NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **ISO 31000 - Risk management — Guidelines**
Focal Document URL: https://www.iso.org/standard/65694.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-iso-31000-2018.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1	Scope	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2	Normative references	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3	Terms and definitions	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4	Principles	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5	Framework	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
5.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	8	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.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 Security, Compliance & Resilience Program (SCRP).	5	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	8	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Assigned Security, Compliance & Resilience 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 Security, Compliance & Resilience Program (SCRP).	8	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.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 Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	8	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	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 Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	8	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Key Performance Indicators (KPIs)	GOV-05.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring and trend analysis of the Security, Compliance & Resilience Program (SCRP).	3	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Key Risk Indicators (KRIs)	GOV-05.2	Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the Security, Compliance & Resilience Program (SCRP).	3	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Business As Usual (BAU) Security, Compliance & Resilience Practices	GOV-14	Mechanisms exist to incorporate security, compliance and resilience principles into Business As Usual (BAU) practices through executive leadership involvement.	8	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are: (1) Implemented correctly; and (2) Operating as intended.	5	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	5	
5.2	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications, Services and/or Data (TAASD) under their control on an ongoing basis for applicable threats and risks, as well as to ensure security, compliance and resilience controls are operating as intended.	5	
5.3	Integration	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
5.3	Integration	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	8	
5.3	Integration	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	3	
5.3	Integration	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Prioritization To Address Evolving Risks & Threats	PRM-02.1	Mechanisms exist to integrate foundational cybersecurity practices with advanced technologies to maintain situation awareness of and minimize the organization's exposure to evolving risks and threats.	5	
5.3	Integration	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	5	
5.3	Integration	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience 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	
5.3	Integration	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	8	
5.3	Integration	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
5.3	Integration	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	8	
5.3	Integration	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.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	
5.4	Design	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.4.1	Understanding the organization and its context	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	8	
5.4.1	Understanding the organization and its context	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	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 security, compliance and resilience control system.	3	
5.4.1	Understanding the organization and its context	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5	
5.4.1	Understanding the organization and its context	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	8	
5.4.1	Understanding the organization and its context	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	8	
5.4.2	Articulating risk management commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	8	
5.4.2	Articulating risk management commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.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 Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	8	
5.4.2	Articulating risk management commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	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 Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	8	
5.4.2	Articulating risk management commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
5.4.2	Articulating risk management commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Materiality Determination	GOV-16	Mechanisms exist to define materiality threshold criteria capable of designating an incident as material.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
5.4.2	Articulating risk management commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	8	
5.4.2	Articulating risk management commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Material Threats	GOV-16.2	Mechanisms exist to define criteria necessary to designate a threat as a material threat.	8	
5.4.2	Articulating risk management commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience 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	
5.4.2	Articulating risk management commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
5.4.2	Articulating risk management commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
5.4.2	Articulating risk management commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	8	
5.4.2	Articulating risk management commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.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.	8	
5.4.2	Articulating risk management commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	8	
5.4.2	Articulating risk management commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Threshold	RSK-01.4	Mechanisms exist to define organizational risk threshold, the level of risk exposure above which risks are addressed and below which risks may be accepted.	8	
5.4.2	Articulating risk management commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	8	
5.4.3	Assigning organizational roles, authorities, responsibilities and accountabilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
5.4.3	Assigning organizational roles, authorities, responsibilities and accountabilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Assigned Security, Compliance & Resilience 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 Security, Compliance & Resilience Program (SCRP).	5	
5.4.3	Assigning organizational roles, authorities, responsibilities and accountabilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.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 Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
5.4.3	Assigning organizational roles, authorities, responsibilities and accountabilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	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 Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
5.4.3	Assigning organizational roles, authorities, responsibilities and accountabilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
5.4.4	Allocating resources	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
5.4.4	Allocating resources	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	8	
5.4.4	Allocating resources	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Targeted Capability Maturity Levels	PRM-01.2	Mechanisms exist to define and identify targeted capability maturity levels.	8	
5.4.4	Allocating resources	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	8	
5.4.4	Allocating resources	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Prioritization To Address Evolving Risks & Threats	PRM-02.1	Mechanisms exist to integrate foundational cybersecurity practices with advanced technologies to maintain situation awareness of and minimize the organization's exposure to evolving risks and threats.	5	
5.4.4	Allocating resources	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	8	
5.4.4	Allocating resources	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience 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	
5.4.4	Allocating resources	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.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.	8	
5.4.5	Establishing communication and consultation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
5.4.5	Establishing communication and consultation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience 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.	8	
5.4.5	Establishing communication and consultation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	8	
5.4.5	Establishing communication and consultation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
5.5	Implementation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	8	
5.5	Implementation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
5.5	Implementation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	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.	8	
5.5	Implementation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	8	
5.6	Evaluation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	8	
5.6	Evaluation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	8	
5.6	Evaluation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.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 Technology Assets, Applications, Services and/or Data (TAASD).	8	
5.7	Improvement	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.7.1	Adapting	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
5.7.2	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
5.7.2	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	5	
6	Process	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
6.2	Communication and consultation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
6.2	Communication and consultation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Formal Indoctrination	HRS-04.2	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.	8	
6.2	Communication and consultation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience 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.	8	
6.2	Communication and consultation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	8	
6.2	Communication and consultation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
6.2	Communication and consultation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
6.3	Scope, context and criteria	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.3.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
6.3.2	Defining the scope	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
6.3.3	External and internal context	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
6.3.4	Defining risk criteria	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	8	
6.3.4	Defining risk criteria	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Threshold	RSK-01.4	Mechanisms exist to define organizational risk threshold, the level of risk exposure above which risks are addressed and below which risks may be accepted.	8	
6.3.4	Defining risk criteria	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	8	
6.4	Risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.4.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.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 Technology Assets, Applications, Services and/or Data (TAASD).	8	
6.4.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	8	
6.4.2	Risk identification	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
6.4.2	Risk identification	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	8	
6.4.3	Risk analysis	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.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 Technology Assets, Applications, Services and/or Data (TAASD).	8	
6.4.3	Risk analysis	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	8	
6.4.4	Risk evaluation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.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 Technology Assets, Applications, Services and/or Data (TAASD).	8	
6.4.4	Risk evaluation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	8	
6.5	Risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.5.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Subset Of	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	10	
6.5.2	Selection of risk treatment options	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.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	
6.5.2	Selection of risk treatment options	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Treatment Options	RSK-06.3	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings.	8	
6.5.3	Preparing and implementing risk treatment plans	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Subset Of	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	10	
6.6	Monitoring and review	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.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 Security, Compliance & Resilience Program (SCRP).	5	
6.6	Monitoring and review	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
6.6	Monitoring and review	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
6.6	Monitoring and review	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
6.7	Recording and reporting	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/65694.html	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	