Set Theory Relationship Mapping (STRM)

Reference Document : Secure Controls Framework (SCF) version 2024.3
Focal Document: ISO 42001:2023
Focal Document URL: https://www.iso.org/standard/81230.html
STRM URL: https://securecontrolsframework.com/content/strm/scf-2024-3-iso-42001-2023.pdf

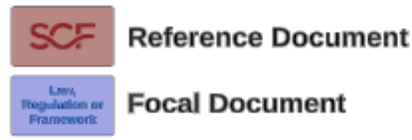
Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

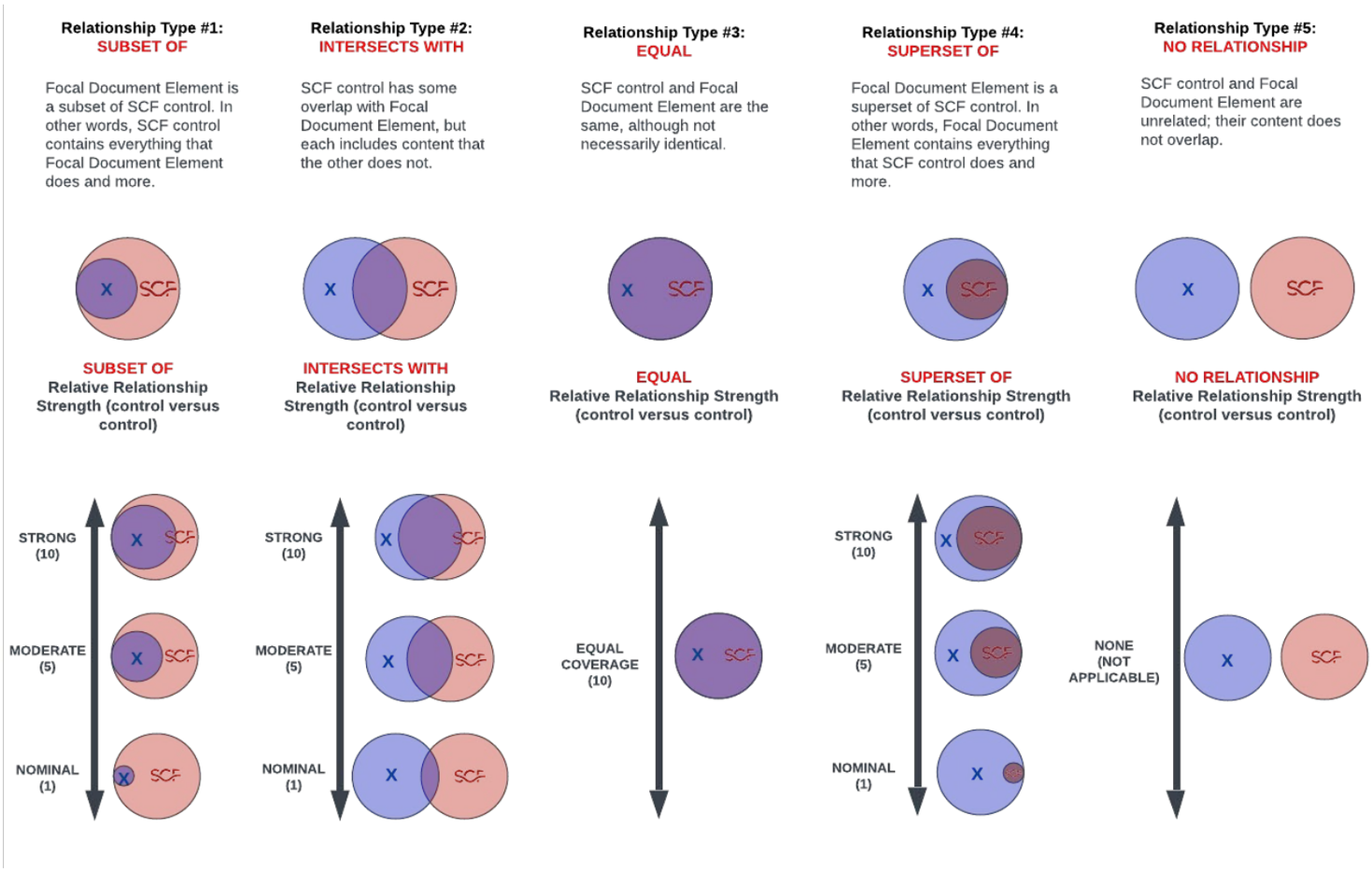
STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two concepts are related:

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 results 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**





Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
1.0	Scope	Buy a copy of ISO 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.
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.
4.1	Understanding the organization and its context	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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: ▪ The resulting risk to organizational operations, assets, individuals and other organizations; and ▪ 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	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: ▪ Intended purposes; ▪ Potentially beneficial uses; ▪ Context-specific laws and regulations; ▪ Norms and expectations; and ▪ 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	AAT-01.3	Mechanisms exist to sustain the value of deployed 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	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	
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	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 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	
			Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: ▪ The resulting risk to organizational operations, assets, individuals and other organizations; and ▪ 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).	5	
4.3	Determining the scope of the AI management system	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management 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	
			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).	5	
			Functional	intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
4.4	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	Leadership	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	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
5.1	Leadership and commitment	Buy a copy of ISO 42001 for control content:	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	
			Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
5.1	Leadership and commitment	https://www.iso.org/standard/81230.html	Functional	intersects with	Risk Management Resourcing	RSK-01.2	Mechanisms exist to reduce the magnitude or likelihood of potential impacts by resourcing the capability required to manage technology-related risks.	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	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	AI 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)	AI 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)	AI 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)	AI 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(d)	AI 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	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	
5.3	Roles, responsibilities and authorities	Buy a copy of ISO 42001 for control content: 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-AI configurations and oversight of AI systems.	5	
			Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
			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	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 authorities	Buy a copy of ISO 42001 for control content: 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	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems.	5	
5.3(b)	Roles, responsibilities and authorities	Buy a copy of ISO 42001 for control content: 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	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI 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.
6.1.1	General	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 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 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	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	
6.1.2	AI 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	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
			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	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	intersects with	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
6.1.2(a)	AI 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	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	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	
		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	
			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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
6.1.2(b)	AI risk assessment	Buy a copy of ISO 42001 for control content: 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.	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	
6.1.2(c)	AI risk assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Unmeasurable AI & Autonomous Technologies Risks	AAT-16.3	Mechanisms exist to identify and document unmeasurable risks or trustworthiness characteristics.	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	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
			Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
			Functional	intersects with	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	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	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	
			Functional	intersects with	AI & Autonomous Technologies Negative Residual Risks	AAT-15.1	Mechanisms exist to identify and document negative, residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers and end users of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
6.1.2(d)	AI risk assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
			Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: ▪ Assumptions affecting risk assessments, risk response and risk monitoring; ▪ Constraints affecting risk assessments, risk response and risk monitoring; ▪ The organizational risk tolerance; and ▪ Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
			Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
			Functional	intersects with	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	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	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	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	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	Risk Framing	RSK-01.1	Mechanisms exist to identify: ▪ Assumptions affecting risk assessments, risk response and risk monitoring; ▪ Constraints affecting risk assessments, risk response and risk monitoring; ▪ The organizational risk tolerance; and ▪ Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
			Functional	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	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5	
6.1.2(d)(2)	AI risk assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	5	
			Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: ▪ Assumptions affecting risk assessments, risk response and risk monitoring; ▪ Constraints affecting risk assessments, risk response and risk monitoring; ▪ The organizational risk tolerance; and ▪ Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
			Functional	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	
6.1.2(d)(3)	AI risk 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: ▪ Assumptions affecting risk assessments, risk response and risk monitoring; ▪ Constraints affecting risk assessments, risk response and risk monitoring; ▪ The organizational risk tolerance; and ▪ Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
			Functional	intersects with	Risk 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 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	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	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	
6.1.2(e)	AI risk assessment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Material Risks	GOV-16.1	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.	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	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: ▪ Assumptions affecting risk assessments, risk response and risk monitoring; ▪ Constraints affecting risk assessments, risk response and risk monitoring; ▪ The organizational risk tolerance; and ▪ Priorities, benefits and trade-offs considered by the organization for managing risk.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
6.1.2(e)(1)	AI risk 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: ▪ Assumptions affecting risk assessments, risk response and risk monitoring; ▪ Constraints affecting risk assessments, risk response and risk monitoring; ▪ The organizational risk tolerance; and ▪ Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
			Functional	intersects with	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	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	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	
6.1.2(e)(2)	AI 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 Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.	5	
			Functional	intersects with	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for systems, applications and/or services to prevent potential disruptions.	5	
			Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: ▪ Assumptions affecting risk assessments, risk response and risk monitoring; ▪ Constraints affecting risk assessments, risk response and risk monitoring; ▪ The organizational risk tolerance; and ▪ Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
			Functional	intersects with	Material Risks	GOV-16.1	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.	5	
6.1.3	AI risk treatment	Buy a copy of ISO 42001 for control content: 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	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	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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	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	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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	
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 Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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	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	
6.1.3(c)	AI risk treatment	Buy a copy of ISO 42001 for control content: 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 Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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	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	
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	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	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	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(e)	AI risk treatment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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	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	
6.1.3(f)	AI risk treatment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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	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	
6.1.3(g)	AI risk treatment	Buy a copy of ISO 42001 for control content: 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 Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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	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 Framing	RSK-01.1	Mechanisms exist to identify: ▪ Assumptions affecting risk assessments, risk response and risk monitoring; ▪ Constraints affecting risk assessments, risk response and risk monitoring; ▪ The organizational risk tolerance; and ▪ Priorities, benefits and trade-offs considered by the organization for managing risk.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
6.1.4	AI 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	
6.2	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	
			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.	5	
			Functional	intersects with	Purpose Validation	GOV-11	Mechanisms exist to monitor mission/business-critical services or functions to ensure those resources are being used consistent with their intended purpose.	5	
6.2(a)	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(b)	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(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)	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(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)	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(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	
6.3	Planning of changes	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
			Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
			Functional	intersects with	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	5	
7.0	Support	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.
7.1	Resources	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	subset of	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	10	
			Functional	intersects with	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	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	
7.2	Competence	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & 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 Autonomous Technologies (AAT).	5	
			Functional	subset of	Human Resources Security Management	HRS-01	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	
			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	
			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	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
			Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
7.3	Awareness	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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 used maliciously.	5	
			Functional	intersects with	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
			Functional	intersects with	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	
			Functional	intersects with	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	
			Functional	intersects with	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's cybersecurity & data privacy policies and provide acknowledgement.	5	
			Functional	intersects with	Use of Critical Technologies	HRS-05.4	Mechanisms exist to govern usage policies for critical technologies.	5	
			Functional	intersects with	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
			Functional	intersects with	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity & data privacy principles in their daily work.	5	
			Functional	intersects with	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	5	
			Functional	intersects with	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	5	
			Functional	intersects with	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
7.4	Communication	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	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	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 meeting the requirements.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: ▪ The resulting risk to organizational operations, assets, individuals and other organizations; and ▪ 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	
7.5	Documented information	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.
7.5.1	General	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	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	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
7.5.1(a)	General	Buy a copy of ISO 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	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	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
7.5.1(b)	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	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	subset of	Cybersecurity & Data 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	
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	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	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	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
			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	
7.5.3	Control of documented information	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	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	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
			Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
			Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
			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 tasks.	5	
7.5.3(a)	Control of documented information	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
			Functional	subset of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	
			Functional	intersects with	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
			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	subset of	Cybersecurity & Data 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	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	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
7.5.3(b)	Control of documented information	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
			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	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
			Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
			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	subset of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security 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	subset of	Data Protection	DCH-01	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.
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	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 operating as intended.	5	
			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	
			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 under their control.	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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
			Functional	subset of	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	Implement Controls	GOV-15.2	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	
8.2	AI risk assessment	Buy a copy of ISO 42001 for control content: 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.	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	
			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	
8.3	AI risk treatment	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	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	
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	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	Risk Framing	RSK-01.1	Mechanisms exist to identify: ▪ Assumptions affecting risk assessments, risk response and risk monitoring; ▪ Constraints affecting risk assessments, risk response and risk monitoring; ▪ The organizational risk tolerance; and ▪ Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
			Functional	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, organizations and society.	5	
9.0	Performance evaluation	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.
9.1	Monitoring, measurement, analysis and evaluation	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.
9.2.1	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)	General	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	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	
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	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	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	
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 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 & 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	
9.2.1(b)	General	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	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	
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: 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 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).	5	
9.2.2(b)	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	
			Functional	intersects with	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate cybersecurity & data protection controls at planned intervals or when the system, service or project undergoes significant changes.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
9.2.2(c)	Internal audit programme	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	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	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	Management review	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	
			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: 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	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(a)	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	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	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	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	
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	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	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	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	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	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	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	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	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	
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	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	
			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)(1)	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	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	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	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	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	
			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)(3)	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	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
9.3.2(e)	Management review inputs	Buy a copy of ISO 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	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	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	
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	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization’s cybersecurity & data protection program.	5	
10.0	Improvement	Buy a copy of ISO 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.
10.1	Continual improvement	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
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	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Test and Evaluation (ST&E) plan to identify and remediate flaws during development.	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.	5	
			Functional	intersects with	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.	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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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	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	
10.2(a)	Nonconformity and corrective action	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	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.	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	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.	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 Test and Evaluation (ST&E) plan to identify and remediate flaws during development.	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	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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 Test and Evaluation (ST&E) plan 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 create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.	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	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	
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	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.	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	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Test and Evaluation (ST&E) plan 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 create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.	5	
			Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	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	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	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.	5	
			Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Test and Evaluation (ST&E) plan 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	
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	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Test and Evaluation (ST&E) plan to identify and remediate flaws during development.	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	RSK-06	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 create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.	5	
			Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
10.2(b)(2)	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	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	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.	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 Test and Evaluation (ST&E) plan to identify and remediate flaws during development.	5	
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	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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	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 create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.	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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	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 Test and Evaluation (ST&E) plan to identify and remediate flaws during development.	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	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Test and Evaluation (ST&E) plan 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	
			Functional	intersects with	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.	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	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	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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	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	
10.2(d)	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 create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.	5	
			Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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 Test and Evaluation (ST&E) plan to identify and remediate flaws during development.	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	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.	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 Test and Evaluation (ST&E) plan to identify and remediate flaws during development.	5	
10.2(e)	Nonconformity and corrective action	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	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	
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	N/A	N/A	No requirements to map to.
A.2	Policies related to AI	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	AI policy	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	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 AI 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.	5	
			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	
A.3.2	AI roles and responsibilities	Buy a copy of ISO 42001 for control content: 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-AI configurations and oversight of AI systems.	5	
			Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
			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	
A.3.3	Reporting of concerns	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	
			Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
			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	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	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	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 End User Feedback	AAT-11.3	Mechanisms exist to collect and integrate feedback from end users and impacted communities into Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related system evaluation metrics.	5	
A.4	Resources for AI systems	Buy a copy of ISO 42001 for control content: 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	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 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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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.4.2	Resource documentation	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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 meeting the requirements.	5	
			Functional	subset of	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	10	
			Functional	intersects with	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	
A.4.3	Data resources	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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.4.4	Tooling resources	Buy a copy of ISO 42001 for control content: 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).	5	
			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	System and computing resources	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
			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).	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 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	
			Functional	intersects with	AI & Autonomous Technologies Stakeholder Diversity	AAT-13	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholder competencies, skills and capacities incorporate demographic diversity, broad domain and user experience expertise.	5	
			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.5	Assessing impacts of AI systems	Buy a copy of ISO 42001 for control content: 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	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	
A.5.2	AI system impact assessment process	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	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.	5	
A.5.3	Documentation of AI system impact assessments	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	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	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	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5	
			Functional	intersects with	AI & Autonomous Technologies Potential Costs Analysis	AAT-04.2	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.	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.	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, organizations and society.	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	
A.5.4	Assessing AI system impact on individuals or groups of individuals	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	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-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 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 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	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	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, organizations and society.	5	
			Functional	intersects with	AI & Autonomous Technologies Potential Costs Analysis	AAT-04.2	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.	5	
A.5.5	Assessing societal impacts of AI systems	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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 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	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	AI & Autonomous Technologies Potential Costs Analysis	AAT-04.2	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.	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, organizations and society.	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 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	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	
A.6	AI system life cycle	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.
A.6.1	Management guidance for AI system development	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	subset of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
			Functional	subset of	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	10	
			Functional	subset of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
A.6.1.2	Objectives for responsible development of AI system	Buy a copy of ISO 42001 for control content: 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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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.6.1.3	Processes for responsible AI system design and development	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
			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	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	
			Functional	intersects with	AI & Autonomous Technologies Knowledge Limits	AAT-14.2	Mechanisms exist to identify and document knowledge limits of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to provide sufficient information to assist relevant stakeholder decision making.	5	
			Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
			Functional	subset of	Technology Development & Acquisition	TDA-01	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	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.6.2	AI system life cycle	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
A.6.2.2	AI system requirements and specification	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	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	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	
			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 meeting the requirements.	5	
			Functional	intersects with	Minimum Viable Product (MVP) Security Requirements	TDA-02	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 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	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	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	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	
A.6.2.3	Documentation of AI system design and development	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Knowledge Limits	AAT-14.2	Mechanisms exist to identify and document knowledge limits of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to provide sufficient information to assist relevant stakeholder decision making.	5	
			Functional	subset of	Technology Development & Acquisition	TDA-01	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	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	
			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).	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	
			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	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence 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	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
A.6.2.4	AI system verification and validation	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	AI & Autonomous Technologies Model Validation	AAT-10.9	Mechanisms exist to validate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) model.	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	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.6.2.5	AI system deployment	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.	10	
			Functional	intersects with	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: ▪ Statutory, regulatory and contractual compliance obligations; ▪ Monitoring capabilities; ▪ Mobile devices; ▪ Databases; ▪ Application security; ▪ Embedded technologies (e.g., IoT, OT, etc.); ▪ Vulnerability management; ▪ Malicious code; ▪ Insider threats and ▪ Performance/load testing.	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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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	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.6.2.6	AI system operation and monitoring	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
			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	
A.6.2.7	AI system technical documentation	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	
			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	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for systems that describe: ▪ Secure configuration, installation and operation of the system; ▪ Effective use and maintenance of security features/functions; and ▪ 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.	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	
A.6.2.8	AI system recording of event logs	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	
			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	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	
			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: ▪ Secure configuration, installation and operation of the system; ▪ Effective use and maintenance of security features/functions; and ▪ Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	
A.7	Data for AI systems	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
			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-identification of information across the information lifecycle.	5	
			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	Data for development and enhancement of AI system	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-identification 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).	5	
A.7.3	Acquisition of data	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	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	
			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-identification of information across the information lifecycle.	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 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	
			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-identification 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	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-identification of information across the information lifecycle.	5	
			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: https://www.iso.org/standard/81230.html	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	
			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-identification of information across the information lifecycle.	5	
A.8	Information for interested parties of AI systems	Buy a copy of ISO 42001 for control content: 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	
			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	
A.8.2	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	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	
			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	
A.8.3	External reporting	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	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	
			Functional	intersects with	AI & Autonomous Technologies Incident & Error Reporting	AAT-11.4	Mechanisms exist to communicate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related incidents and/or errors to relevant stakeholders, including affected communities.	5	
			Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: ▪ Internal stakeholders; ▪ Affected clients & third-parties; and ▪ Regulatory authorities.	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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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.8.4	Communication of incidents	Buy a copy of ISO 42001 for control content: https://www.iso.org/standard/81230.html	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: ▪ Internal stakeholders; ▪ Affected clients & third-parties; and ▪ Regulatory authorities.	5	
			Functional	intersects with	AI & Autonomous Technologies Incident & Error Reporting	AAT-11.4	Mechanisms exist to communicate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related incidents and/or errors to relevant stakeholders, including affected communities.	5	
			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.8.5	Information for interested parties	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	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.9	Use of AI 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	
			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.9.2	Processes for responsible use of AI 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	
			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	Objectives for responsible use of 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	
			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.9.4	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	
			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	
			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.10	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.	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 and monitoring performance against those plans.	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	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
			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	
A.10.2	Allocating responsibilities	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	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 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	
			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	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	
A.10.3	Suppliers	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	
			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 and monitoring performance against those plans.	5	
A.10.4	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: ▪ Intended purposes; ▪ Potentially beneficial uses; ▪ Context-specific laws and regulations; ▪ Norms and expectations; and ▪ Prospective settings in which the system(s) will be deployed.	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 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	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)