

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

Focal Document: ISO/IEC 27701: 2025 (Privacy information management systems)
Focal Document URL: <https://www.iso.org/standard/27701>
Published STRM URL: <https://content.securecontrolsframework.com/strm/scf-strm-general-iso-27701-2025.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/27701	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/27701	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3	Terms, definitions and abbreviations	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	10	
4	Context of the organization	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
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/27701	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	
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/27701	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.	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/27701	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.	5	
4.2	Understanding the needs and expectations of interested parties	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	8	
4.2	Understanding the needs and expectations of interested parties	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
4.2	Understanding the needs and expectations of interested parties	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
4.2(a)	Understanding the needs and expectations of interested parties	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
4.2(a)	Understanding the needs and expectations of interested parties	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
4.2(b)	Understanding the needs and expectations of interested parties	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
4.2(b)	Understanding the needs and expectations of interested parties	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
4.2(c)	Understanding the needs and expectations of interested parties	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
4.2(c)	Understanding the needs and expectations of interested parties	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
4.3	Determining the scope of the privacy information management system	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	10	
4.4	Privacy information management system	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
5	Leadership	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Security, Compliance & Resilience Program (SCRPR)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
5.1	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
5.1	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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 (SCRPR).	5	
5.1	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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 (SCRPR), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	5	
5.1	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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.	5	
5.1	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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 (SCRPR).	5	
5.1	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
5.1	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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.	5	
5.1	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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.	5	
5.1	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	8	
5.1	Leadership and commitment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program.	8	
5.2	Privacy policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
5.2(a)	Privacy policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
5.2(b)	Privacy policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
5.2(c)	Privacy policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
5.2(d)	Privacy policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
5.3	Roles, responsibilities and authorities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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 (SCRPR).	8	
5.3	Roles, responsibilities and authorities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
5.3	Roles, responsibilities and authorities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program.	8	
5.3(a)	Roles, responsibilities and authorities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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 (SCRPR).	8	
5.3(a)	Roles, responsibilities and authorities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
5.3(b)	Roles, responsibilities and authorities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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 (SCRPR).	10	
6	Planning	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.1	Actions to address risks and opportunities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.1.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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.	5	
6.1.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	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
6.1.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
6.1.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determine: (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	
6.1.1(a)	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
6.1.1(b)	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
6.1.2	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
6.1.2	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	8	
6.1.2(a)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
6.1.2(a)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
6.1.2(a)(1)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
6.1.2(a)(1)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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.	5	
6.1.2(a)(1)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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.	5	
6.1.2(a)(1)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
6.1.2(a)(2)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
6.1.2(a)(2)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
6.1.2(b)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
6.1.2(c)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	8	
6.1.2(c)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
6.1.2(c)(1)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
6.1.2(c)(2)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
6.1.2(d)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
6.1.2(d)(1)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
6.1.2(d)(2)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
6.1.2(d)(3)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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.	8	
6.1.2(d)(3)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
6.1.2(e)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
6.1.2(e)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
6.1.2(e)(1)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
6.1.2(e)(2)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	8	
6.1.2(e)(2)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	8	
6.1.2(e)(2)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	8	
6.1.2(e)(2)	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
6.1.3	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	8	
6.1.3	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments;	5	
6.1.3	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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(a)	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Equal	Risk Treatment Options	RSK-06.3	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings.	10	
6.1.3(b)	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	10	
6.1.3(c)	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
6.1.3(c)	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
6.1.3(d)	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
6.1.3(e)	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Statement of Applicability (SOA)	CPL-12	Mechanisms exist to produce a Statement of Applicability (SOA), or similar document, for compliance-related scoping activities.	10	
6.1.3(f)	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
6.1.3(g)	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
6.1.3(h)	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	8	
6.1.3(h)	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	8	
6.1.3(h)	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
6.1.3(h)	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5	
6.2	Privacy objectives and planning to achieve them	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
6.2(a)	Privacy objectives and planning to achieve them	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
6.2(b)	Privacy objectives and planning to achieve them	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
6.2(c)	Privacy objectives and planning to achieve them	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	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
6.2(d)	Privacy objectives and planning to achieve them	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PR1-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
6.2(e)	Privacy objectives and planning to achieve them	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PR1-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
6.2(e)	Privacy objectives and planning to achieve them	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Dissemination of Data Privacy Program Information	PR1-01.3	Mechanisms exist to: (1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; (2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; (3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy officer(s) regarding data privacy practices; and (4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.	8	
6.2(f)	Privacy objectives and planning to achieve them	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PR1-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
6.2(g)	Privacy objectives and planning to achieve them	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PR1-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
6.3	Planning of changes	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PR1-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
7	Support	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7.1	Resources	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PR1-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
7.1	Resources	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
7.1	Resources	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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.	5	
7.2	Competence	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
7.2	Competence	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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.	8	
7.2	Competence	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
7.2	Competence	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Continuing Professional Education (CPE) - Security, Compliance & Resilience Personnel	SAT-03.7	Mechanisms exist to ensure security, compliance and resilience personnel receive Continuing Professional Education (CPE) training to maintain currency and proficiency with industry-recognized secure practices that are pertinent to their assigned roles and responsibilities.	5	
7.3	Awareness	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
7.3	Awareness	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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.	8	
7.3	Awareness	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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.	8	
7.3	Awareness	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
7.4	Communication	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PR1-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
7.4	Communication	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Dissemination of Data Privacy Program Information	PR1-01.3	Mechanisms exist to: (1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; (2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; (3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy officer(s) regarding data privacy practices; and (4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.	5	
7.5	Documented information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7.5.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	8	
7.5.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PR1-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
7.5.1(a)	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PR1-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
7.5.1(b)	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
7.5.1(b)	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PR1-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
7.5.2	Creating and updating documented information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
7.5.2	Creating and updating documented information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PR1-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
7.5.3	Control of documented information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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	
7.5.3	Control of documented information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Privacy Program	PR1-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
7.5.3(a)	Control of documented information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Dissemination of Data Privacy Program Information	PR1-01.3	Mechanisms exist to: (1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; (2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; (3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy officer(s) regarding data privacy practices; and (4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.	10	
7.5.3(b)	Control of documented information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
7.5.3(b)	Control of documented information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	5	
8	Operation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.1	Operational planning and control	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
8.2	Privacy risk assessment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
8.3	Privacy risk treatment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	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.	5	
9	Performance evaluation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.1	Monitoring, measurement, analysis and evaluation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	10	
9.2	Internal audit	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.2.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Internal Audit Function	CP1-02.1	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.	10	
9.2.1(a)	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Internal Audit Function	CP1-02.1	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.	10	
9.2.1(b)	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Internal Audit Function	CP1-02.1	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.	10	
9.2.2	Internal audit programme	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	Security, Compliance & Resilience Controls Oversight	CP1-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	10	
9.2.2	Internal audit programme	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Periodic Audits	CP1-02.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	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
9.2.2(a)	Internal audit programme	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
9.2.2(b)	Internal audit programme	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
9.2.2(c)	Internal audit programme	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
9.3	Management review	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.3.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
9.3.1	General	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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 (SCRPR).	8	
9.3.2	Management review inputs	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
9.3.2(a)	Management review inputs	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
9.3.2(b)	Management review inputs	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
9.3.2(c)	Management review inputs	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
9.3.2(d)	Management review inputs	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
9.3.2(e)	Management review inputs	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
9.3.3	Management review results	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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.	10	
9.3.3	Management review results	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	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 (SCRPR), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	8	
10	Improvement	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10.1	Continual improvement	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Subset Of	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 (SCRPR), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	10	
10.2	Nonconformity and corrective action	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	8	
10.2(a)	Nonconformity and corrective action	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	8	
10.2(b)	Nonconformity and corrective action	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	8	
10.2(c)	Nonconformity and corrective action	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	8	
10.2(d)	Nonconformity and corrective action	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	8	
10.2(e)	Nonconformity and corrective action	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	8	
11	Further information on annexes	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/27701	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control