Set Theory Relationship Mapping (STRM)



Reference Document: Secure Controls Framework (SCF) version 2024.4

Focal Document: ISO 42001:2023

Focal Document URL: https://www.iso.org/standard/81230.html

STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-iso-42001-2023.pdf

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

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

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

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

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

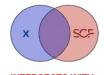


Relationship Type #1: SUBSET OF

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 control)



Relationship Type #2:

INTERSECTS WITH

SCF control has some

Document Element, but

each includes content that

overlap with Focal

the other does not.

INTERSECTS WITH Relative Relationship Strength (control versus

Relationship Type #3: EQUAL

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



Relative Relationship Strength (control versus control)

Relationship Type #4: SUPERSET OF

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

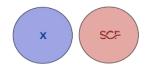
NO RELATIONSHIP SCF control and Focal Document Element are

Relationship Type #5:

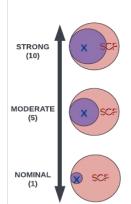
Document Element are unrelated; their content does not overlap.

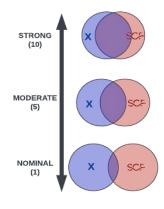


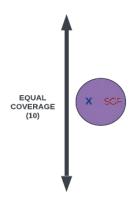
SUPERSET OF
Relative Relationship Strength
(control versus control)

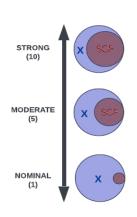


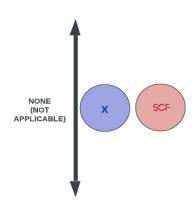
NO RELATIONSHIP
Relative Relationship Strength
(control versus control)











		Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
1.0	Scope	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	no relationship	N/A	N/A	N/A	(optional) N/A	No requirements to map to.
2.0	Normative references	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5	
4.0	Context of the organization	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
			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	Section 4.1 includes "climate action changes" that a reasonable person would conclude has nothing to do with cybersecurity and is merely an inclusion for Environmental, Social & Governance (ESG) compliance to push a political agenda. If climate change is a material concern for the organziation, then Artifical Intelligence (AI) initiatives should be avoided entirely, due to the high electricity consumption requirements.
			Functional	intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity & data privacy-specific business plan and set of objectives to achieve that plan.	5	
			Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
			Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
4.1		Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	subset of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
			Functional	intersects with	AI & Autonomous Technologies Context Definition	AAT-03	Mechanisms exist to establish and document the context surrounding Artificial Intelligence (AI) and Autonomous Technologies (AAT), including: (1) Intended purposes; (2) Potentially beneficial uses; (3) Context-specific laws and regulations; (4) Norms and expectations; and (5) Prospective settings in which the system(s) will be deployed.	5	
			Functional	intersects with	AI & Autonomous Technologies Requirements Definitions	AAT-14	Mechanisms exist to take socio-technical implications into account to address risks associated with Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			Functional	intersects with	AI & Autonomous Technologies Value Sustainment AI & Autonomous	AAT-01.3	Mechanisms exist to sustain the value of deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			Functional	intersects with	Technologies Mission and Goals Definition	AAT-03.1	Mechanisms exist to define and document the organization's mission and defined goals for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			Functional	intersects with	AI & Autonomous Technologies-Related Legal Requirements Definition	AAT-01.1	Mechanisms exist to identify, understand, document and manage applicable statutory and regulatory requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			Functional	intersects with	AI & Autonomous Technologies Environmental Impact & Sustainability	AAT-17.2	Mechanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			Functional	intersects with	Al & Autonomous Technologies-Related Legal Requirements Definition	AAT-01.1	Mechanisms exist to identify, understand, document and manage applicable statutory and regulatory requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			Functional	intersects with	AI & Autonomous Technologies Mission and Goals Definition	AAT-03.1	Mechanisms exist to define and document the organization's mission and defined goals for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			Functional	subset of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
4.2	Understanding the needs and expectations of interested parties	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
			Functional	intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity & data privacy-specific business plan and set of objectives to achieve that plan.	5	
			Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC). Mechanisms exist to define and manage the scope for its attack surface management	5	
			Functional	intersects with	Attack Surface Scope	VPM-01.1	activities.	5	
			Functional	intersects with	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties).	5	
4.3	_ :	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity & data privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	
			Functional	intersects with	AI & Autonomous Technologies Targeted Application Scope	AAT-04.3	Mechanisms exist to specify and document the targeted application scope of the proposed use and operation of Artificial Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to document and validate the scope of cybersecurity & data privacy	5	
			Functional	intersects with	Compliance Scope	CPL-01.2	controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
4.4	AI management system	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	subset of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
5.0	l eadersnin	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional Functional	no relationship	N/A N/A	N/A N/A	N/A N/A	N/A N/A	No requirements to map to. No requirements to map to.
			Functional	intersects with	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
			Functional	intersects with	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.	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	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	
			Functional	intersects with	AI & Autonomous Technologies Requirements Definitions	AAT-14	Mechanisms exist to take socio-technical implications into account to address risks associated with Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			Functional	intersects with	AI & Autonomous Technologies Ongoing Assessments	AAT-11.2	Mechanisms exist to conduct regular assessments of Artificial Intelligence (AI) and Autonomous Technologies (AAT) with independent assessors and stakeholders not involved in the development of the AAT.	5	
			Functional	intersects with	AI & Autonomous Technologies Viability Decisions	AAT-15	Mechanisms exist to define the criteria as to whether Artificial Intelligence (AI) and Autonomous Technologies (AAT) achieved intended purposes and stated objectives to determine whether its development or deployment should proceed.	5	
			Functional	intersects with	AI & Autonomous Technologies Stakeholder Competencies	AAT-13.1	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related operator and practitioner proficiency requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT) are defined, assessed and documented.	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
			Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy	(optional) 5	
5.1	Leadership and commitmen	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Risk Management Resourcing	RSK-01.2	program measures of performance. Mechanisms exist to reduce the magnitude or likelihood of potential impacts by resourcing the capability required to manage technology-related risks.	5	
		Tittps.// www.iso.org/standard/01230.html	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	
			Functional	subset of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
			Functional	intersects with	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
			Functional	intersects with	AI & Autonomous Technologies Internal Controls	AAT-02.2	Mechanisms exist to identify and document internal cybersecurity & data privacy controls for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	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	
			Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	
			Functional	intersects with	Business As Usual (BAU) Secure Practices	GOV-14	Mechanisms exist to incorporate cybersecurity & data privacy principles into Business As Usual (BAU) practices through executive leadership involvement.	5	
			Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
5.2	Al policy	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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(a)	Al policy	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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)	Al policy	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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(c)	Al policy	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	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)	Al policy	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Updating AI & Autonomous Technologies	AAT-10.14	Mechanisms exist to integrate continual improvements for deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			Functional	intersects with	AI & Autonomous Technologies Continuous Improvements	AAT-07.3	Mechanisms exist to continuously improve Artificial Intelligence (AI) and Autonomous Technologies (AAT) capabilities to maximize benefits and minimize negative impacts associated with AAT.	5	
			Functional	intersects with	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for human-Al configurations and oversight of Al systems.	5	
			Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
5.3	•		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	
	authorities	https://www.iso.org/standard/81230.html	Functional	intersects with	Responsibility To Supersede, Deactivate and/or Disengage AI & Autonomous Technologies	AAT-15.2	Mechanisms exist to define the criteria and responsible party(ies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AAT) that demonstrate performance or outcomes inconsistent with intended use.	5	
			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	
5.3(a)	Roles, responsibilities and	Buy a copy of ISO 42001 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	
3.3(a)	authorities	https://www.iso.org/standard/81230.html	Functional	intersects with	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for human-Al configurations and oversight of Al systems.	5	
5.3(b)	•	Buy a copy of ISO 42001 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	
	authorities	https://www.iso.org/standard/81230.html	Functional	intersects with	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for human-Al configurations and oversight of Al systems.	5	
6.0	Planning	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
6.1	Actions to address risks and opportunities	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
			Functional	intersects with	Updating AI & Autonomous Technologies AI & Autonomous	AAT 02.1	Mechanisms exist to integrate continual improvements for deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to identify Artificial Intelligence (AI) and Autonomous Technologies	5	
			Functional	intersects with	Technologies Risk Mapping		(AAT) in use and map those components to potential legal risks, including statutory and regulatory compliance requirements. Mechanisms exist to facilitate the implementation of strategic, operational and	5	
6.1.1	General	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	subset of	Risk Management Program AI & Autonomous	RSK-01	tactical risk management controls. Mechanisms exist to document the risks and potential impacts of Artificial Intelligence	10	
			Functional	intersects with	Technologies Risk Profiling Al & Autonomous	AAT-09	(AI) and Autonomous Technologies (AAT) designed, developed, deployed, evaluated and used. Mechanisms exist to leverage decision makers from a diversity of demographics,	5	
			Functional	intersects with	Technologies Risk Management Decisions	AAT-07	disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
			Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to document the risks and potential impacts of Artificial Intelligence	10	
			Functional	intersects with	AI & Autonomous Technologies Risk Profiling	AAT-09	(AI) and Autonomous Technologies (AAT) designed, developed, deployed, evaluated and used.	5	
6.1.2	Al risk assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
			Functional	intersects with	AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.	5	
			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	intersects with	Risk Register Risk Management Program	RSK-04.1 RSK-01	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks. Mechanisms exist to facilitate the implementation of strategic, operational and	5 10	
			i anctional	JUNICE UI	Al & Autonomous	W3K-01	tactical risk management controls. Mechanisms exist to leverage decision makers from a diversity of demographics,	10	
6.1.2(a)	Al risk assessment	Buy a copy of ISO 42001 for control content:	Functional	intersects with	Technologies Risk Management Decisions	AAT-07	disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
]		https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts. Mechanisms exist to conduct recurring assessments of risk that includes the likelihood.	5	
		_		1	ī	ı	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood	Í	I



				Relationship		SCF#	Control Description	(optional)	Notes (optional)
			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	AI & Autonomous Technologies Risk	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and	5	
6.1.2(b)	Al risk assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Management Decisions AI & Autonomous Technologies Likelihood &	AAT-07.2	managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks. Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous	5	
			Functional	intersects with	Impact Risk Analysis Risk Assessment	RSK-04	Technologies (AAT) in similar contexts. Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption,	5	
			Functional	intersects with	Unmeasurable AI & Autonomous Technologies	AAT-16.3	modification or destruction of the organization's systems and data. Mechanisms exist to identify and document unmeasurable risks or trustworthiness characteristics.	5	
			Functional	intersects with	Risks Previously Unknown AI & Autonomous Technologies	AAT-17.3	Mechanisms exist to respond to and recover from a previously unknown Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified.	5	
			Functional	intersects with	Threats & Risks 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	
6.1.2(c)	AI risk assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional Functional	intersects with	Material Risks AI & Autonomous Technologies Likelihood &		Mechanisms exist to define criteria necessary to designate a risk as a material risk. Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous	5	
			Functional	intersects with	AI & Autonomous Technologies Risk	AAT-07	Technologies (AAT) in similar contexts. Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and	5	
			Functional	intersects with	Management Decisions Risk Assessment	RSK-04	managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks. Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption,	5	
					AI & Autonomous		modification or destruction of the organization's systems and data. Mechanisms exist to identify and document negative, residual risks (defined as the		
			Functional	intersects with	Technologies Negative Residual Risks	AAT-15.1	sum of all unmitigated risks) to both downstream acquirers and end users of Artificial Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to conduct recurring assessments of risk that includes the likelihood	5	
			Functional	intersects with	Risk Assessment	RSK-04	and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data. Mechanisms exist to identify:	5	
			Functional	intersects with	Risk Framing	RSK-01.1	 (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing 	5	
6.1.2(d)	Al risk assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	subset of	Risk Management Program	RSK-01	risk. Mechanisms exist to facilitate the implementation of strategic, operational and	10	
			Functional	intersects with	AI & Autonomous Technologies Likelihood &		tactical risk management controls. Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous	5	
			Functional	intersects with	Impact Risk Analysis AI & Autonomous Technologies Risk	AAT-07	Technologies (AAT) in similar contexts. Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and	5	
			Functional	intersects with	Management Decisions Material Risks	GOV-16.1	managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks. Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5	
			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,	5	
			Functional	intersects with	AI & Autonomous Technologies Likelihood &	AAT-07.2	modification or destruction of the organization's systems and data. Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous	5	
6.1.2(d)(1)	AI risk assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Impact Risk Analysis Risk Framing	RSK-01.1	Technologies (AAT) in similar contexts. 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	5	
			Functional	intersects with	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
			Functional Functional	intersects with intersects with	Material Risks Material Risks		Mechanisms exist to define criteria necessary to designate a risk as a material risk. Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5 5	
			Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
6.1.2(d)(2)	Al risk assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
			Functional	intersects with	AI & Autonomous Technologies Likelihood &	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous	5	
			Functional	intersects with	Impact Risk Analysis Risk Assessment	RSK-04	Technologies (AAT) in similar contexts. Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption,	5	
			Functional	intersects with	Risk Framing	RSK-01.1	modification or destruction of the organization's systems and data. 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	5	
			Functional	intersects with	Risk Assessment	RSK-∩⁄I	(4) Priorities, benefits and trade-offs considered by the organization for managing risk. Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption,	5	
6.1.2(d)(3)	Al risk assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html			AI & Autonomous		modification or destruction of the organization's systems and data. Mechanisms exist to leverage decision makers from a diversity of demographics,	-	
			Functional Functional	intersects with	Technologies Risk Management Decisions Material Risks		disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks. Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5	
			Functional	intersects with	AI & Autonomous Technologies Likelihood &		Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous	5	
			Functional	intersects with	Impact Risk Analysis Material Risks	GOV-16.1	Technologies (AAT) in similar contexts. Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5	
			Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data. Mechanisms exist to facilitate the implementation of strategic, operational and	5	
			Functional	subset of	Risk Management Program	RSK-01	tactical risk management controls.	10	
6.1.2(e)	Al risk assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
		The state of the s	Functional	intersects with	AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.	5	
			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	



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 Functional	intersects with	Risk Framing Material Risks	RSK-01.1 GOV-16.1	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. Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5	
6.1.2(e)(1)	Al risk assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Risk Management Decisions		Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
			Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
			Functional	intersects with	AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.	5	
			Functional	intersects with	AI & Autonomous Technologies Risk Management Decisions AI & Autonomous	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks. Mechanisms exist to define the potential likelihood and impact of each identified risk	5	
			Functional Functional	intersects with	Technologies Likelihood & Impact Risk Analysis Risk Ranking	AAT-07.2 RSK-05	based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts. Mechanisms exist to identify and assign a risk ranking to newly discovered security	5	
		Buy a copy of ISO 42001 for control content:	Functional	intersects with	Impact-Level Prioritization	RSK-02.1	vulnerabilities that is based on industry-recognized practices. Mechanisms exist to prioritize the impact level for systems, applications and/or	5	
6.1.2(e)(2)	Al risk assessment	https://www.iso.org/standard/81230.html	T directional	mersees with	impact zever rionalzation	NON OZII	services to prevent potential disruptions. Mechanisms exist to identify:		
			Functional	intersects with	Risk Framing	RSK-01.1	 (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing 	5	
			Functional	intersects with	Material Risks	GOV-16.1		5	
			Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data. Mechanisms exist to facilitate the implementation of strategic, operational and	5	
			Functional	subset of	Risk Management Program	RSK-01	tactical risk management controls.	10	
6.1.3	AI risk treatment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
			Functional	intersects with	Risk Response	RSK-06.1 RSK-06	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	
			Functional	intersects with	Risk Remediation	RSK-06.1	Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to respond to findings from cybersecurity & data privacy	5	
			Functional	intersects with	Risk Response	K3K-00.1	assessments, incidents and audits to ensure proper remediation has been performed. Mechanisms exist to facilitate the implementation of strategic, operational and	5	
6.1.3(a)	AI risk treatment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional Functional	subset of intersects with	Risk Management Program Risk Remediation	RSK-01 RSK-06	tactical risk management controls. Mechanisms exist to remediate risks to an acceptable level.	10 5	
		THELPS://www.iso.org/stanuard/61250.Html	Functional	intersects with	AI & Autonomous	K3K-U0	Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to leverage decision makers from a diversity of demographics,	5	
			Functional Functional	intersects with	Technologies Risk Management Decisions Risk Remediation		disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks. Mechanisms exist to remediate risks to an acceptable level.	5	
			Functional	intersects with	Al & Autonomous Technologies Risk Management Decisions		Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
6.1.3(b)	AI risk treatment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	
			Functional	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	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	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 Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
6.1.3(c)	AI risk treatment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
			Functional	intersects with	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	
			Functional	intersects with	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
			Functional	intersects with	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
6.1.3(d)	AI risk treatment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Risk Management Decisions		Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks. Mechanisms exist to facilitate the implementation of strategic, operational and	5	
			Functional	subset of	Risk Management Program	RSK-01	tactical risk management controls.	10	
			Functional	intersects with	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	
			Functional Functional	intersects with intersects with	Risk Remediation Risk Remediation	RSK-06 RSK-06	Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to remediate risks to an acceptable level.	5 5	
64.24.3	Al wiels Assess	Buy a copy of ISO 42001 for control content:	Functional	intersects with	AI & Autonomous Technologies Risk Management Decisions		Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
6.1.3(e)	Al risk treatment	https://www.iso.org/standard/81230.html	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 Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	
			Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
6.1.3(f)	AI risk treatment	Buy a copy of ISO 42001 for control content:	Functional	intersects with	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
		https://www.iso.org/standard/81230.html	Functional	intersects with	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed. Mechanisms exist to facilitate the implementation of strategic, operational and	5	
			Functional	subset of	Risk Management Program	RSK-01	tactical risk management controls.	10	
			Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to remediate risks to an acceptable level	10	
6.1.3(g)	AI risk treatment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
		The state of the s	Functional	intersects with	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
					ivianagement Decisions		indiaging Actincial intelligence (Al) and Autonomous Technologies (AAT)-related risks.		



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 Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
6.1.4	Al system impact assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
			Functional	intersects with	AI & Autonomous Technologies Risk Profiling	AAT-09	Mechanisms exist to document the risks and potential impacts of Artificial Intelligence (AI) and Autonomous Technologies (AAT) designed, developed, deployed, evaluated and used.	5	
			Functional	intersects with	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	5	
			Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
			Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
6.2	Al objectives and planning to achieve them	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system. Mechanisms exist to monitor mission/business-critical services or functions to ensure	5	
	At a his atives and alamains to	During against ICO 42004 for control contents	Functional	intersects with	Purpose Validation	GOV-11	those resources are being used consistent with their intended purpose.	5	
6.2(a)	achieve them	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
6.2(b)	Al objectives and planning to achieve them	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
6.2(c)	AI objectives and planning to achieve them	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
6.2(d)	Al objectives and planning to achieve them	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
6.2(e)	AI objectives and planning to achieve them	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
6.2(f)	Al objectives and planning to achieve them	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
6.2(g)	AI objectives and planning to achieve them	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
		During against ISO 42004 for control contents	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
6.3	Planning of changes	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program. Mechanisms exist to prohibit unauthorized changes, unless organization-approved	10	
7.0	Support	Buy a copy of ISO 42001 for control content:	Functional Functional	intersects with no relationship	Prohibition Of Changes N/A	CHG-02.1 N/A	change requests are received. N/A	5 N/A	No requirements to map to.
7.0	Зиррогі	https://www.iso.org/standard/81230.html	Functional	intersects with	Updating AI & Autonomous	AAT-10.14	Mechanisms exist to integrate continual improvements for deployed Artificial	5	No requirements to map to.
			Functional	subset of	Technologies Cybersecurity & Data Privacy Portfolio Management	PRM-01	Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving	10	
7.1	Resources	Buy a copy of ISO 42001 for control content:	Functional	intersects with	Allocation of Resources	PRM-03	cybersecurity & data privacy objectives. Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.	5	
,. <u>.</u>	Resources	https://www.iso.org/standard/81230.html	Functional	intersects with	Trustworthy AI & Autonomous Technologies	AAT-01.2	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) are designed to be reliable, safe, fair, secure, resilient, transparent, explainable and data privacy-enhanced to minimize emergent properties or unintended consequences.	5	
			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	
			Functional	intersects with	Al & Autonomous Technologies Training	AAT-05	Mechanisms exist to ensure personnel and external stakeholders are provided with position-specific risk management training for Artificial Intelligence (AI) and	5	
			Functional	subset of	Human Resources Security Management	HRS-01	Autonomous Technologies (AAT). Mechanisms exist to facilitate the implementation of personnel security controls.	10	
			Functional	intersects with	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
			Functional	intersects with	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
7.2	Competence	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Al & Autonomous Technologies Stakeholder	AAT-13.1	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related operator and practitioner proficiency requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT) are defined, assessed and	5	
			Functional	intersects with	Roles With Special Protection Measures	HRS-04.1	documented. Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined	5	
			Functional	intersects with	Position Categorization	HRS-02	personnel screening criteria. Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
			Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
			Functional	intersects with	Formal Indoctrination	HRS-04.2	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information are formally indoctrinated for all the relevant types of information to which they have access on the system.	5	
			Functional	intersects with	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	5	
			Functional	intersects with	Use of Mobile Devices	HRS-05.5	used maliciously. 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	
		Buy a copy of ISO 42001 for control content:	Functional	intersects with	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5	
7.3	Awareness	https://www.iso.org/standard/81230.html	Functional	intersects with	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's cybersecurity & data privacy policies and provide acknowledgement.	5	
			Functional Functional	intersects with	Use of Critical Technologies Rules of Behavior	HRS-05.4 HRS-05.1	Mechanisms exist to govern usage policies for critical technologies. Mechanisms exist to define acceptable and unacceptable rules of behavior for the use	5	
			Functional	intersects with	Terms of Employment	HRS-05.1 HRS-05	of technologies, including consequences for unacceptable behavior. Mechanisms exist to require all employees and contractors to apply cybersecurity &	5	
			Functional	intersects with	Access Agreements	HRS-06	data privacy principles in their daily work. Mechanisms exist to require internal and third-party users to sign appropriate access	5	
			Functional	intersects with	Social Media & Social Networking Restrictions		agreements prior to being granted access. 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	5	
			Functional	intersects with	Personnel Sanctions	HRS-07	and sharing account information. Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
			Functional	subset of	Artificial Intelligence (AI) & Autonomous Technologies	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous	10	
			i uncuonal	วนมระเ 01	Governance	AA1-U1	Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
			Functional	intersects with	Robust Stakeholder Engagement for AI &	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about	(optional) 5	
7.4	Communication	Buy a copy of ISO 42001 for control content:			Autonomous Technologies Cybersecurity & Data Privacy	PRM-04	positive, negative and unanticipated impacts. Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented	_	
7.4	Communication	https://www.iso.org/standard/81230.html	Functional	intersects with	In Project Management	PRIM-04	correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
							Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: (1) The resulting risk to organizational operations, assets, individuals and other		
			Functional	intersects with	Business Process Definition	PRM-06	organizations; and (2) Information protection needs arising from the defined business processes and	5	
		Buy a copy of ISO 42001 for control content:					revises the processes as necessary, until an achievable set of protection needs is obtained.		
7.5	Documented information	https://www.iso.org/standard/81230.html	Functional	no relationship	N/A Cybersecurity & Data	N/A	N/A Mechanisms exist to facilitate the implementation of cybersecurity & data protection	N/A	No requirements to map to.
			Functional	subset of	Protection Governance Program	GOV-01	governance controls. Mechanisms exist to identify and document Standardized Operating Procedures (SOP),	10	
7.5.1	General	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	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	
			Functional	intersects with	Publishing Cybersecurity & Data Protection	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
7.5.1(a)	General	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Standardized Operating	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned	5	
		inttps.//www.iso.org/standard/61230.ittilii	Functional	subset of	Procedures (SOP) Cybersecurity & Data Protection Governance	GOV-01	tasks. Mechanisms exist to facilitate the implementation of cybersecurity & data protection	10	
			Functional	Subset of	Program Standardized Operating	907-01	governance controls. Mechanisms exist to identify and document Standardized Operating Procedures (SOP),		
			Functional	intersects with	Procedures (SOP) Cybersecurity & Data	OPS-01.1	or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
7.5.1(b)	General	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	subset of	Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
			Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	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	Standardized Operating	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned	5	
7.5.2	Creating and updating documented information	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	subset of	Procedures (SOP) Cybersecurity & Data Protection Governance	GOV-01	tasks. Mechanisms exist to facilitate the implementation of cybersecurity & data protection	10	
			Functional	subset of	Program Periodic Review & Update of	GOV-01	governance controls. Mechanisms exist to review the cybersecurity & data privacy program, including	10	
			Functional	intersects with	Cybersecurity & Data Protection Program Sensitive / Regulated Data	GOV-03	policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
			Functional	intersects with	Protection Publishing Cybersecurity &		Mechanisms exist to protect sensitive/regulated data wherever it is stored. Mechanisms exist to establish, maintain and disseminate cybersecurity & data	5	
			Functional	intersects with	Data Protection Documentation	GOV-02	protection policies, standards and procedures. Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized	5	
			Functional Functional	intersects with subset of	Disclosure of Information Data Protection	DCH-03.1 DCH-01	parties with a need to know. Mechanisms exist to facilitate the implementation of data protection controls.	5 10	
7.5.3	Control of documented information	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	
			Functional	intersects with	Defining Access Authorizations for Sensitive/Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.	5	
			Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned	5	
			Functional Functional	subset of	Data Protection Operations Security	DCH-01 OPS-01	Mechanisms exist to facilitate the implementation of data protection controls. Mechanisms exist to facilitate the implementation of operational security controls.	10	
			Functional	intersects with	Sensitive / Regulated Data Protection	<u> </u>	Mechanisms exist to racintate the implementation of operational security controls. Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
			Functional	intersects with	Defining Access Authorizations for	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.	5	
7.5.3(a)	Control of documented	Buy a copy of ISO 42001 for control content:	Functional	subset of	Sensitive/Regulated Data Cybersecurity & Data Protection Governance	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection	10	
(4)	information	https://www.iso.org/standard/81230.html			Program Publishing Cybersecurity &		governance controls. Mechanisms exist to establish, maintain and disseminate cybersecurity & data	10	
			Functional	intersects with	Data Protection Documentation	GOV-02	protection policies, standards and procedures. Mechanisms exist to identify and document Standardized Operating Procedures (SOP),	5	
			Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
			Functional	intersects with	Disclosure of Information Disclosure of Information	DCH-03.1 DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know. Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized	5	
			Functional Functional	intersects with	Defining Access Authorizations for	DCH-03.1	parties with a need to know. Mechanisms exist to explicitly define authorizations for specific individuals and/or	5	
			Functional	intersects with	Sensitive/Regulated Data Sensitive / Regulated Data		roles for logical and /or physical access to sensitive/regulated data. Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
			Functional	subset of	Protection Cybersecurity & Data Protection Governance	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection	10	
7.5.3(b)	Control of documented information	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html			Program Standardized Operating		governance controls. Mechanisms exist to identify and document Standardized Operating Procedures (SOP),		
			Functional	intersects with	Procedures (SOP)		or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
			Functional	subset of	Operations Security Publishing Cybersecurity &	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls. Mechanisms exist to establish, maintain and disseminate cybersecurity & data	10	
			Functional Functional	intersects with subset of	Data Protection Documentation Data Protection	GOV-02 DCH-01	protection policies, standards and procedures. Mechanisms exist to facilitate the implementation of data protection controls.	10	
8.0	Operation	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
			Functional	intersects with	AI & Autonomous Technologies Internal Controls	AAT-02.2	Mechanisms exist to identify and document internal cybersecurity & data privacy controls for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			Functional	intersects with	AI & Autonomous Technologies-Related Legal Requirements Definition	AAT-01.1	Mechanisms exist to identify, understand, document and manage applicable statutory and regulatory requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			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	
			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	5	
							operating as intended.		



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)
8.1	Operational planning and control	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required cybersecurity & data privacy controls for each system, application and/or service under their control are implemented correctly and are operating as intended.	5	
	Control	The part of the pa	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service	5	
			Functional	intersects with	Operationalizing Cybersecurity & Data	GOV-15	under their control. Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service	5	
			Functional	subset of	Protection Practices Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	under their control. Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented	10	
			Functional	intersects with	Implement Controls	GOV-15.2	effectively. Mechanisms exist to compel data and/or process owners to implement required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
			Functional	intersects with	AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.	5	
			Functional	subset of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
			Functional	intersects with	Situational Awareness of AI & Autonomous Technologies	AAT-02	Mechanisms exist to develop and maintain an inventory of Artificial Intelligence (AI) and Autonomous Technologies (AAT) (internal and third-party).	5	
8.2	Al risk assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Risk Mapping	AAT-02.1	Mechanisms exist to identify Artificial Intelligence (AI) and Autonomous Technologies (AAT) in use and map those components to potential legal risks, including statutory and regulatory compliance requirements.	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	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
			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	
		Buy a copy of ISO 42001 for control content:	Functional	intersects with	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
8.3	AI risk treatment	https://www.iso.org/standard/81230.html	Functional	intersects with	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	
			Functional Functional	intersects with	Risk Remediation Business Impact Analysis (BIA)	RSK-06 RSK-08	Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	5	
			Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
8.4	AI system impact assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	intersects with	Al & Autonomous Technologies Impact	AAT-07.1	Mechanisms exist to characterize the impacts of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities,	5	
9.0	Performance evaluation	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	no relationship	Characterization N/A	N/A	organizations and society. N/A	N/A	No requirements to map to.
9.1	_	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related testing, identification of incidents and information sharing	5	
9.2	Internal audit	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
			Functional	intersects with	AI & Autonomous Technologies Ongoing Assessments	AAT-11.2	Mechanisms exist to conduct regular assessments of Artificial Intelligence (AI) and Autonomous Technologies (AAT) with independent assessors and stakeholders not involved in the development of the AAT.	5	
9.2.1	General	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	AI TEVV Trustworthiness Assessment	AAT-10.1	Mechanisms exist to evaluate Artificial Intelligence (AI) and Autonomous Technologies (AAT) for trustworthy behavior and operation including security, anonymization and disaggregation of captured and stored data for approved purposes.	5	
			Functional	intersects with	AI TEVV Trustworthiness Assessment	AAT-10.1	Mechanisms exist to evaluate Artificial Intelligence (AI) and Autonomous Technologies (AAT) for trustworthy behavior and operation including security, anonymization and disaggregation of captured and stored data for approved purposes.	5	
9.2.1(a)	General	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Ongoing Assessments	AAT-11.2	Mechanisms exist to conduct regular assessments of Artificial Intelligence (AI) and Autonomous Technologies (AAT) with independent assessors and stakeholders not involved in the development of the AAT.	5	
			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	AI TEVV Trustworthiness Assessment	AAT-10.1	Mechanisms exist to evaluate Artificial Intelligence (AI) and Autonomous Technologies (AAT) for trustworthy behavior and operation including security, anonymization and disaggregation of captured and stored data for approved purposes.	5	
9.2.1(a)(1)	General	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	AI & Autonomous Technologies Ongoing Assessments	AAT-11.2	Mechanisms exist to conduct regular assessments of Artificial Intelligence (AI) and Autonomous Technologies (AAT) with independent assessors and stakeholders not involved in the development of the AAT.	5	
			Functional	intersects with	AI TEVV Trustworthiness Assessment	AAT-10.1	Mechanisms exist to evaluate Artificial Intelligence (AI) and Autonomous Technologies (AAT) for trustworthy behavior and operation including security, anonymization and disaggregation of captured and stored data for approved purposes.	5	
9.2.1(a)(2)	General	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Ongoing Assessments	AAT-11.2	Mechanisms exist to conduct regular assessments of Artificial Intelligence (AI) and Autonomous Technologies (AAT) with independent assessors and stakeholders not involved in the development of the AAT.	5	
			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	
		Buy a copy of ISO 42001 for control content:	Functional	intersects with	AI TEVV Trustworthiness Assessment	AAT-10.1	Mechanisms exist to evaluate Artificial Intelligence (AI) and Autonomous Technologies (AAT) for trustworthy behavior and operation including security, anonymization and disaggregation of captured and stored data for approved purposes. Mechanisms exist to implement an internal audit function that is capable of providing	5	
9.2.1(b)	General	https://www.iso.org/standard/81230.html	Functional	intersects with	Internal Audit Function	CPL-02.1	senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
			Functional	intersects with	AI & Autonomous Technologies Ongoing Assessments	AAT-11.2	Mechanisms exist to conduct regular assessments of Artificial Intelligence (AI) and Autonomous Technologies (AAT) with independent assessors and stakeholders not involved in the development of the AAT.	5	
9.2.2	Internal audit programme	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
9.2.2(a)	Internal audit programme	Buy a copy of ISO 42001 for control content:	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	
		https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Targeted Application Scope	AAT-04.3	Mechanisms exist to specify and document the targeted application scope of the proposed use and operation of Artificial Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to implement an internal audit function that is capable of providing	5	
		1	1	intersects with	Internal Audit Function	l	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the	-	l

ISO 42001:2023



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)
J.Z.Z(0)	internal addit programme	https://www.iso.org/standard/81230.html	Functional	intersects with	Independent Assessors		Mechanisms exist to utilize independent assessors to evaluate cybersecurity & data protection controls at planned intervals or when the system, service or project	5	
			Functional	intersects with	Internal Audit Function	CPL-02.1	undergoes significant changes. Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the	5	
9.2.2(c)	Internal audit programme	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	organization's technology and information governance processes. 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	Managament rovious	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
9.3.1	General	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
		Tittps.//www.iso.org/stanuaru/61230.iitiiii	Functional	intersects with	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
9.3.2	Management review inputs	Buy a copy of ISO 42001 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	
		https://www.iso.org/standard/81230.html	Functional	intersects with	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
			Functional	intersects with	Robust Stakeholder Engagement for AI &	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about	5	
			Functional	intersects with	Autonomous Technologies Risk Register	RSK-04.1	positive, negative and unanticipated impacts. Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
9.3.2(a)	Management review inputs	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
			Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnorabilities.	5	
			Functional	intersects with	Robust Stakeholder Engagement for AI &	AAT-11	eliminate known vulnerabilities. Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about	5	
			Functional	intersects with	Autonomous Technologies Risk Register	RSK-04.1	positive, negative and unanticipated impacts. Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
9.3.2(b)	Management review inputs	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
			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	
			Functional	intersects with	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
9.3.2(c)	Management review inputs	Buy a copy of ISO 42001 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	
9.3.2(C)	Management review inputs	https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Stakeholder Feedback Integration	AAT-11.1	Mechanisms exist to regularly collect, consider, prioritize and integrate risk-related feedback from those external to the team that developed or deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			Functional	intersects with	Stakeholder Identification & Involvement	$I \Delta SI - 0.1.7$	Mechanisms exist to identify and involve pertinent stakeholders of critical systems, applications and services to support the ongoing secure management of those assets.	5	
			Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
9.3.2(d)	Management review inputs	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Robust Stakeholder Engagement for AI & Autonomous Technologies		Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts. Mechanisms exist to coordinate cybersecurity, data protection and business alignment	5	
			Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	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	
			Functional	intersects with	Robust Stakeholder Engagement for AI & Autonomous Technologies		Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
9.3.2(d)(1)	Management review inputs	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Steering Committee & Program Oversight	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	
			Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
		Duran and ISO 42004 for control contract	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 inputs	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	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	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
9.3.2(d)(3)	Management review inputs	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
		Tittps.//www.iso.org/stanuaru/61230.html	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	
			Functional	intersects with	Robust Stakeholder Engagement for AI & Autonomous Technologies		Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
9.3.2(e)	Management review inputs	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
			Functional	intersects with	Updating AI & Autonomous Technologies AI & Autonomous	AAT-10.14	Mechanisms exist to integrate continual improvements for deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to continuously improve Artificial Intelligence (AI) and Autonomous	5	
		Pure a convention 42004 for the second	Functional	intersects with	Technologies Continuous Improvements		Technologies (AAT) capabilities to maximize benefits and minimize negative impacts associated with AAT. Mechanisms exist to continuously improve Artificial intelligence (AI) and Autonomous Technologies (AAT) capabilities to maximize benefits and minimize negative impacts associated with AAT.	5	
9.3.3	Management review results	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	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 42001 for control content: https://www.iso.org/standard/81230.html	Functional	no relationship	N/A AI & Autonomous	N/A	N/A Mechanisms exist to continuously improve Artificial Intelligence (AI) and Autonomous	N/A	No requirements to map to.
10.1	Continual improvement	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Technologies Continuous Improvements	AAT-07.3	Technologies (AAT) capabilities to maximize benefits and minimize negative impacts associated with AAT.	5	
			Functional	intersects with	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
			Functional	intersects with	AI & Autonomous Technologies Risk Response	AAT-18.1	Mechanisms exist to prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output.	5	
			Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to require system developers and integrators to develop and	5	
10.2	Nonconformity and corrective action	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Developer Threat Analysis & Flaw Remediation	TDA-15	implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	
			Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
			Functional	intersects with	Previously Unknown AI & Autonomous Technologies Threats & Risks	AAT-17.3	Mechanisms exist to respond to and recover from a previously unknown Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified.	5	
			Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
			Functional	intersects with	Vulnerability Remediation Process Previously Unknown AI &	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
			Functional	intersects with	Autonomous Technologies Threats & Risks	AAT-17.3	Mechanisms exist to respond to and recover from a previously unknown Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified.	5	
			Functional	intersects with	AI & Autonomous Technologies Risk Response	AAT-18.1	Mechanisms exist to prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output.	5	
10.2(a)	Nonconformity and	Buy a copy of ISO 42001 for control content:	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar	5	
. ,	corrective action	https://www.iso.org/standard/81230.html	Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
			Functional	intersects with	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	
			Functional	intersects with	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
			Functional	intersects with	Risk Remediation Threat Analysis & Flaw	RSK-06	Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to require system developers and integrators to create and execute	5	
			Functional	intersects with	Remediation During Development	IAO-04	a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
			Functional	intersects with	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	
10.2(a)(1)	Nonconformity and corrective action	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Risk Response	AAT-18.1	Mechanisms exist to prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output.	5	
			Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
			Functional	intersects with	Previously Unknown AI & Autonomous Technologies Threats & Risks	AAT-17.3	Mechanisms exist to respond to and recover from a previously unknown Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified.	5	
			Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
			Functional	intersects with	Previously Unknown AI & Autonomous Technologies Threats & Risks	AAT-17.3	Mechanisms exist to respond to and recover from a previously unknown Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified.	5	
			Functional	intersects with	AI & Autonomous Technologies Risk Response	AAT-18.1	Mechanisms exist to prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output.	5	
			Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar	5	
10.2(a)(2)	Nonconformity and corrective action	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
			Functional	intersects with	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
			Functional	intersects with	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	
			Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated. Mechanisms exist to prioritize, respond to and remediate Artificial Intelligence (AI)	5	
			Functional	intersects with	AI & Autonomous Technologies Risk Response	AAT-18.1	and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output.	5	
			Functional	intersects with	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	
			Functional Functional	intersects with	Risk Remediation Vulnerability Remediation	RSK-06 VPM-02	Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and	5	
10.2(b)	Nonconformity and corrective action	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Process Previously Unknown AI & Autonomous Technologies	AAT-17.3	Mechanisms exist to respond to and recover from a previously unknown Artificial	5	
			Functional	intersects with	Threats & Risks Threat Analysis & Flaw Remediation During	IAO-04	Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified. Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and	5	
			Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	remediate flaws during development. Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or	5	
			Functional	intersects with	Threat Analysis & Flaw Remediation During Development	IAO-04	eliminate known vulnerabilities. Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
			Functional	intersects with	Al & Autonomous Technologies Risk Response	AAT-18.1	Mechanisms exist to prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other	5	
			Functional	intersects with	Plan of Action & Milestones	IAO-05	analytical output. Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or	5	
10.2(b)(1)	Nonconformity and corrective action	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	(POA&M) Risk Remediation	RSK-06	deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities. Mechanisms exist to remediate risks to an acceptable level.	5	
			Functional	intersects with	Previously Unknown AI & Autonomous Technologies Threats & Risks	AAT-17.3	Mechanisms exist to respond to and recover from a previously unknown Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified.	5	
			Functional	intersects with	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	
			Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
			Functional	intersects with	AI & Autonomous Technologies Risk Response	AAT-18.1	Mechanisms exist to prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output.	5	
			Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
			Functional	intersects with	Risk Remediation Vulnerability Remediation		eliminate known vulnerabilities. Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and	5	
10 2/h\/2\	Nonconformity and	Buy a copy of ISO 42001 for control content:	Functional	intersects with	Process	VPM-02	remediated.	5	<u> </u>



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(b)(2)	corrective action	https://www.iso.org/standard/81230.html	Functional	intersects with	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	
			Functional	intersects with	Previously Unknown AI & Autonomous Technologies Threats & Risks	AAT-17.3	Mechanisms exist to respond to and recover from a previously unknown Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified.	5	
			Functional	intersects with	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
			Functional Functional	intersects with	Risk Remediation Al & Autonomous		Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other	5	
			Functional	intersects with	Technologies Risk Response Previously Unknown AI & Autonomous Technologies	AAT-17.3	analytical output. Mechanisms exist to respond to and recover from a previously unknown Artificial	5	
			- anctional	micersects with	Threats & Risks Developer Threat Analysis &	7411 2715	Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified. Mechanisms exist to require system developers and integrators to develop and		
10.2(b)(3)	Nonconformity and corrective action	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Flaw Remediation	TDA-15	implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production. Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar	5	
			Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
			Functional	intersects with	Vulnerability Remediation Process Threat Applysis & Flaw	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated. Mechanisms exist to require system developers and integrators to create and execute.	5	
			Functional	intersects with	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
			Functional	intersects with	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
			Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
			Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
10.2(c)	Nonconformity and corrective action	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	
			Functional	intersects with	AI & Autonomous Technologies Risk Response	AAT-18.1	Mechanisms exist to prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output.	5	
			Functional Functional	intersects with	Previously Unknown AI & Autonomous Technologies Threats & Risks Risk Remediation	AAT-17.3 RSK-06	Mechanisms exist to respond to and recover from a previously unknown Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified. Mechanisms exist to remediate risks to an acceptable level.	5	
			Functional	intersects with	Al & Autonomous Technologies Risk Response		Mechanisms exist to Princulate HSRS to an acceptable level. Mechanisms exist to prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output.	5	
			Functional	intersects with	Previously Unknown AI & Autonomous Technologies Threats & Risks	AAT-17.3	Mechanisms exist to respond to and recover from a previously unknown Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified.	5	
10.2(d)	Nonconformity and	Buy a copy of ISO 42001 for control content:	Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
`,	corrective action	https://www.iso.org/standard/81230.html	Functional	intersects with	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	
			Functional	intersects with	Risk Remediation Threat Analysis & Flaw	RSK-06	Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to require system developers and integrators to create and execute	5	
			Functional	intersects with	Remediation During Development Vulnerability Remediation	IAO-04	a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development. Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and	5	
			Functional	intersects with	Process Previously Unknown AI &	VPM-02	remediated. Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
			Functional	intersects with	Autonomous Technologies Threats & Risks	AAT-17.3	Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified. Mechanisms exist to require system developers and integrators to develop and	5	
			Functional	intersects with	Developer Threat Analysis & Flaw Remediation Threat Analysis & Flaw	TDA-15	implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production. Mechanisms exist to require system developers and integrators to create and execute	5	
10.2(e)	Nonconformity and	Buy a copy of ISO 42001 for control content:	Functional	intersects with	Remediation During Development	IAO-04	a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
10.2(e)	corrective action	https://www.iso.org/standard/81230.html	Functional Functional	intersects with	Risk Remediation Vulnerability Remediation Process	RSK-06 VPM-02	Mechanisms exist to remediate risks to an acceptable level. Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
			Functional	intersects with	Al & Autonomous Technologies Risk Response	AAT-18.1	Mechanisms exist to prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output.	5	
			Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or	5	
A.1	General	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	no relationship	N/A	N/A	eliminate known vulnerabilities. N/A	N/A	No requirements to map to.
A.2	Policies related to Al	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
A.2.2	Al policy	Buy a copy of ISO 42001 for control content:	Functional	subset of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
		https://www.iso.org/standard/81230.html	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	
A.2.3	Alignment with other organizational policies	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
A.2.4	Review of the Al policy	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
A.3	Internal organization	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks. Mechanisms exist to establish an authoritative chain of command with clear lines of	5	
			Functional	intersects with	Authoritative Chain of Command	GOV-04.2	communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
			Functional	intersects with	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for human-Al configurations and oversight of Al systems.	5	
		Buy a copy of ISO 42001 for control content:	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
A.3.2	AI roles and responsibilities	https://www.iso.org/standard/81230.html	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	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	
			Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
							Mechanisms exist to cover: (1) Preparation;	(optional)	
			Functional	intersects with	Incident Handling	IRO-02	(2) Automated event detection or manual incident report intake; (3) Analysis;	5	
							(4) Containment; (5) Eradication; and		
					AI & Autonomous		(6) Recovery. Mechanisms exist to regularly collect, consider, prioritize and integrate risk-related		
A.3.3	Reporting of concerns	Buy a copy of ISO 42001 for control content:	Functional	intersects with	Technologies Stakeholder Feedback Integration	AAT-11.1	feedback from those external to the team that developed or deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
7 11.51.5	neporting or concerns	https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Continuous	AAT-07.3	Mechanisms exist to continuously improve Artificial Intelligence (AI) and Autonomous Technologies (AAT) capabilities to maximize benefits and minimize negative impacts	5	
					Improvements Robust Stakeholder		associated with AAT. Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence		
			Functional	intersects with	Engagement for AI & Autonomous Technologies	AAT-11	(AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
			Functional	intersects with	Al & Autonomous Technologies Ongoing	AAT-11.2	Mechanisms exist to conduct regular assessments of Artificial Intelligence (AI) and Autonomous Technologies (AAT) with independent assessors and stakeholders not involved in the development of the AAT.	5	
			Functional	intersects with	Assessments Al & Autonomous Technologies End User	ΛΛΤ ₋ 11 2	Mechanisms exist to collect and integrate feedback from end users and impacted communities into Artificial Intelligence (AI) and Autonomous Technologies (AAT)-	5	
			runctional	microccis with	Feedback	AAT 11.5	related system evaluation metrics. Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies	3	
			Functional	intersects with	Trustworthy AI & Autonomous Technologies	AAT-01.2	(AAT) are designed to be reliable, safe, fair, secure, resilient, transparent, explainable and data privacy-enhanced to minimize emergent properties or unintended	5	
A.4	Resources for AI systems	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html			Artificial Intelligence (AI) 9.		consequences. Mechanisms exist to ensure policies, processes, procedures and practices related to		
			Functional	subset of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented	10	
					Cybersecurity & Data Privacy		effectively. Mechanisms exist to identify critical system components and functions by performing		
			Functional	intersects with	Requirements Definition	PRM-05	a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
			Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
A.4.2	Resource documentation	Buy a copy of ISO 42001 for control content:	Functional	intersects with	Cybersecurity & Data Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to	5	
A.4.2	Nesource documentation	https://www.iso.org/standard/81230.html			iii ri oject Waliagement		meeting the requirements. Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-		
			Functional	subset of	Cybersecurity & Data Privacy Portfolio Management	PRM-01	related resource planning controls that define a viable plan for achieving cybersecurity & data privacy-	10	
			Functional	intersects with	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects	5	
		Buy a copy of ISO 42001 for control content:					/ initiatives. Mechanisms exist to identify and document data sources utilized in the training	_	
A.4.3	Data resources	https://www.iso.org/standard/81230.html	Functional	intersects with	Data Source Identification AI & Autonomous	AAT-12.1	and/or operation of Artificial Intelligence and Autonomous Technologies (AAT). Mechanisms exist to specify and document the targeted application scope of the	5	
A.4.4	Tooling resources	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Technologies Targeted Application Scope	AAT-04.3	proposed use and operation of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
		inceps.// www.iso.org/standard/01250.intiiii	Functional	intersects with	Situational Awareness of AI & Autonomous Technologies	AAT-02	Mechanisms exist to develop and maintain an inventory of Artificial Intelligence (AI) and Autonomous Technologies (AAT) (internal and third-party).	5	
	System and computing	Buy a copy of ISO 42001 for control content:	Functional	intersects with	Situational Awareness of AI & Autonomous Technologies	AAT-02	Mechanisms exist to develop and maintain an inventory of Artificial Intelligence (AI) and Autonomous Technologies (AAT) (internal and third-party).	5	
A.4.5	resources	https://www.iso.org/standard/81230.html	Functional	intersects with	Al & Autonomous Technologies Targeted	AAT-04.3	Mechanisms exist to specify and document the targeted application scope of the proposed use and operation of Artificial Intelligence (AI) and Autonomous	5	
					Application Scope Al & Autonomous		Technologies (AAT). Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related operator and practitioner proficiency requirements for Artificial		
			Functional	intersects with	Technologies Stakeholder Competencies	AAT-13.1	Intelligence (AI) and Autonomous Technologies (AAT) are defined, assessed and documented.	5	
A.4.6	Human resources	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Stakeholder	AAT-13	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholder competencies, skills and capacities incorporate demographic	5	
		,,	- unetional	microccio with	Diversity	700113	diversity, broad domain and user experience expertise.	, j	
			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	
	Assessing impacts of Al	Buy a copy of ISO 42001 for control content:	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
A.5	Assessing impacts of Al systems	https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies-Related Legal	AAT-01.1	Mechanisms exist to identify, understand, document and manage applicable statutory and regulatory requirements for Artificial Intelligence (AI) and Autonomous	5	
			Functional	intersects with	Requirements Definition Security Impact Analysis for	CHG-03	Technologies (AAT). Mechanisms exist to analyze proposed changes for potential security impacts, prior to	5	
A.5.2	Al system impact assessment process	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Changes Stakeholder Notification of	CHG-05	the implementation of the change. Mechanisms exist to ensure stakeholders are made aware of and understand the	5	
			Functional	:	Changes AI & Autonomous	AAT 02.4	impact of proposed changes. Mechanisms exist to identify Artificial Intelligence (AI) and Autonomous Technologies	_	
			Functional	intersects with	Technologies Risk Mapping Al & Autonomous	AA1-02.1	(AAT) in use and map those components to potential legal risks, including statutory and regulatory compliance requirements. Mechanisms exist to identify, understand, document and manage applicable statutory	5	
			Functional	intersects with	Technologies-Related Legal Requirements Definition	AAT-01.1	and regulatory requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			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,	5	
					Security Impact Analysis for	CUC 03	modification or destruction of the organization's systems and data. Mechanisms exist to analyze proposed changes for potential security impacts, prior to		
A.5.3	Documentation of AI system	Buy a copy of ISO 42001 for control content:	Functional	intersects with	Changes AI & Autonomous	CHG-03	the implementation of the change. Mechanisms exist to assess potential costs, including non-monetary costs, resulting	5	
A.3.3	impact assessments	https://www.iso.org/standard/81230.html	Functional	intersects with	Technologies Potential Costs Analysis	AAT-04.2	from expected or realized Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related errors or system functionality and trustworthiness.	5	
			Functional	intersects with	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	5	
			Functional	intersects with	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes. Mechanisms exist to characterize the impacts of proposed Artificial Intelligence (AI)	5	
			Functional	intersects with	AI & Autonomous Technologies Impact Characterization	AAT-07.1	Mechanisms exist to characterize the impacts of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities,	5	
			Functional	intersects with	Characterization Data Protection Impact	RSK-10	organizations and society. Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to	5	
	<u> </u>		runcuonal	miler sects WITH	Assessment (DPIA)	NON-1U	identify and remediate reasonably-expected risks. Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems,	3	
			Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
			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,	5	
					AI & Autonomous	 .	modification or destruction of the organization's systems and data. Mechanisms exist to identify, understand, document and manage applicable statutory	-	
			Functional	intersects with	Technologies-Related Legal Requirements Definition	AAT-01.1	and regulatory requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
	Assessing Al system impact		Functional	intersects with	AI & Autonomous Technologies Requirements	AAT-14	Mechanisms exist to take socio-technical implications into account to address risks associated with Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
A.5.4	on individuals or groups of individuals	https://www.iso.org/standard/81230.html			Definitions Al & Autonomous		Mechanisms exist to identify Artificial Intelligence (AI) and Autonomous Technologies		
			Functional	intersects with	Technologies Risk Mapping	AAT-02.1	(AAT) in use and map those components to potential legal risks, including statutory and regulatory compliance requirements.	5	
			Functional	intersects with	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	5	
			Functional	intersects with	Al & Autonomous Technologies Impact	AAT-07.1	Mechanisms exist to characterize the impacts of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities,	5	
			I		Characterization		organizations and society. Mechanisms exist to assess potential costs, including non-monetary costs, resulting		
			F	time .	Al & Autonomous	A A -	· · · · · · · · · · · · · · · · · · ·	<u> </u>	
			Functional	intersects with	AI & Autonomous Technologies Potential Costs Analysis AI & Autonomous	AAT-04.2	from expected or realized Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related errors or system functionality and trustworthiness. Mechanisms exist to assess potential costs, including non-initially costs, resulting from expected years, resulting from expected	5	



Al systems Al system life cycle Management guidance for Al system development Objectives for responsible	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with subset of subset of	AI & Autonomous Technologies Risk Mapping Business Impact Analysis (BIA) AI & Autonomous Technologies Potential Costs	RSK-08 AAT-04.2 AAT-07.1 RSK-10 AAT-14 RSK-04 N/A	Mechanisms exist to identify Artificial Intelligence (AI) and Autonomous Technologies (AAT) in use and map those components to potential legal risks, including statutory and regulatory compliance requirements. Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks. Mechanisms exist to assess potential costs, including non-monetary costs, resulting from expected or realized Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related errors or system functionality and trustworthiness. Mechanisms exist to characterize the impacts of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities, organizations and society. Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks. Mechanisms exist to take socio-technical implications into account to address risks associated with Artificial Intelligence (AI) and Autonomous Technologies (AAT). 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.	(optional) 5 5 5 5 5 N/A	
Al systems Al system life cycle Management guidance for Al system development Objectives for responsible	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional Functional Functional Functional Functional Functional Functional	intersects with intersects with intersects with intersects with no relationship subset of	Business Impact Analysis (BIA) AI & Autonomous Technologies Potential Costs Analysis AI & Autonomous Technologies Impact Characterization Data Protection Impact Assessment (DPIA) AI & Autonomous Technologies Requirements Definitions Risk Assessment N/A Technology Development &	AAT-04.2 AAT-07.1 RSK-10 AAT-14 RSK-04 N/A	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks. Mechanisms exist to assess potential costs, including non-monetary costs, resulting from expected or realized Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related errors or system functionality and trustworthiness. Mechanisms exist to characterize the impacts of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities, organizations and society. Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks. Mechanisms exist to take socio-technical implications into account to address risks associated with Artificial Intelligence (AI) and Autonomous Technologies (AAT). 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 5 5	
Al systems Al system life cycle Management guidance for Al system development Objectives for responsible	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional Functional Functional Functional Functional Functional	intersects with intersects with intersects with intersects with no relationship subset of	Technologies Potential Costs Analysis AI & Autonomous Technologies Impact Characterization Data Protection Impact Assessment (DPIA) AI & Autonomous Technologies Requirements Definitions Risk Assessment N/A Technology Development &	AAT-04.2 AAT-07.1 RSK-10 AAT-14 RSK-04 N/A	Mechanisms exist to assess potential costs, including non-monetary costs, resulting from expected or realized Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related errors or system functionality and trustworthiness. Mechanisms exist to characterize the impacts of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities, organizations and society. Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks. Mechanisms exist to take socio-technical implications into account to address risks associated with Artificial Intelligence (AI) and Autonomous Technologies (AAT). 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 5 5	
Al systems Al system life cycle Management guidance for Al system development Objectives for responsible	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional Functional Functional Functional Functional	intersects with intersects with intersects with no relationship subset of	AI & Autonomous Technologies Impact Characterization Data Protection Impact Assessment (DPIA) AI & Autonomous Technologies Requirements Definitions Risk Assessment N/A Technology Development &	RSK-10 AAT-14 RSK-04 N/A	Mechanisms exist to characterize the impacts of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities, organizations and society. Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks. Mechanisms exist to take socio-technical implications into account to address risks associated with Artificial Intelligence (AI) and Autonomous Technologies (AAT). 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 5	
Management guidance for Al system development Objectives for responsible	https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content:	Functional Functional Functional Functional	intersects with intersects with no relationship subset of	Data Protection Impact Assessment (DPIA) AI & Autonomous Technologies Requirements Definitions Risk Assessment N/A Technology Development &	RSK-10 AAT-14 RSK-04 N/A	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks. Mechanisms exist to take socio-technical implications into account to address risks associated with Artificial Intelligence (AI) and Autonomous Technologies (AAT). 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	
Management guidance for Al system development Objectives for responsible	https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content:	Functional Functional Functional	intersects with no relationship subset of	AI & Autonomous Technologies Requirements Definitions Risk Assessment N/A Technology Development &	RSK-04 N/A	Mechanisms exist to take socio-technical implications into account to address risks associated with Artificial Intelligence (AI) and Autonomous Technologies (AAT). 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	
Management guidance for Al system development Objectives for responsible	https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content:	Functional Functional Functional	intersects with no relationship subset of	Definitions Risk Assessment N/A Technology Development &	RSK-04 N/A	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	
Management guidance for Al system development Objectives for responsible	https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content:	Functional Functional	no relationship subset of	N/A Technology Development &	N/A	modification or destruction of the organization's systems and data.	-	
Management guidance for Al system development Objectives for responsible	https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content:	Functional Functional	subset of	Technology Development &	·	N/A	N/A	
Al system development Objectives for responsible	https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content:	Functional		Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique	10	No requirements to map to.
Al system development Objectives for responsible	https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content:		subset of	Cybersecurity & Data Privacy		business needs. Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-		
		Functional	İ	Portfolio Management	PRM-01	related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives. Mechanisms exist to facilitate the implementation of tailored development and	10	
			subset of	Technology Development & Acquisition	TDA-01	acquisition strategies, contract tools and procurement methods to meet unique business needs. Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies	10	
		Functional	intersects with	Trustworthy AI & Autonomous Technologies	AAT-01.2	(AAT) are designed to be reliable, safe, fair, secure, resilient, transparent, explainable and data privacy-enhanced to minimize emergent properties or unintended consequences.	5	
		Functional	intersects with	AI & Autonomous Technologies Implementation Tasks Definition	AAT-14.1	Mechanisms exist to define the tasks that Artificial Intelligence (AI) and Autonomous Technologies (AAT) will support (e.g., classifiers, generative models, recommenders).	5	
		Functional	intersects with	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5	
Processes for responsible Al	Buy a copy of ISO 42001 for control content:	Functional	intersects with	AI & Autonomous Technologies Intellectual Property Infringement Protections	AAT-12	Mechanisms exist to identify data sources for Artificial Intelligence (AI) and Autonomous Technologies (AAT) to prevent third-party Intellectual Property (IP) rights infringement.	5	
system design and development	https://www.iso.org/standard/81230.html	Functional	intersects with	Data Source Identification AI & Autonomous	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT). Mechanisms exist to identify and document knowledge limits of Artificial Intelligence	5	
		Functional	intersects with	Technologies Knowledge Limits		relevant stakeholder decision making.	5	
		Functional	subset of	Technology Development & Acquisition	TDA-01	Mechanisms exist to develop applications based on secure coding principles. Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
		Functional	intersects with	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Technologies (AAT)-related testing, identification of incidents and information sharing.		
Al system lite cycle		Functional	intersects with	Product Management	TDA-01.1		5	
		Functional	subset of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
		Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Poyelenment Life Cycle (SDLC)	5	
		Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC). Cycle (SDLC) are controlled through formal change control procedures.	5	
		Functional	intersects with	Cybersecurity & Data Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to	5	
Al system requirements and specification	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Minimum Viable Product	TDA-02	meeting the requirements. Mechanisms exist to ensure risk-based technical and functional specifications are established to define a Minimum Viable Product (MVP)	5	
		Functional	intersects with	AI & Autonomous Technologies Internal	AAT-02.2	Mechanisms exist to identify and document internal cybersecurity & data privacy	5	
		Functional	intersects with	Controls Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to update	5	
		Functional	intersects with	AI & Autonomous	ΔΔΤ-14	correct security deficiencies. Mechanisms exist to take socio-technical implications into account to address risks	5	
				Definitions Cybersecurity & Data Privacy		associated with Artificial Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to address all capital planning and investment requests, including		
		Functional	intersects with	Resource Management Al & Autonomous	PRM-02	the resources needed to implement the cybersecurity & data privacy programs and document all exceptions to this requirement. Mechanisms exist to identify and document knowledge limits of Artificial Intelligence	5	_
		Functional	intersects with	Technologies Knowledge Limits	AAT-14.2	(AI) and Autonomous Technologies (AAT) to provide sufficient information to assist relevant stakeholder decision making.	5	
		Functional	subset of	Technology Development & Acquisition	TDA-01	acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
		Functional	intersects with	AI & Autonomous Technologies Intellectual Property Infringement Protections	AAT-12	Mechanisms exist to identify data sources for Artificial Intelligence (AI) and Autonomous Technologies (AAT) to prevent third-party Intellectual Property (IP) rights infringement.	5	
		Functional	intersects with	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related testing, identification of incidents and information sharing.	5	
Documentation of Al system	Buy a copy of ISO 42001 for control content:	Functional	intersects with	AI & Autonomous Technologies Requirements Definitions	AAT-14	Mechanisms exist to take socio-technical implications into account to address risks associated with Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
		Functional	intersects with	AI & Autonomous Technologies Mission and Goals Definition	AAT-03.1	Mechanisms exist to define and document the organization's mission and defined goals for Artificial Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to require software developers to ensure that their software	5	
		Functional	intersects with	Development Methods, Techniques & Processes	1 1111/1/1/1/1/1/1/1/1/1/1/1/1/1/1/1/1/	development processes employ industry-recognized secure practices for secure	5	
		Functional	intersects with	AI & Autonomous Technologies Implementation Tasks Definition	AAT-14.1	Mechanisms exist to define the tasks that Artificial Intelligence (AI) and Autonomous Technologies (AAT) will support (e.g., classifiers, generative models, recommenders).	5	
		Functional	intersects with	Data Source Identification	AAT-12.1	and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
		Functional	intersects with	Technologies Business Case	AAT-04	benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
		Functional	intersects with	AI & Autonomous Technologies Model	AAT-10.9	Mechanisms exist to validate the Artificial Intelligence (AI) and Autonomous	5	
	Al system life cycle Al system requirements and specification	Al system life cycle Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Processes for responsible AI system design and development https://www.iso.org/standard/81230.html Functional	Processes for responsible AI system delign and development and system delign and development and system delign and development and development are set to see the system delign and development are set to see the system delign and development are set to see the system of 150 42001 for control content: https://www.iso.org/standard/81230.html	Processes for responsible Naystern long and control contents and even form one and control contents are set to the set of	Perceional Intersects with Perceional Intersects with Perceionage conscionation Perceional Perc	Production Pro	Part



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)
A.6.2.4	Al system verification and validation	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI TEVV Trustworthiness Assessment	AAT-10.1	Mechanisms exist to evaluate Artificial Intelligence (AI) and Autonomous Technologies (AAT) for trustworthy behavior and operation including security, anonymization and disaggregation of captured and stored data for approved purposes.	5	
			Functional	intersects with	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related testing, identification of incidents and information sharing.	5	
	A system deniovment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls. Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices;	10	
			Functional	intersects with	Specialized Assessments	IAO-02.2	 (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Automonous Technologies (AAT). 	5	
A.6.2.5			Functional	intersects with	AI & Autonomous Technologies Implementation Tasks Definition	AAT-14.1	Mechanisms exist to define the tasks that Artificial Intelligence (AI) and Autonomous Technologies (AAT) will support (e.g., classifiers, generative models, recommenders).	5	
			Functional	intersects with	Security Authorization	IAO-07	Mechanisms exist to ensure systems, projects and services are officially authorized prior to "go live" in a production environment.	5	
			Functional	intersects with	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical cybersecurity & data privacy controls.	5	
			Functional	intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity & data privacy controls in systems, applications and services through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
			Functional	intersects with	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related testing, identification of incidents and information sharing.	5	
	Al system operation and	Buy a copy of ISO 42001 for control content:	Functional	intersects with	AI TEVV Post-Deployment Monitoring	AAT-10.13	Mechanisms exist to proactively and continuously monitor deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
A.6.2.6	monitoring	https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Production Monitoring	AAT-16	Mechanisms exist to monitor the functionality and behavior of the deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
		Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
	Al system recording of event		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	
A.6.2.7			Functional	intersects with	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for systems that describe: (1) Secure configuration, installation and operation of the system; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	
			Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
			Functional	intersects with	Secure Practices Guidelines	OPS-05	Mechanisms exist to provide guidelines and recommendations for the secure use of products and/or services to assist in the configuration, installation and use of the product and/or service. Mechanisms exist to design and implement product management processes to update	5	
			Functional	intersects with	Product Management	TDA-01.1	products, including systems, software and services, to improve functionality and correct security deficiencies.	5	
			Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures. Mechanisms exist to define supporting business processes and implement appropriate	5	
			Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	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	
			Functional	intersects with	Secure Practices Guidelines	OPS-05	Mechanisms exist to provide guidelines and recommendations for the secure use of products and/or services to assist in the configuration, installation and use of the product and/or service.	5	
A.6.2.8			Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
			Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to update products, including systems, software and services, to improve functionality and correct security deficiencies.	5	
			Functional	intersects with	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for systems that describe: (1) Secure configuration, installation and operation of the system; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	
			Functional	intersects with	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
A.7	Data for All systems	Buy a copy of ISO 42001 for control content:	Functional	intersects with	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and deidentification of information across the information lifecycle.	5	
A. <i>7</i>	Data for Al systems	https://www.iso.org/standard/81230.html	Functional	intersects with	Trustworthy AI & Autonomous Technologies	AAT-01.2	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) are designed to be reliable, safe, fair, secure, resilient, transparent, explainable and data privacy-enhanced to minimize emergent properties or unintended consequences.	5	
A.7.2	<u> </u>	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and deidentification of information across the information lifecycle.	5	
	,		Functional	intersects with	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT). Mechanisms exist to identify and document data sources utilized in the training	5	
A.7.3	Acquisition of data	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional Functional	intersects with	Data Source Identification Data Quality Operations	DCH-22	and/or operation of Artificial Intelligence and Autonomous Technologies (AAT). Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-	5	
	Own Pro- China		Functional	intersects with	Data Source Identification	AAT-12.1	identification of information across the information lifecycle. Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
A.7.4	Quality of data for AI systems	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-	5	
			Functional	intersects with	Data Quality Operations	DCH-22	identification of information across the information lifecycle. Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and deidentification of information across the information lifecycle.	5	
A.7.5	Data provenance	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to systems, system components and associated data.	5	
			Functional	intersects with	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
A.7.6	Data preparation	Buy a copy of ISO 42001 for control content:	Functional	intersects with	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT). Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT)	5	
A.7.0	Data preparation	https://www.iso.org/standard/81230.html	Functional	intersects with	Data Quality Operations	DCH-22	data to ensure the accuracy, relevance, timeliness, impact, completeness and de- identification of information across the information lifecycle.	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
	Information for interested	Dura agree f ISO 42004 for control control	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	
A.8	parties of Al systems	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Robust Stakeholder Engagement for AI &	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about	5	
A.8.2			Functional	intersects with	Autonomous Technologies Stakeholder Identification & Involvement	AST-01.2	positive, negative and unanticipated impacts. Mechanisms exist to identify and involve pertinent stakeholders of critical systems, applications and services to support the ongoing secure management of those assets.	5	
	System documentation and information for users	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Robust Stakeholder Engagement for AI &	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about	5	
					Autonomous Technologies Robust Stakeholder		positive, negative and unanticipated impacts. Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence	-	
	I External renorting I		Functional	intersects with	Engagement for AI & Autonomous Technologies Stakeholder Identification &		(AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts. Mechanisms exist to identify and involve pertinent stakeholders of critical systems,	5	
A.8.3		Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Involvement Al & Autonomous	AST-01.2	applications and services to support the ongoing secure management of those assets. Mechanisms exist to communicate Artificial Intelligence (AI) and Autonomous	5	
			Functional	intersects with	Technologies Incident & Error Reporting	AAT-11.4	Technologies (AAT)-related incidents and/or errors to relevant stakeholders, including affected communities. Mechanisms exist to timely-report incidents to applicable:	5	
			Functional	intersects with	Incident Stakeholder Reporting	IRO-10	(1) Internal stakeholders; (2) Affected clients & third-parties; and	5	
			Functional	intersects with	Robust Stakeholder Engagement for AI &	AAT-11	(3) Regulatory authorities. Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about	5	
	Communication of incidents	Ruy a copy of ISO 42001 for control content:	Functional	intersects with	Autonomous Technologies Incident Stakeholder Reporting	IRO-10	positive, negative and unanticipated impacts. Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and	5	
A.8.4		Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Incident & Error	AAT-11.4	(3) Regulatory authorities. Mechanisms exist to communicate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related incidents and/or errors to relevant stakeholders, including	5	
					Reporting Stakeholder Identification &		affected communities. Mechanisms exist to identify and involve pertinent stakeholders of critical systems,	-	
			Functional	intersects with	Involvement Robust Stakeholder	AST-01.2	applications and services to support the ongoing secure management of those assets. Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence	5	
A.8.5	Information for interested parties	1 ' ' '	Functional	intersects with	Engagement for AI & Autonomous Technologies	AAT-11	(AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
	P. 2.2.	https://www.iso.org/standard/81230.html	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	
	I lise of Al systems	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
A.9			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	
	-	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
A.9.2			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	
A.9.3	1 -	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
			Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
	Intended use of the AI system	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
A.9.4			Functional	intersects with	Al TEVV Post-Deployment Monitoring	AAT-10.13	Mechanisms exist to proactively and continuously monitor deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
	Third-party and customer relationships	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain. Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM)	5	
			Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
A.10			Functional	intersects with	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	5	
			Functional	subset of	Third-Party Management Responsible, Accountable,	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls. Mechanisms exist to document and maintain a Responsible, Accountable, Supportive,	10	
			Functional	intersects with	Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs). Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM)	5	
	I Allocating responsibilities I	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
			Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
A.10.2			Functional Functional	subset of	Third-Party Management Supply Chain Protection	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls. Mechanisms exist to evaluate security risks associated with the services and product	10 5	
			Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-03	assignment for cybersecurity & data privacy controls between internal stakeholders	5	
			Functional	intersects with	Third-Party Services	TPM-04	and External Service Providers (ESPs). Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	5	
	I Siinniiers I	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
			Functional	intersects with	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
			Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
A.10.3			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	
			Functional	intersects with	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	5	
			Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions	5	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
	Customers	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Context Definition	AAT-03	Mechanisms exist to establish and document the context surrounding Artificial Intelligence (AI) and Autonomous Technologies (AAT), including: (1) Intended purposes; (2) Potentially beneficial uses; (3) Context-specific laws and regulations; (4) Norms and expectations; and (5) Prospective settings in which the system(s) will be deployed.	5	
A.10.4			Functional	intersects with	AI & Autonomous Technologies-Related Legal Requirements Definition	AAT-01.1	Mechanisms exist to identify, understand, document and manage applicable statutory and regulatory requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
			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	

ISO 42001:2023

