customers.	5	
			Functional	subset of	Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
4.4	•	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
5.0	I Leadershin	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	Cybersecurity & Data Protection Governance	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity &	10	
5.1	Leadership and commitment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	subset of	Program  Steering Committee & Program Oversight	GOV-01.1	data protection governance controls.  Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	10	
			Functional	intersects with	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the mission of the organization.	5	
			Functional	intersects with	Publishing Cybersecurity &  Data Protection	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity &	5	
5.1(a)		Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	runcuonal	intersects with	Documentation	GUV-UZ	data protection policies, standards and procedures.	5	
	commitment	Tittps.//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(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.	10	
5.1(c)		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)		Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	subset of	Cybersecurity & Data Protection Governance Program  Cybersecurity & Data	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
F 4/-1	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)	· ·	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	
			Functional	intersects with	Assigned Cybersecurity & Data Protection	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop,	5	



Secure Controls Framework (SCF) 2 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)
	communicité	Tittps.// 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(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	
			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 commitment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Assigned Cybersecurity & Data Protection	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data	5	
5.2	Policy	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Responsibilities  Fublishing Cybersecurity &  Data Protection	GOV-02	protection program.  Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
5.2(a)	Policy	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & 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	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	intersects with	Documentation  Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
5.3	Organizational roles, responsibilities and authorities	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
			Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
5.3(a)	Organizational roles, responsibilities and	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	
	Organizational roles,	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	
5.3(b)	responsibilities and 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		Buy a copy of ISO 27001 for control content:	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	
	and opportunities	https://www.iso.org/standard/27001	Functional	subset of	Protection Governance Program Cybersecurity & Data	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
6.1.1(a)		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(b)	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.  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.  Mechanisms exist to facilitate the implementation of cybersecurity &	10	
6.1.1(c)	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	data protection governance controls.  Mechanisms exist to facilitate the implementation of strategic,	10	
			Functional	subset of	Risk Management Program  Cybersecurity & Data		operational and tactical risk management controls.  Mechanisms exist to facilitate the implementation of cybersecurity &	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	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.  Mechanisms exist to facilitate the implementation of cybersecurity &	10	
6.1.1(e)(1)		Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	subset of	Protection Governance Program	GOV-01	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.  Mechanisms exist to facilitate the implementation of cybersecurity &	10	
6.1.1(e)(2)		Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	subset of	Protection Governance Program	GOV-01	data protection governance controls.  Mechanisms exist to facilitate the implementation of strategic,	10	
			Functional	subset of	Risk Management Program	RSK-01	operational and tactical risk management controls.  Mechanisms exist to identify:  (1) Assumptions affecting risk assessments, risk response and risk monitoring;	10	
6.1.2	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	<ul> <li>(2) Constraints affecting risk assessments, risk response and risk monitoring;</li> <li>(3) The organizational risk tolerance; and</li> <li>(4) Priorities, benefits and trade-offs considered by the organization for managing risk.</li> </ul>	5	
	1		Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic,		1



Secure Controls Framework (SCF) 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)
							Mechanisms exist to identify:  (1) Assumptions affecting risk assessments, risk response and risk	(орионат)	
							monitoring; (2) Constraints affecting risk assessments, risk response and risk		
6.1.2(a)	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	monitoring; (3) The organizational risk tolerance; and	5	
	TISK d33C33TICTC	inttps.//www.iso.org/standard/27001					(4) Priorities, benefits and trade-offs considered by the organization for managing risk.		
			Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic,	10	
			Functional	subset of	Risk Management Program	RSK-01	operational and tactical risk management controls.  Mechanisms exist to facilitate the implementation of strategic,	10	
							operational and tactical risk management controls.  Mechanisms exist to identify:		
6.1.2(a)(1)		Buy a copy of ISO 27001 for control content:					(1) Assumptions affecting risk assessments, risk response and risk monitoring;		
	risk assessment	https://www.iso.org/standard/27001	Functional	intersects with	Risk Framing	RSK-01.1	(2) Constraints affecting risk assessments, risk response and risk monitoring;	5	
							(3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for		
			Functional	subset of	Risk Management Program	RSK-01	managing risk.  Mechanisms exist to facilitate the implementation of strategic,	10	
			Tanctional	30030101	Nisk Wanagement Flogram	NOK 01	operational and tactical risk management controls.  Mechanisms exist to identify:	10	
6.1.2(a)(2)	Information security	Buy a copy of ISO 27001 for control content:					(1) Assumptions affecting risk assessments, risk response and risk monitoring;		
0.1.2(a)(2)	risk assessment	https://www.iso.org/standard/27001	Functional	intersects with	Risk Framing	RSK-01.1	(2) Constraints affecting risk assessments, risk response and risk monitoring;	5	
							(3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for		
							managing risk.  Mechanisms exist to identify:		
							(1) Assumptions affecting risk assessments, risk response and risk monitoring;		
	Information security	Buy a copy of ISO 27001 for control content:	Functional	intersects with	Risk Framing	RSK-01.1	(2) Constraints affecting risk assessments, risk response and risk monitoring;	5	
6.1.2(b)	risk assessment	https://www.iso.org/standard/27001					(3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for		
							managing risk.  Mechanisms exist to facilitate the implementation of strategic,		
			Functional	subset of	Risk Management Program	RSK-01	operational and tactical risk management controls.	10	
							Mechanisms exist to identify:  (1) Assumptions affecting risk assessments, risk response and risk		
			Functional	intersects with	Risk Framing	RSK-01.1	monitoring; (2) Constraints affecting risk assessments, risk response and risk	5	
6.1.2(c)		Buy a copy of ISO 27001 for control content:					monitoring; (3) The organizational risk tolerance; and		
512.2(5)	risk assessment	https://www.iso.org/standard/27001					(4) Priorities, benefits and trade-offs considered by the organization for managing risk.		
			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.	5	
							Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk		
			Functional	intersects with	Risk Framing	RSK-01.1	monitoring; (2) Constraints affecting risk assessments, risk response and risk	5	
C 4 2/-V/4V	Information security	Buy a copy of ISO 27001 for control content:	Fullctional	intersects with	NISK FLAITHING	K3K-U1.1	monitoring; (3) The organizational risk tolerance; and	3	
6.1.2(c)(1)	risk assessment	https://www.iso.org/standard/27001					(4) Priorities, benefits and trade-offs considered by the organization for managing risk.		
			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.	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.	5	
	Information security	Buy a copy of ISO 27001 for control content:					Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk		
6.1.2(c)(2)	risk assessment	https://www.iso.org/standard/27001					monitoring; (2) Constraints affecting risk assessments, risk response and risk		
			Functional	intersects with	Risk Framing	RSK-01.1	monitoring; (3) The organizational risk tolerance; and	5	
							(4) Priorities, benefits and trade-offs considered by the organization for managing risk.		
			Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
							Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use,		
			Functional	intersects with	Risk Assessment	RSK-04	disclosure, disruption, modification or destruction of the organization's systems and data.	5	
6.1.2(d)		Buy a copy of ISO 27001 for control content:					Mechanisms exist to identify:		
	risk assessment	https://www.iso.org/standard/27001					(1) Assumptions affecting risk assessments, risk response and risk monitoring;		
			Functional	intersects with	Risk Framing	RSK-01.1	(2) Constraints affecting risk assessments, risk response and risk monitoring;	5	
							(3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for		
			Functional	intersects with	Risk Management Program	RSK-01	managing risk.  Mechanisms exist to facilitate the implementation of strategic,	5	
			. S.ISSIOHUI	With Section With			operational and tactical risk management controls.  Mechanisms exist to identify:		
							(1) Assumptions affecting risk assessments, risk response and risk monitoring;		
6.1.2/4//1/	Information security	Buy a copy of ISO 27001 for control content:	Functional	subset of	Risk Framing	RSK-01.1	(2) Constraints affecting risk assessments, risk response and risk monitoring;	10	
6.1.2(d)(1)	risk assessment	https://www.iso.org/standard/27001					(3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for		
							managing risk.  Mechanisms exist to conduct recurring assessments of risk that includes		
			Functional	intersects with	Risk Assessment	RSK-04	the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's	5	
							systems and data.  Mechanisms exist to identify:		
							(1) Assumptions affecting risk assessments, risk response and risk		
			Functional	intersects with	Risk Framing	RSK-01.1	monitoring; (2) Constraints affecting risk assessments, risk response and risk	5	
							monitoring; (3) The organizational risk tolerance; and (4) Priorities happiits and trade offs considered by the organization for		
6.1.2(d)(2)	Information security risk assessment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001					(4) Priorities, benefits and trade-offs considered by the organization for managing risk.		
			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,	5	
			. uncuondi	microects with	ווופר ספפסטווופוונ	113N-7U4	disclosure, disruption, modification or destruction of the organization's systems and data.		
					•	<u> </u>	•		•



Secure Controls Framework (SCF) 4 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)
			Functional	intersects with	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize systems and data in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5	
6.1.2(d)(3)	•	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
			Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic,  Mechanisms exist to conduct recurring assessments of risk that includes	10	
			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	
6.1.2(e)	•	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
			Functional	subset of	Risk Management Program		Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
6.1.2(e)(1)	•	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional Functional	intersects with	Risk Assessment Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes 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 Functional	intersects with subset of	Risk Framing Risk Management Program	RSK-01.1 RSK-01	Mechanisms exist to identify:  Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5 10	
6.1.2(e)(2)		Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
		3,000	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	
6.1.3		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(a)	· ·	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional 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	
6.1.3(b)		Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional Functional	intersects with	Risk Remediation Risk Response	RSK-06 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	
		Buy a copy of ISO 27001 for control content:	Functional Functional	intersects with intersects with	Risk Remediation Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.  Mechanisms exist to remediate risks to an acceptable level.  Mechanisms exist to respond to findings from cybersecurity & data	5 5	
6.1.3(c)	•	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.  Mechanisms exist to respond to findings from cybersecurity & data	5	
6.1.3(d)	·	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional Functional	intersects with	Risk Response Risk Remediation	RSK-06.1	privacy assessments, incidents and audits to ensure proper remediation has been performed.  Mechanisms exist to remediate risks to an acceptable level.	5	
6.1.3(e)	Information security risk treatment	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional Functional	intersects with	Risk Remediation  Risk Response	RSK-06	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	5	
	risk treatment	Thttps://www.iso.org/stanuaru/27001	Functional	intersects with	Risk Remediation	RSK-06.1	has been performed.  Mechanisms exist to remediate risks to an acceptable level.	5	
6.1.3(f)	·	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	
6.2	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)	Inniectives and highning	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)	Inniectives and highning	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 cocurity	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	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	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's	5	
6.2(g)	objectives and planning	Ruy a copy of ISO 27001 for control content:	Functional	intersects with	Define Control Objectives	GOV-09	internal control system.  Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's	5	
6.2(h)	Information security objectives and planning	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Define Control Objectives	GOV-09	internal control system.  Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's	5	
6.2(i)	Information security	Ruy a copy of ISO 27001 for control content:	Functional	intersects with	Define Control Objectives	GOV-09	internal control system.  Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5	



Secure Controls Framework (SCF) 5 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)
6.2(j)	Inhiactives and highning	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)	Inniectives and highning	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	Sunnort	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.
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 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	
7.2	Competence	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.  Mechanisms exist to manage personnel security risk by assigning a risk	5	
7.2(a)	Competence	Buy a copy of ISO 27001 for control content:	Functional	intersects with	Position Categorization	HRS-02	designation to all positions and establishing screening criteria for individuals filling those positions.	5	
7.2(a)	Competence	https://www.iso.org/standard/27001	Functional	intersects with	Competency Requirements for Security-Related Positions Competency Requirements	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
7.2(b)	I (omnetence	Buy a copy of ISO 27001 for control content:	Functional	intersects with	for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
		https://www.iso.org/standard/27001	Functional	intersects with	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
7.2(-)	Commentered	Buy a copy of ISO 27001 for control content:	Functional	intersects with	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
7.2(c)	I COMPATANCA	https://www.iso.org/standard/27001	Functional	intersects with	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
			Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
7.2(d)	Competence	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
			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	
			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	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	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
7.3	Awareness	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
		Titeps.// www.iso.org/standard/2/001	Functional	intersects with	Use of Critical Technologies	HRS-05.4	Mechanisms exist to govern usage policies for critical technologies.	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.  Mechanisms exist to ensure personnel receive recurring familiarization	5	
			Functional	intersects with	Policy Familiarization & Acknowledgement	HRS-05.7	with the organization's cybersecurity & data privacy policies and provide acknowledgement.	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	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	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.  Mechanisms exist to verify that individuals accessing a system processing,	5	
			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	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)	Δwareness	Buy a copy of ISO 27001 for control content:	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	
		https://www.iso.org/standard/27001	Functional	intersects with	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	5	
			Functional	intersects with	Use of Critical Technologies	HRS-05.4	Mechanisms exist to govern usage policies for critical technologies.	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.  Mechanisms exist to communicate with users about their roles and	10	
			Functional	intersects with	User Awareness  Defined Roles &	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.  Mechanisms exist to define cybersecurity roles & responsibilities for all	5	
			Functional	intersects with	Responsibilities	HRS-03	personnel.  Mechanisms exist to require all employees and contractors to apply	5	
			Functional	intersects with	Terms of Employment  Social Media & Social	HRS-05	cybersecurity & data privacy principles in their daily work.  Mechanisms exist to define rules of behavior that contain explicit	5	
			Functional	intersects with	Networking Restrictions  Use of Communications		restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.  Mechanisms exist to establish usage restrictions and implementation	5	
7.3(b)	Awareness	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Technology  Human Resources Security		guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.  Mechanisms exist to facilitate the implementation of personnel security	5	
			Functional	subset of	Management	HRS-01	controls.	10	
			Functional	intersects with	Use of Critical Technologies	HRS-05.4	Mechanisms exist to govern usage policies for critical technologies.  Mechanisms exist to verify that individuals accessing a system processing,	5	
			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.  Mechanisms exist to define acceptable and unacceptable rules of	5	
			Functional	intersects with	Rules of Behavior	HRS-05.1	behavior for the use of technologies, including consequences for unacceptable behavior.	5	



Secure Controls Framework (SCF) 6 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)
			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	
			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	
7.3(0)	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 Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
7.4	Communication	Buy a copy of ISO 27001 for control content:	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	Communication	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	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.	5	
- 41		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 Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
			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	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 Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
			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 Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
			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	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of	5	
7.4(d)	Communication	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	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	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	
7.5	Documented information	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	no relationship	N/A	N/A	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	
7.5.2	Creating and updating	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	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 and effectiveness.	5	
			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	
	Creating and updating	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 and effectiveness.	5	



Secure Controls Framework (SCF) 7 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)
		TITEPS://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	
7.5.2(b)	Creating and updating	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 and effectiveness.	5	
- (-)		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	
7.5.2(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: https://www.iso.org/standard/27001	Functional Functional	intersects with	Periodic Review & Update Publishing Cybersecurity & Data Protection Documentation	GOV-03 GOV-02	Mechanisms exist to review the cybersecurity & data privacy program,  Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
7.5.3(a)	Control of documented information	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
7.5.3(b)	Control of documented information	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
7.5.3(c)	Control of documented information	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
7.5.3(d)	Control of documented information	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	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(e)	Control of documented information	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation Publishing Cybersecurity &	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
7.5.3(f)	Control of documented information	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Data Protection  Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
8.0	Operation	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	no relationship	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 Functional	subset of subset of	Operations Security  Cybersecurity & Data  Protection Governance	OPS-01 GOV-01	controls.  Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
			Functional	intersects with	Program Cybersecurity & Data Protection Controls	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
0.4	Operational planning	Buy a copy of ISO 27001 for control content:	Functional	intersects with	Oversight  Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper	5	
8.1	and control	https://www.iso.org/standard/27001	Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	execution of day-to-day / assigned tasks.  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	-	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 Functional	subset of intersects with	Risk Management Program Risk Remediation	RSK-01 RSK-06	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.  Mechanisms exist to remediate risks to an acceptable level.	10 5	
8.3	•	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	
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.	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	Monitoring, measurement, analysis and evaluation	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
			Functional Functional	subset of intersects with	Statutory, Regulatory & Contractual Compliance Cybersecurity & Data Protection Controls	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.  Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	10 5	
			Functional	intersects with	Oversight  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,	Duy 2 copy of ISO 27004 fee	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(a)	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	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	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	
Q 1/h\	Monitoring,	Buy a copy of ISO 27001 for control content:	Functional	intersects with	Measures of Performance	GOV-05	protection program.  Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.  Mechanisms exist to document and review instances of non-compliance.	5	
9.1(b)	measurement, analysis and evaluation	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	
			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	
			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	



Secure Controls Framework (SCF) 8 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)
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.		
			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	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	
	and evaluation		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	
			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 provide governance oversight reporting and	5	
0.1(a)	Monitoring,	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	
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.  Mechanisms exist to document and review instances of non-compliance	5	
			Functional	intersects with	Non-Compliance Oversight	CPL-01.1	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	I 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.
		The part of the state of the st	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	intersects with	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor systems, applications and/or services under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity & data privacy controls are operating as intended.	3	
9.2.2	Internal audit programme	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
			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)		Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
9.2.2(b)	Internal audit programme	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
9.2.2(c)	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		Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	no relationship	N/A	N/A	N/A	N/A	This is merely a section title without content.
9.3.1		Buy a copy of ISO 27001 for control content:	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	
J.J.1	Schola	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)	_	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	
(4)	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)	_	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	
2.3.2(8)	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	
	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	



Set Theory Relationship Mapping (STRM)

Secure Controls Framework (SCF) 9 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	Notes (optional)
J.J.2(U)	inputs	https://www.iso.org/standard/27001	Functional		Steering Committee &	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board,	(optional)	
			Functional	intersects with	Program Oversight	GOV-01.1	comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.  Mechanisms exist to coordinate cybersecurity, data protection and	5	
	Management review	Buy a copy of ISO 27001 for control content:	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	
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	
0.00(1)(4)	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	5	
9.3.2(d)(1)	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.	5	
9.3.2(d)(2)	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	
3.3.2(u)(2)	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)(3)	_	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	
	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.	5	
9.3.2(d)(4)	_	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	
	inputs	Tittps://www.iso.org/stanuaru/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(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	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	
			Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.  Mechanisms exist to provide governance oversight reporting and	5	
9.3.2(f)	Management review inputs	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	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	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(g)	Management review inputs	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	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	
			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	
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	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	
			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	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	no relationship	N/A Cybersecurity & Data	N/A	N/A	N/A	This is merely a section title without content.
			Functional	subset of	Protection Governance Program Cybersecurity & Data	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
10.1	Continual improvement	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.  Mechanisms exist to coordinate cybersecurity, data protection and	5	
			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	
10.2	Nonconformity and corrective action	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Non-Compliance Oversight	CPL-01.1	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)	Nonconformity and corrective action	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Non-Compliance Oversight	CPL-01.1	appropriate risk mitigation actions.	5	
10.2(a)(1)	Nonconformity and corrective action	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
10.2(a)(2)	Nonconformity and corrective action	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
10.2(b)	Nonconformity and corrective action	Buy a copy of ISO 27001 for control content: https://www.iso.org/standard/27001	Functional	intersects with	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	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	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	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	1	5	
10.2(d)		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(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	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	



Secure Controls Framework (SCF) 10 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)
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	



Secure Controls Framework (SCF) 11 of 11