

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:

Focal Document URL:

Published STRM URL: <https://store.isaca.org/store#/store#/store/browse/detail/a254w00004k9ZEA5>
<https://content.securecontrolsframework.com/strm/scf-strm-general-cobit-2019.pdf>

Control Objectives for Information and Related Technologies (COBIT) (2019)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Security Controls Framework (SCF) Control Description	Strength of Relationship	Notes
EDM01.01	Evaluate the governance system	Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and evaluate the current and future design of governance of enterprise I&T.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRCP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
EDM01.02	Direct the governance system	Inform leaders on I&T governance principles and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of I&T in line with the agreed governance principles, decision-making models and authority levels. Define the information required for informed decision making.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRCP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
EDM01.03	Monitor the governance system	Monitor the effectiveness and performance of the enterprise's governance of I&T. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of I&T to enable value creation.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRCP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
EDM01.03	Monitor the governance system	Monitor the effectiveness and performance of the enterprise's governance of I&T. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of I&T to enable value creation.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRCP) measures of performance.	8	
EDM02.01	Establish the target investment mix	Review and ensure clarity of the enterprise and I&T strategies and current services. Define an appropriate investment mix based on cost, alignment with strategy, type of benefit for the programs in the portfolio, degree of risk, and financial measures such as cost and expected return on investment (ROI) over the full economic life cycle. Adjust the enterprise and I&T strategies where necessary.	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	
EDM02.01	Establish the target investment mix	Review and ensure clarity of the enterprise and I&T strategies and current services. Define an appropriate investment mix based on cost, alignment with strategy, type of benefit for the programs in the portfolio, degree of risk, and financial measures such as cost and expected return on investment (ROI) over the full economic life cycle. Adjust the enterprise and I&T strategies where necessary.	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 (SCRCP) and document all exceptions to this requirement.	8	
EDM02.01	Establish the target investment mix	Review and ensure clarity of the enterprise and I&T strategies and current services. Define an appropriate investment mix based on cost, alignment with strategy, type of benefit for the programs in the portfolio, degree of risk, and financial measures such as cost and expected return on investment (ROI) over the full economic life cycle. Adjust the enterprise and I&T strategies where necessary.	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	
EDM02.02	Evaluate value optimization	Continually evaluate the portfolio of I&T-enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value. Identify and evaluate any changes in direction to management that will optimize value creation.	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	
EDM02.02	Evaluate value optimization	Continually evaluate the portfolio of I&T-enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value. Identify and evaluate any changes in direction to management that will optimize value creation.	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 (SCRCP) and document all exceptions to this requirement.	8	
EDM02.02	Evaluate value optimization	Continually evaluate the portfolio of I&T-enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value. Identify and evaluate any changes in direction to management that will optimize value creation.	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	
EDM02.03	Direct value optimization	Direct value management principles and practices to enable optimal value realization from I&T-enabled investments throughout their full economic life cycle.	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	
EDM02.03	Direct value optimization	Direct value management principles and practices to enable optimal value realization from I&T-enabled investments throughout their full economic life cycle.	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 (SCRCP) and document all exceptions to this requirement.	8	
EDM02.03	Direct value optimization	Direct value management principles and practices to enable optimal value realization from I&T-enabled investments throughout their full economic life cycle.	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	
EDM02.04	Monitor value optimization	Monitor key goals and metrics to determine whether the enterprise receives expected value and benefit from I&T-enabled investments and services. Identify significant issues and consider corrective actions.	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	
EDM02.04	Monitor value optimization	Monitor key goals and metrics to determine whether the enterprise receives expected value and benefit from I&T-enabled investments and services. Identify significant issues and consider corrective actions.	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 (SCRCP) and document all exceptions to this requirement.	8	
EDM02.04	Monitor value optimization	Monitor key goals and metrics to determine whether the enterprise receives expected value and benefit from I&T-enabled investments and services. Identify significant issues and consider corrective actions.	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	
EDM03.01	Evaluate risk management	Continually examine and evaluate the effect of risk on the current and future use of I&T in the enterprise. Consider whether the enterprise's risk appetite is appropriate and ensure that risk to enterprise value related to the use of I&T is identified and managed.	Functional	Intersects With	Security, Compliance & Resilience 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	
EDM03.01	Evaluate risk management	Continually examine and evaluate the effect of risk on the current and future use of I&T in the enterprise. Consider whether the enterprise's risk appetite is appropriate and ensure that risk to enterprise value related to the use of I&T is identified and managed.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
EDM03.02	Direct risk management	Direct the establishment of risk management practices to provide reasonable assurance that I&T risk management practices are appropriate and that actual I&T risk does not exceed the board's risk appetite.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
EDM03.03	Monitor risk management	Monitor the key goals and metrics of the risk management processes. Determine how deviations or problems will be identified, tracked and reported for remediation.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
EDM04.01	Evaluate resource management	Continually examine and evaluate the current and future need for business and I&T resources (financial and human), options for resourcing (including sourcing strategies), and allocation and management principles to meet the needs of the enterprise in the optimal manner.	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	
EDM04.01	Evaluate resource management	Continually examine and evaluate the current and future need for business and I&T resources (financial and human), options for resourcing (including sourcing strategies), and allocation and management principles to meet the needs of the enterprise in the optimal manner.	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 (SCRCP) and document all exceptions to this requirement.	8	
EDM04.01	Evaluate resource management	Continually examine and evaluate the current and future need for business and I&T resources (financial and human), options for resourcing (including sourcing strategies), and allocation and management principles to meet the needs of the enterprise in the optimal manner.	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	
EDM04.02	Direct resource management	Ensure the adoption of resource management principles to enable optimal use of business and I&T resources throughout their full economic life cycle.	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	
EDM04.02	Direct resource management	Ensure the adoption of resource management principles to enable optimal use of business and I&T resources throughout their full economic life cycle.	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 (SCRCP) and document all exceptions to this requirement.	8	
EDM04.02	Direct resource management	Ensure the adoption of resource management principles to enable optimal use of business and I&T resources throughout their full economic life cycle.	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	
EDM04.03	Monitor resource management	Monitor the key goals and metrics of the resource management processes. Determine how deviations or problems will be identified, tracked and reported for remediation.	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	
EDM04.03	Monitor resource management	Monitor the key goals and metrics of the resource management processes. Determine how deviations or problems will be identified, tracked and reported for remediation.	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 (SCRCP) and document all exceptions to this requirement.	8	
EDM04.03	Monitor resource management	Monitor the key goals and metrics of the resource management processes. Determine how deviations or problems will be identified, tracked and reported for remediation.	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	
EDM05.01	Evaluate stakeholder engagement and reporting requirements	Continually examine and evaluate current and future requirements for stakeholder engagement and reporting (including reporting mandated by regulatory requirements), and communication to other stakeholders. Establish principles for engaging and communicating with stakeholders.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRCP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
EDM05.01	Evaluate stakeholder engagement and reporting requirements	Continually examine and evaluate current and future requirements for stakeholder engagement and reporting (including reporting mandated by regulatory requirements), and communication to other stakeholders. Establish principles for engaging and communicating with stakeholders.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRCP) measures of performance.	8	
EDM05.01	Evaluate stakeholder engagement and reporting requirements	Continually examine and evaluate current and future requirements for stakeholder engagement and reporting (including reporting mandated by regulatory requirements), and communication to other stakeholders. Establish principles for engaging and communicating with stakeholders.	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	
EDM05.01	Evaluate stakeholder engagement and reporting requirements	Continually examine and evaluate current and future requirements for stakeholder engagement and reporting (including reporting mandated by regulatory requirements), and communication to other stakeholders. Establish principles for engaging and communicating with stakeholders.	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	
EDM05.01	Evaluate stakeholder engagement and reporting requirements	Continually examine and evaluate current and future requirements for stakeholder engagement and reporting (including reporting mandated by regulatory requirements), and communication to other stakeholders. Establish principles for engaging and communicating with stakeholders.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	8	
EDM05.01	Evaluate stakeholder engagement and reporting requirements	Continually examine and evaluate current and future requirements for stakeholder engagement and reporting (including reporting mandated by regulatory requirements), and communication to other stakeholders. Establish principles for engaging and communicating with stakeholders.	Functional	Intersects With	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.	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
EDM05.01	Evaluate stakeholder engagement and reporting requirements	Continually examine and evaluate current and future requirements for stakeholder engagement and reporting (including reporting mandated by regulatory requirements), and communication to other stakeholders. Establish principles for engaging and communicating with stakeholders.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	8	
EDM05.02	Direct stakeholder engagement, communication and reporting	Ensure the establishment of effective stakeholder involvement, communication and reporting, including mechanisms for ensuring the quality and completeness of information, overseeing mandatory reporting, and creating a communication strategy for stakeholders.	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	
EDM05.02	Direct stakeholder engagement, communication and reporting	Ensure the establishment of effective stakeholder involvement, communication and reporting, including mechanisms for ensuring the quality and completeness of information, overseeing mandatory reporting, and creating a communication strategy for stakeholders.	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	
EDM05.02	Direct stakeholder engagement, communication and reporting	Ensure the establishment of effective stakeholder involvement, communication and reporting, including mechanisms for ensuring the quality and completeness of information, overseeing mandatory reporting, and creating a communication strategy for stakeholders.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	8	
EDM05.02	Direct stakeholder engagement, communication and reporting	Ensure the establishment of effective stakeholder involvement, communication and reporting, including mechanisms for ensuring the quality and completeness of information, overseeing mandatory reporting, and creating a communication strategy for stakeholders.	Functional	Intersects With	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.	8	
EDM05.02	Direct stakeholder engagement, communication and reporting	Ensure the establishment of effective stakeholder involvement, communication and reporting, including mechanisms for ensuring the quality and completeness of information, overseeing mandatory reporting, and creating a communication strategy for stakeholders.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	8	
EDM05.02	Direct stakeholder engagement, communication and reporting	Ensure the establishment of effective stakeholder involvement, communication and reporting, including mechanisms for ensuring the quality and completeness of information, overseeing mandatory reporting, and creating a communication strategy for stakeholders.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	8	
EDM05.03	Monitor stakeholder engagement	Monitor stakeholder engagement levels and the effectiveness of stakeholder communication. Assess mechanisms for ensuring accuracy, reliability and effectiveness, and ascertain whether the requirements of different stakeholders in terms of reporting and communication are met.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRPP) measures of performance.	8	
EDM05.03	Monitor stakeholder engagement	Monitor stakeholder engagement levels and the effectiveness of stakeholder communication. Assess mechanisms for ensuring accuracy, reliability and effectiveness, and ascertain whether the requirements of different stakeholders in terms of reporting and communication are met.	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	
EDM05.03	Monitor stakeholder engagement	Monitor stakeholder engagement levels and the effectiveness of stakeholder communication. Assess mechanisms for ensuring accuracy, reliability and effectiveness, and ascertain whether the requirements of different stakeholders in terms of reporting and communication are met.	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	
EDM05.03	Monitor stakeholder engagement	Monitor stakeholder engagement levels and the effectiveness of stakeholder communication. Assess mechanisms for ensuring accuracy, reliability and effectiveness, and ascertain whether the requirements of different stakeholders in terms of reporting and communication are met.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	8	
EDM05.03	Monitor stakeholder engagement	Monitor stakeholder engagement levels and the effectiveness of stakeholder communication. Assess mechanisms for ensuring accuracy, reliability and effectiveness, and ascertain whether the requirements of different stakeholders in terms of reporting and communication are met.	Functional	Intersects With	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.	8	
EDM05.03	Monitor stakeholder engagement	Monitor stakeholder engagement levels and the effectiveness of stakeholder communication. Assess mechanisms for ensuring accuracy, reliability and effectiveness, and ascertain whether the requirements of different stakeholders in terms of reporting and communication are met.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	8	
AP001.01	Design the management system for enterprise I&T	Design a management system tailored to the needs of the enterprise. Management needs of the enterprise are defined through the use of the goals cascade and by application of design factors. Ensure the governance components are integrated and aligned with the enterprise's governance and management philosophy and operating style.	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	
AP001.01	Design the management system for enterprise I&T	Design a management system tailored to the needs of the enterprise. Management needs of the enterprise are defined through the use of the goals cascade and by application of design factors. Ensure the governance components are integrated and aligned with the enterprise's governance and management philosophy and operating style.	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	
AP001.02	Communicate management objectives, direction and decisions made	Communicate awareness and promote understanding of alignment and I&T objectives to stakeholders throughout the enterprise. Communicate at regular intervals on important I&T-related decisions and their impact for the organization.	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	
AP001.02	Communicate management objectives, direction and decisions made	Communicate awareness and promote understanding of alignment and I&T objectives to stakeholders throughout the enterprise. Communicate at regular intervals on important I&T-related decisions and their impact for the organization.	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	
AP001.03	Implement management processes to support the achievement of governance and management objectives	Define target process capability levels and implementation priority based on the management system design.	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	
AP001.03	Implement management processes to support the achievement of governance and management objectives	Define target process capability levels and implementation priority based on the management system design.	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	
AP001.04	Define and implement the organizational structures	Put in place the required internal and extended organizational structures (e.g., committees) per the management system design, enabling effective and efficient decision making. Ensure that required technology and information knowledge is included in the composition of management structures.	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	
AP001.04	Define and implement the organizational structures	Put in place the required internal and extended organizational structures (e.g., committees) per the management system design, enabling effective and efficient decision making. Ensure that required technology and information knowledge is included in the composition of management structures.	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.	8	
AP001.05	Establish roles and responsibilities	Define and communicate roles and responsibilities for enterprise I&T, including authority levels, responsibilities and accountability.	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 (SCRPP).	8	
AP001.06	Optimize the placement of the IT function	Position the IT capabilities in the overall organizational structure to reflect the strategic importance and operational dependency of IT within the enterprise. The reporting line of the CIO and representation of IT within senior management should be commensurate with the importance of I&T within the enterprise.	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	
AP001.06	Optimize the placement of the IT function	Position the IT capabilities in the overall organizational structure to reflect the strategic importance and operational dependency of IT within the enterprise. The reporting line of the CIO and representation of IT within senior management should be commensurate with the importance of I&T within the enterprise.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	8	
AP001.06	Optimize the placement of the IT function	Position the IT capabilities in the overall organizational structure to reflect the strategic importance and operational dependency of IT within the enterprise. The reporting line of the CIO and representation of IT within senior management should be commensurate with the importance of I&T within the enterprise.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	8	
AP001.06	Optimize the placement of the IT function	Position the IT capabilities in the overall organizational structure to reflect the strategic importance and operational dependency of IT within the enterprise. The reporting line of the CIO and representation of IT within senior management should be commensurate with the importance of I&T within the enterprise.	Functional	Intersects With	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.	8	
AP001.07	Define information (data) and system ownership	Define and maintain responsibilities for ownership of information (data) and information systems. Ensure that owners classify information and systems and protect them in line with their classification.	Functional	Subset Of	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	10	
AP001.08	Define target skills and competencies	Define the required skills and competencies to achieve relevant management objectives.	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	
AP001.08	Define target skills and competencies	Define the required skills and competencies to achieve relevant management objectives.	Functional	Intersects With	Identify Critical Skills & Gaps	HRS-13	Mechanisms exist to evaluate the critical security, compliance and resilience skills needed to support the organization's mission and identify gaps that exist.	8	
AP001.08	Define target skills and competencies	Define the required skills and competencies to achieve relevant management objectives.	Functional	Intersects With	Remediate Identified Skills Deficiencies	HRS-13.1	Mechanisms exist to remediate critical skills deficiencies necessary to support the organization's mission and business functions.	8	
AP001.08	Define target skills and competencies	Define the required skills and competencies to achieve relevant management objectives.	Functional	Intersects With	Manage Organizational Knowledge	PRM-08	Mechanisms exist to manage the organizational knowledge of the security, compliance and resilience staff.	8	
AP001.09	Define and communicate policies and procedures	Put in place procedures to maintain compliance with and performance measurement of policies and other components of the control framework. Enforce the consequences of noncompliance or inadequate performance. Track trends and performance and consider these in the future design and improvement of the control framework.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRPP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
AP001.09	Define and communicate policies and procedures	Put in place procedures to maintain compliance with and performance measurement of policies and other components of the control framework. Enforce the consequences of noncompliance or inadequate performance. Track trends and performance and consider these in the future design and improvement of the control framework.	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	
AP001.09	Define and communicate policies and procedures	Put in place procedures to maintain compliance with and performance measurement of policies and other components of the control framework. Enforce the consequences of noncompliance or inadequate performance. Track trends and performance and consider these in the future design and improvement of the control framework.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	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
AP001.10	Define and implement infrastructure, services and applications to support the governance and management system	Define and implement infrastructure, services and applications to support the governance and management system (e. architecture repositories, risk management system, project management tools, costtracking tools and incident monitoring tools).	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a critically analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	8	
AP001.10	Define and implement infrastructure, services and applications to support the governance and management system	Define and implement infrastructure, services and applications to support the governance and management system (e. architecture repositories, risk management system, project management tools, costtracking tools and incident monitoring tools).	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	
AP001.11	Manage continual improvement of the IS&T management system	Continually improve processes and other management system components to ensure that they can deliver against governance and management objectives. Consider COBIT implementation guidance, emerging standards, compliance requirements, automation opportunities and the feedback of stakeholders.	Functional	Intersects With	Service Delivery (Business Process Support)	OP5-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	8	
AP002.01	Understand enterprise context and direction	Understand the enterprise context (industry drivers, relevant regulations, basis for competition), its current way of working and its ambition level in terms of digitization.	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	
AP002.01	Understand enterprise context and direction	Understand the enterprise context (industry drivers, relevant regulations, basis for competition), its current way of working and its ambition level in terms of digitization.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
AP002.02	Assess current capabilities, performance and digital maturity of the enterprise	Assess the performance of current IS&T services and develop an understanding of current business and IS&T capabilities (both internal and external). Assess current digital maturity of the enterprise and its appetite for change.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRCP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
AP002.02	Assess current capabilities, performance and digital maturity of the enterprise	Assess the performance of current IS&T services and develop an understanding of current business and IS&T capabilities (both internal and external). Assess current digital maturity of the enterprise and its appetite for change.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRCP) measures of performance.	8	
AP002.02	Assess current capabilities, performance and digital maturity of the enterprise	Assess the performance of current IS&T services and develop an understanding of current business and IS&T capabilities (both internal and external). Assess current digital maturity of the enterprise and its appetite for change.	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 (SCRCP).	8	
AP002.02	Assess current capabilities, performance and digital maturity of the enterprise	Assess the performance of current IS&T services and develop an understanding of current business and IS&T capabilities (both internal and external). Assess current digital maturity of the enterprise and its appetite for change.	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 (SCRCP).	8	
AP002.02	Assess current capabilities, performance and digital maturity of the enterprise	Assess the performance of current IS&T services and develop an understanding of current business and IS&T capabilities (both internal and external). Assess current digital maturity of the enterprise and its appetite for change.	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	
AP002.03	Define target digital capabilities	Based on the understanding of enterprise context and direction, define the target IS&T products and services and required capabilities. Consider reference standards, best practices and validated emerging technologies.	Functional	Intersects With	Targeted Capability Maturity Levels	PRM-01.2	Mechanisms exist to define and identify targeted capability maturity levels.	8	
AP002.04	Conduct a gap analysis	Identify gaps between current and target environments and describe the high-level changes in the enterprise architecture.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	8	
AP002.05	Define the strategic plan and road map	Develop a holistic digital strategy, in cooperation with relevant stakeholders, and detail a road map that defines the incremental steps required to achieve the goals and objectives. Ensure focus on the transformation journey through the appointment of a person who helps spearhead the digital transformation and drives alignment between business and IS&T.	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	
AP002.05	Define the strategic plan and road map	Develop a holistic digital strategy, in cooperation with relevant stakeholders, and detail a road map that defines the incremental steps required to achieve the goals and objectives. Ensure focus on the transformation journey through the appointment of a person who helps spearhead the digital transformation and drives alignment between business and IS&T.	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	
AP002.05	Define the strategic plan and road map	Develop a holistic digital strategy, in cooperation with relevant stakeholders, and detail a road map that defines the incremental steps required to achieve the goals and objectives. Ensure focus on the transformation journey through the appointment of a person who helps spearhead the digital transformation and drives alignment between business and IS&T.	Functional	Intersects With	Targeted Capability Maturity Levels	PRM-01.2	Mechanisms exist to define and identify targeted capability maturity levels.	8	
AP002.06	Communicate the IS&T strategy and direction	Create awareness and understanding of the business and IS&T objectives and direction, as captured in the IS&T strategy, through communication to appropriate stakeholders and users throughout the enterprise.	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	
AP003.01	Develop the enterprise architecture vision	The architecture vision provides a first-cut, high-level description of the baseline and target architectures, covering the business, information, data, application and technology domains. The architecture vision provides the sponsor with a key tool to sell the benefits of the proposed capabilities to stakeholders within the enterprise. The architecture vision describes how the new capabilities (in line with IS&T strategy and objectives) will meet enterprise goals and strategic objectives and address stakeholder concerns when implemented.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
AP003.01	Develop the enterprise architecture vision	The architecture vision provides a first-cut, high-level description of the baseline and target architectures, covering the business, information, data, application and technology domains. The architecture vision provides the sponsor with a key tool to sell the benefits of the proposed capabilities to stakeholders within the enterprise. The architecture vision describes how the new capabilities (in line with IS&T strategy and objectives) will meet enterprise goals and strategic objectives and address stakeholder concerns when implemented.	Functional	Intersects With	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of security, compliance and resilience controls and related processes.	8	
AP003.01	Develop the enterprise architecture vision	The architecture vision provides a first-cut, high-level description of the baseline and target architectures, covering the business, information, data, application and technology domains. The architecture vision provides the sponsor with a key tool to sell the benefits of the proposed capabilities to stakeholders within the enterprise. The architecture vision describes how the new capabilities (in line with IS&T strategy and objectives) will meet enterprise goals and strategic objectives and address stakeholder concerns when implemented.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
AP003.01	Develop the enterprise architecture vision	The architecture vision provides a first-cut, high-level description of the baseline and target architectures, covering the business, information, data, application and technology domains. The architecture vision provides the sponsor with a key tool to sell the benefits of the proposed capabilities to stakeholders within the enterprise. The architecture vision describes how the new capabilities (in line with IS&T strategy and objectives) will meet enterprise goals and strategic objectives and address stakeholder concerns when implemented.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	8	
AP003.02	Define reference architecture	The reference architecture describes the current and target architectures for the business, information, data, application and technology domains.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
AP003.02	Define reference architecture	The reference architecture describes the current and target architectures for the business, information, data, application and technology domains.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
AP003.02	Define reference architecture	The reference architecture describes the current and target architectures for the business, information, data, application and technology domains.	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	
AP003.02	Define reference architecture	The reference architecture describes the current and target architectures for the business, information, data, application and technology domains.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	8	
AP003.02	Define reference architecture	The reference architecture describes the current and target architectures for the business, information, data, application and technology domains.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	8	
AP003.03	Select opportunities and solutions	Rationalize the gaps between baseline and target architectures, accounting for both business and technical perspectives, and logically group them into project work packages. Integrate the project with any related IS&T-enabled investment programs to ensure that the architectural initiatives are aligned with and enable these initiatives as part of overall enterprise change. Make this a collaborative effort with key enterprise stakeholders from business and IT to assess the enterprise's transformation readiness, and identify opportunities, solutions and all implementation constraints.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
AP003.03	Select opportunities and solutions	Rationalize the gaps between baseline and target architectures, accounting for both business and technical perspectives, and logically group them into project work packages. Integrate the project with any related IS&T-enabled investment programs to ensure that the architectural initiatives are aligned with and enable these initiatives as part of overall enterprise change. Make this a collaborative effort with key enterprise stakeholders from business and IT to assess the enterprise's transformation readiness, and identify opportunities, solutions and all implementation constraints.	Functional	Intersects With	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of security, compliance and resilience controls and related processes.	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
AP003.03	Select opportunities and solutions	Rationalize the gaps between baseline and target architectures, accounting for both business and technical perspectives, and logically group them into project work packages. Integrate the project with any related I&T-enabled investment programs to ensure that the architectural initiatives are aligned with and enable these initiatives as part of overall enterprise change. Make this a collaborative effort with key enterprise stakeholders from business and IT to assess the enterprise's transformation readiness, and identify opportunities, solutions and all implementation constraints.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
AP003.03	Select opportunities and solutions	Rationalize the gaps between baseline and target architectures, accounting for both business and technical perspectives, and logically group them into project work packages. Integrate the project with any related I&T-enabled investment programs to ensure that the architectural initiatives are aligned with and enable these initiatives as part of overall enterprise change. Make this a collaborative effort with key enterprise stakeholders from business and IT to assess the enterprise's transformation readiness, and identify opportunities, solutions and all implementation constraints.	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	
AP003.03	Select opportunities and solutions	Rationalize the gaps between baseline and target architectures, accounting for both business and technical perspectives, and logically group them into project work packages. Integrate the project with any related I&T-enabled investment programs to ensure that the architectural initiatives are aligned with and enable these initiatives as part of overall enterprise change. Make this a collaborative effort with key enterprise stakeholders from business and IT to assess the enterprise's transformation readiness, and identify opportunities, solutions and all implementation constraints.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	8	
AP003.04	Define architecture implementation	Create a viable implementation and migration plan in alignment with the program and project portfolios. Ensure the plan is closely coordinated to deliver value and that the required resources are available to complete the necessary work.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
AP003.04	Define architecture implementation	Create a viable implementation and migration plan in alignment with the program and project portfolios. Ensure the plan is closely coordinated to deliver value and that the required resources are available to complete the necessary work.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
AP003.05	Provide enterprise architecture services	Provide enterprise architecture services within the enterprise that include guidance to and monitoring of implementation projects, formalizing ways of working through architecture contracts, and measuring and communicating architecture's value and compliance monitoring.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
AP003.05	Provide enterprise architecture services	Provide enterprise architecture services within the enterprise that include guidance to and monitoring of implementation projects, formalizing ways of working through architecture contracts, and measuring and communicating architecture's value and compliance monitoring.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
AP004.01	Create an environment conducive to innovation	Create an environment that is conducive to innovation, considering methods such as culture, reward, collaboration, technology forums, and mechanisms to promote and capture employee ideas.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRPP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	8	
AP004.01	Create an environment conducive to innovation	Create an environment that is conducive to innovation, considering methods such as culture, reward, collaboration, technology forums, and mechanisms to promote and capture employee ideas.	Functional	Intersects With	Data Privacy Program	PRV-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	
AP004.01	Create an environment conducive to innovation	Create an environment that is conducive to innovation, considering methods such as culture, reward, collaboration, technology forums, and mechanisms to promote and capture employee ideas.	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	
AP004.02	Maintain an understanding of the enterprise environment	Work with relevant stakeholders to understand their challenges. Maintain an adequate understanding of enterprise strategy, competitive environment and other constraints, so that opportunities enabled by new technologies can be identified.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
AP004.03	Monitor and scan the technology environment	Set up a technology watch process to perform systematic monitoring and scanning of the enterprise's external environment to identify emerging technologies that have the potential to create value (e.g. by realizing the enterprise strategy, optimizing costs, avoiding obsolescence, and better enabling enterprise and I&T processes). Monitor the marketplace, competitive landscape, industry sectors, and legal and regulatory trends to be able to analyze emerging technologies or innovation ideas in the enterprise context.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
AP004.04	Assess the potential of emerging technologies and innovative ideas	Analyze identified emerging technologies and/or other I&T innovative suggestions to understand their business potential. Work with stakeholders to validate assumptions on the potential of new technologies and innovation.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
AP004.05	Recommend appropriate further initiatives	Evaluate and monitor the results of proof-of-concept initiatives and, if favorable, generate recommendations for further initiatives. Gain stakeholder support.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
AP004.05	Recommend appropriate further initiatives	Evaluate and monitor the results of proof-of-concept initiatives and, if favorable, generate recommendations for further initiatives. Gain stakeholder support.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
AP004.05	Recommend appropriate further initiatives	Evaluate and monitor the results of proof-of-concept initiatives and, if favorable, generate recommendations for further initiatives. Gain stakeholder support.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	8	
AP004.06	Monitor the implementation and use of innovation	Monitor the implementation and use of emerging technologies and innovations during adoption, integration and for the full economic life cycle to ensure that the promised benefits are realized and to identify lessons learned.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
AP005.01	Determine the availability and sources of funds	Determine potential sources of funds, different funding options and the implications of the funding source on the investment return expectations.	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	
AP005.02	Evaluate and select programs to fund	Based on requirements for the overall investment portfolio mix and the I&T strategic plan and road map, evaluate and prioritize program business cases and decide on investment proposals. Allocate funds and initiate programs.	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	
AP005.03	Monitor, optimize and report on investment portfolio performance	On a regular basis, monitor and optimize the performance of the investment portfolio and individual programs throughout the entire investment life cycle. Ensure continuous follow-up on the alignment of the portfolio with I&T strategy.	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	
AP005.04	Maintain portfolios	Maintain portfolios of investment programs and projects, I&T products and services, and I&T assets.	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	
AP005.05	Manage benefits achievement	Monitor the benefits of providing and maintaining appropriate I&T products, services and capabilities, based on the agreed and current business case.	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	
AP006.01	Manage finance and accounting	Establish and maintain a method to manage and account for all I&T-related costs, investments and depreciation as an integral part of enterprise financial systems and accounts. Report using the enterprise's financial measurement systems.	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	
AP006.02	Prioritize resource allocation	Implement a decision-making process to prioritize the allocation of resources and establish rules for discretionary investments by individual business units. Include the potential use of external service providers and consider the buy, develop and rent options.	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	
AP006.03	Create and maintain budgets	Prepare a budget reflecting investment priorities based on the portfolio of I&T-enabled programs and I&T services.	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	
AP006.04	Model and allocate costs	Establish and use an I&T costing model based, for example, on the service definition. This approach ensures that allocation of costs for services is identifiable, measurable and predictable, and encourages the responsible use of resources, including those provided by service providers. Regularly review and benchmark the cost/chargeback model to maintain its relevance and appropriateness for evolving business and IT activities.	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	
AP006.05	Manage costs	Implement a cost management process that compares actual costs against budget. Costs should be monitored and reported. Deviations from budget should be identified in a timely manner and their impact on enterprise processes and services assessed.	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	
AP007.01	Acquire and maintain adequate and appropriate staffing	Establish and maintain a method to manage and account for all I&T-related costs, investments and depreciation as an integral part of the enterprise financial systems and accounts. Report using the enterprise's financial measurement systems.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
AP007.02	Identify key IT personnel	Identify key IT personnel. Use knowledge capture (documentation), knowledge sharing, succession planning and staff backup to minimize reliance on a single individual performing critical job functions.	Functional	Intersects With	Identify Vital Security, Compliance & Resilience Staff	HRS-13.2	Mechanisms exist to identify vital security, compliance and resilience staff.	8	
AP007.03	Maintain the skills and competencies of personnel	Define and manage the skills and competencies required of personnel. Regularly verify that personnel have the competencies to fulfill their roles on the basis of their education, training and/or experience. Verify that these competencies are being maintained, using qualification and certification programs where appropriate. Provide employees with ongoing learning and opportunities to maintain their knowledge, skills and competencies at a level required to achieve enterprise goals.	Functional	Intersects With	Identify Critical Skills & Gaps	HRS-13	Mechanisms exist to evaluate the critical security, compliance and resilience skills needed to support the organization's mission and identify gaps that exist.	8	
AP007.03	Maintain the skills and competencies of personnel	Define and manage the skills and competencies required of personnel. Regularly verify that personnel have the competencies to fulfill their roles on the basis of their education, training and/or experience. Verify that these competencies are being maintained, using qualification and certification programs where appropriate. Provide employees with ongoing learning and opportunities to maintain their knowledge, skills and competencies at a level required to achieve enterprise goals.	Functional	Intersects With	Remediate Identified Skills Deficiencies	HRS-13.1	Mechanisms exist to remediate critical skills deficiencies necessary to support the organization's mission and business functions.	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
AP007.03	Maintain the skills and competencies of personnel	Define and manage the skills and competencies required of personnel. Regularly verify that personnel have the competencies to fulfill their roles on the basis of their education, training and/or experience. Verify that these competencies are being maintained, using qualification and certification programs where appropriate. Provide employees with ongoing learning and opportunities to maintain their knowledge, skills and competencies at a level required to achieve enterprise goals.	Functional	Intersects With	Establish Redundancy for Vital Security, Compliance & Resilience Staff	HRS-13.3	Mechanisms exist to establish redundancy for vital security, compliance and resilience staff.	8	
AP007.03	Maintain the skills and competencies of personnel	Define and manage the skills and competencies required of personnel. Regularly verify that personnel have the competencies to fulfill their roles on the basis of their education, training and/or experience. Verify that these competencies are being maintained, using qualification and certification programs where appropriate. Provide employees with ongoing learning and opportunities to maintain their knowledge, skills and competencies at a level required to achieve enterprise goals.	Functional	Intersects With	Perform Succession Planning	HRS-13.4	Mechanisms exist to perform succession planning for vital security, compliance and resilience roles.	8	
AP007.04	Assess and recognize/reward employee job performance	Conduct timely, regular performance evaluations against individual objectives derived from enterprise goals, established standards, specific job responsibilities, and the skills and competency framework. Implement a remuneration/recognition process that rewards successful attainment of performance goals.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
AP007.05	Plan and track the usage of IT and business human resources	Understand and track the current and future demand for business and IT human resources with responsibilities for enterprise I&T. Identify shortfalls and provide input into sourcing plans, enterprise and IT recruitment processes, and business and IT recruitment processes.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
AP007.06	Manage contract staff	Ensure that consultants and contract personnel who support the enterprise with I&T skills know and comply with the organization's policies and meet agreed contractual requirements.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
AP007.06	Manage contract staff	Ensure that consultants and contract personnel who support the enterprise with I&T skills know and comply with the organization's policies and meet agreed contractual requirements.	Functional	Intersects With	Third-Party Personnel	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.	8	
AP008.01	Understand business expectations	Understand current business issues, objectives and expectations for I&T. Ensure that requirements are understood, managed and communicated, and their status agreed and approved.	Functional	Subset Of	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	10	
AP008.01	Understand business expectations	Understand current business issues, objectives and expectations for I&T. Ensure that requirements are understood, managed and communicated, and their status agreed and approved.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a critically analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	8	
AP008.01	Understand business expectations	Understand current business issues, objectives and expectations for I&T. Ensure that requirements are understood, managed and communicated, and their status agreed and approved.	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	
AP008.02	Align I&T strategy with business expectations and identify opportunities for IT to enhance the business	Align I&T strategies with current business objectives and expectations to enable IT to be a value-add partner for the business and a governance component for enhanced enterprise performance.	Functional	Subset Of	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	10	
AP008.03	Manage the business relationship	Manage the relationship between the IT service organization and its business partners. Ensure that relationship roles and responsibilities are defined and assigned, and communication is facilitated.	Functional	Subset Of	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	10	
AP008.04	Coordinate and communicate	Work with all relevant stakeholders and coordinate the end-to-end delivery of I&T services and solutions provided to the business.	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	
AP008.04	Coordinate and communicate	Work with all relevant stakeholders and coordinate the end-to-end delivery of I&T services and solutions provided to the business.	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	
AP008.05	Provide input to the continual improvement of services	Continually improve and evolve I&T-enabled services and service delivery to the enterprise to align with changing enterprise objectives and technology.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	8	
AP009.01	Identify I&T services	Analyze business requirements and the degree to which I&T-enabled services and service levels support business processes. Discuss and agree with the business on potential services and service levels. Compare potential service levels against the current service portfolio; identify new or changed services or service level options.	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	8	
AP009.01	Identify I&T services	Analyze business requirements and the degree to which I&T-enabled services and service levels support business processes. Discuss and agree with the business on potential services and service levels. Compare potential service levels against the current service portfolio; identify new or changed services or service level options.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8	
AP009.02	Catalog I&T-enabled services	Define and maintain one or more service catalogues for relevant target groups. Publish and maintain live I&T-enabled services in the service catalogues.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	3	
AP009.03	Define and prepare service agreements	Define and prepare service agreements based on options in the service catalogues. Include internal operational agreements.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
AP009.03	Define and prepare service agreements	Define and prepare service agreements based on options in the service catalogues. Include internal operational agreements.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	
AP009.04	Monitor and report service levels	Monitor service levels, report on achievements and identify trends. Provide the appropriate management information to aid performance management.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	8	
AP009.04	Monitor and report service levels	Monitor service levels, report on achievements and identify trends. Provide the appropriate management information to aid performance management.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	8	
AP009.05	Review service agreements and contracts	Conduct periodic reviews of the service agreements and revise when needed.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	8	
AP009.05	Review service agreements and contracts	Conduct periodic reviews of the service agreements and revise when needed.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	8	
AP010.01	Identify and evaluate vendor relationships and contracts	Continuously search for and identify vendors and categorize them into type, maintain periodically. Establish criteria to evaluate vendors and contracts. Review the overall portfolio of existing and alternative vendors and contracts.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
AP010.02	Select vendors	Select suppliers according to a fair and formal practice to ensure a viable best-fit based on specified requirements. Requirements should be optimized with input from potential suppliers.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
AP010.03	Manage vendor relationships and contracts	Formalize and manage the supplier relationship for each supplier. Manage, maintain and monitor contracts and service delivery. Ensure that new or changed contracts conform to enterprise standards and legal and regulatory requirements. Deal with contractual disputes.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
AP010.03	Manage vendor relationships and contracts	Formalize and manage the supplier relationship for each supplier. Manage, maintain and monitor contracts and service delivery. Ensure that new or changed contracts conform to enterprise standards and legal and regulatory requirements. Deal with contractual disputes.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	8	
AP010.03	Manage vendor relationships and contracts	Formalize and manage the supplier relationship for each supplier. Manage, maintain and monitor contracts and service delivery. Ensure that new or changed contracts conform to enterprise standards and legal and regulatory requirements. Deal with contractual disputes.	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	
AP010.03	Manage vendor relationships and contracts	Formalize and manage the supplier relationship for each supplier. Manage, maintain and monitor contracts and service delivery. Ensure that new or changed contracts conform to enterprise standards and legal and regulatory requirements. Deal with contractual disputes.	Functional	Intersects With	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	8	
AP010.04	Manage vendor risk	Identify and manage risk relating to vendors' ability to continually provide secure, efficient and effective service delivery. This also includes the subcontractors or upstream vendors that are relevant in the service delivery of the direct vendor.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
AP010.04	Manage vendor risk	Identify and manage risk relating to vendors' ability to continually provide secure, efficient and effective service delivery. This also includes the subcontractors or upstream vendors that are relevant in the service delivery of the direct vendor.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	8	
AP010.04	Manage vendor risk	Identify and manage risk relating to vendors' ability to continually provide secure, efficient and effective service delivery. This also includes the subcontractors or upstream vendors that are relevant in the service delivery of the direct vendor.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	8	
AP010.04	Manage vendor risk	Identify and manage risk relating to vendors' ability to continually provide secure, efficient and effective service delivery. This also includes the subcontractors or upstream vendors that are relevant in the service delivery of the direct vendor.	Functional	Intersects With	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	8	
AP010.04	Manage vendor risk	Identify and manage risk relating to vendors' ability to continually provide secure, efficient and effective service delivery. This also includes the subcontractors or upstream vendors that are relevant in the service delivery of the direct vendor.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	8	
AP010.04	Manage vendor risk	Identify and manage risk relating to vendors' ability to continually provide secure, efficient and effective service delivery. This also includes the subcontractors or upstream vendors that are relevant in the service delivery of the direct vendor.	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	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
AP010.04	Manage vendor risk	Identify and manage risk relating to vendors' ability to continually provide secure, efficient and effective service delivery. This also includes the subcontractors or upstream vendors that are relevant in the service delivery of the direct vendor.	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	8	
AP010.05	Monitor vendor performance and compliance	Periodically review overall vendor performance, compliance to contract requirements and value for money. Address identified issues.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
AP010.05	Monitor vendor performance and compliance	Periodically review overall vendor performance, compliance to contract requirements and value for money. Address identified issues.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	8	
AP011.01	Establish a quality management system (QMS)	Establish and maintain a quality management system (QMS) that provides a standard, formal and continuous approach to quality management of information. The QMS should enable technology and business processes to align with business requirements and enterprise quality management.	Functional	Subset Of	Quality Management System (QMS)	GOV-18	Mechanisms exist to govern a Quality Management System (QMS) to ensure security, compliance and resilience processes conform with applicable statutory, regulatory and/or contractual obligations.	10	
AP011.01	Establish a quality management system (QMS)	Establish and maintain a quality management system (QMS) that provides a standard, formal and continuous approach to quality management of information. The QMS should enable technology and business processes to align with business requirements and enterprise quality management.	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	8	
AP011.01	Establish a quality management system (QMS)	Establish and maintain a quality management system (QMS) that provides a standard, formal and continuous approach to quality management of information. The QMS should enable technology and business processes to align with business requirements and enterprise quality management.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	8	
AP011.02	Focus quality management on customers	Focus quality management on customers by determining their requirements and ensuring integration in quality management practices.	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	8	
AP011.02	Focus quality management on customers	Focus quality management on customers by determining their requirements and ensuring integration in quality management practices.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	8	
AP011.03	Manage quality standards, practices and procedures and integrate quality management into key processes and solutions	Identify and maintain standards, procedures and practices for key processes to guide the enterprise in meeting the intent of the agreed quality management standards (QMS). This activity should align with IS&T control framework requirements. Consider certification for key processes, organizational units, products or services.	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	8	
AP011.03	Manage quality standards, practices and procedures and integrate quality management into key processes and solutions	Identify and maintain standards, procedures and practices for key processes to guide the enterprise in meeting the intent of the agreed quality management standards (QMS). This activity should align with IS&T control framework requirements. Consider certification for key processes, organizational units, products or services.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	8	
AP011.04	Perform quality monitoring control and reviews	Monitor the quality of processes and services on an ongoing basis, in line with quality management standards. Define, plan and implement measurements to monitor customer satisfaction with quality as well as the value provided by the quality management system (QMS). The information gathered should be used by the process owner to improve quality.	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	8	
AP011.04	Perform quality monitoring control and reviews	Monitor the quality of processes and services on an ongoing basis, in line with quality management standards. Define, plan and implement measurements to monitor customer satisfaction with quality as well as the value provided by the quality management system (QMS). The information gathered should be used by the process owner to improve quality.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	8	
AP011.05	Maintain continuous improvement	Maintain and regularly communicate an overall quality plan that promotes continuous improvement. The plan should define the need for, and benefits of, continuous improvement. Collect and analyze data about the quality management system (QMS) and improve its effectiveness. Correct nonconformities to prevent recurrence.	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	8	
AP011.05	Maintain continuous improvement	Maintain and regularly communicate an overall quality plan that promotes continuous improvement. The plan should define the need for, and benefits of, continuous improvement. Collect and analyze data about the quality management system (QMS) and improve its effectiveness. Correct nonconformities to prevent recurrence.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	8	
AP012.01	Collect data	Identify and collect relevant data to enable effective IS&T-related risk identification, analysis and reporting.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
AP012.01	Collect data	Identify and collect relevant data to enable effective IS&T-related risk identification, analysis and reporting.	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	
AP012.01	Collect data	Identify and collect relevant data to enable effective IS&T-related risk identification, analysis and reporting.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	8	
AP012.01	Collect data	Identify and collect relevant data to enable effective IS&T-related risk identification, analysis and reporting.	Functional	Intersects With	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	8	
AP012.01	Collect data	Identify and collect relevant data to enable effective IS&T-related risk identification, analysis and reporting.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	8	
AP012.01	Collect data	Identify and collect relevant data to enable effective IS&T-related risk identification, analysis and reporting.	Functional	Intersects With	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	8	
AP012.01	Collect data	Identify and collect relevant data to enable effective IS&T-related risk identification, analysis and reporting.	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	
AP012.02	Analyze risk	Develop a substantiated view on actual IS&T risk, in support of risk decisions.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
AP012.02	Analyze risk	Develop a substantiated view on actual IS&T risk, in support of risk decisions.	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	
AP012.02	Analyze risk	Develop a substantiated view on actual IS&T risk, in support of risk decisions.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	8	
AP012.02	Analyze risk	Develop a substantiated view on actual IS&T risk, in support of risk decisions.	Functional	Intersects With	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	8	
AP012.02	Analyze risk	Develop a substantiated view on actual IS&T risk, in support of risk decisions.	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	
AP012.03	Maintain a risk profile	Maintain an inventory of known risk and risk attributes, including expected frequency, potential impact and responses. Document related resources, capabilities and current control activities related to risk items.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
AP012.03	Maintain a risk profile	Maintain an inventory of known risk and risk attributes, including expected frequency, potential impact and responses. Document related resources, capabilities and current control activities related to risk items.	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	8	
AP012.03	Maintain a risk profile	Maintain an inventory of known risk and risk attributes, including expected frequency, potential impact and responses. Document related resources, capabilities and current control activities related to risk items.	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	
AP012.03	Maintain a risk profile	Maintain an inventory of known risk and risk attributes, including expected frequency, potential impact and responses. Document related resources, capabilities and current control activities related to risk items.	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	8	
AP012.03	Maintain a risk profile	Maintain an inventory of known risk and risk attributes, including expected frequency, potential impact and responses. Document related resources, capabilities and current control activities related to risk items.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	8	
AP012.03	Maintain a risk profile	Maintain an inventory of known risk and risk attributes, including expected frequency, potential impact and responses. Document related resources, capabilities and current control activities related to risk items.	Functional	Intersects With	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	8	
AP012.03	Maintain a risk profile	Maintain an inventory of known risk and risk attributes, including expected frequency, potential impact and responses. Document related resources, capabilities and current control activities related to risk items.	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	
AP012.04	Articulate risk	Communicate information on the current state of IS&T-related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.	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
AP012.04	Articulate risk	Communicate information on the current state of I&T-related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.	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	
AP012.04	Articulate risk	Communicate information on the current state of I&T-related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.	Functional	Intersects With	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	8	
AP012.04	Articulate risk	Communicate information on the current state of I&T-related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	8	
AP012.04	Articulate risk	Communicate information on the current state of I&T-related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.	Functional	Intersects With	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	8	
AP012.04	Articulate risk	Communicate information on the current state of I&T-related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.	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	
AP012.05	Define a risk management action portfolio	Manage opportunities to reduce risk to an acceptable level as a portfolio.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	(2) Applicable security, compliance and/or resilience control: (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner).	8	
AP012.05	Define a risk management action portfolio	Manage opportunities to reduce risk to an acceptable level as a portfolio.	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	
AP012.05	Define a risk management action portfolio	Manage opportunities to reduce risk to an acceptable level as a portfolio.	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.	8	
AP012.05	Define a risk management action portfolio	Manage opportunities to reduce risk to an acceptable level as a portfolio.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
AP012.05	Define a risk management action portfolio	Manage opportunities to reduce risk to an acceptable level as a portfolio.	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
AP012.06	Respond to risk	Respond in a timely manner to materialized risk events with effective measures to limit the magnitude of loss.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
AP012.06	Respond to risk	Respond in a timely manner to materialized risk events with effective measures to limit the magnitude of loss.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	8	
AP012.06	Respond to risk	Respond in a timely manner to materialized risk events with effective measures to limit the magnitude of loss.	Functional	Intersects With	Risk Response	RSK-06.1	Remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or	8	
AP012.06	Respond to risk	Respond in a timely manner to materialized risk events with effective measures to limit the magnitude of loss.	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.	8	
AP013.01	Establish and maintain an information security management system (ISMS)	Establish and maintain an information security management system (ISMS) that provides a standard, formal and continuous approach to information security management, enabling secure technology and business processes that are aligned with business requirements.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRIP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
AP013.02	Define and manage an information security and privacy risk treatment plan	Maintain an information security plan that describes how information security risk is to be managed and aligned with enterprise strategy and enterprise architecture. Ensure that recommendations for implementing security improvements are based on approved business cases, implemented as an integral part of services and solutions development, and operated as an integral part of business operation.	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	
AP013.03	Monitor and review the information security management system (ISMS)	Maintain and regularly communicate the need for, and benefits of, continuous improvement in information security. Collect and analyze data about the information security management system (ISMS), and improve its effectiveness. Correct nonconformities to prevent recurrence.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRIP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
AP014.01	Define and communicate the organization's data management strategy and roles and responsibilities	Define how to manage and improve the organization's data assets, in line with enterprise strategy and objectives. Communicate the data management strategy to all stakeholders. Assign roles and responsibilities to ensure that corporate data are managed as critical assets and the data management strategy is implemented and maintained in an effective and sustainable manner.	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	
AP014.01	Define and communicate the organization's data management strategy and roles and responsibilities	Define how to manage and improve the organization's data assets, in line with enterprise strategy and objectives. Communicate the data management strategy to all stakeholders. Assign roles and responsibilities to ensure that corporate data are managed as critical assets and the data management strategy is implemented and maintained in an effective and sustainable manner.	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 (SCRIP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	8	
AP014.01	Define and communicate the organization's data management strategy and roles and responsibilities	Define how to manage and improve the organization's data assets, in line with enterprise strategy and objectives. Communicate the data management strategy to all stakeholders. Assign roles and responsibilities to ensure that corporate data are managed as critical assets and the data management strategy is implemented and maintained in an effective and sustainable manner.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRIP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
AP014.01	Define and communicate the organization's data management strategy and roles and responsibilities	Define how to manage and improve the organization's data assets, in line with enterprise strategy and objectives. Communicate the data management strategy to all stakeholders. Assign roles and responsibilities to ensure that corporate data are managed as critical assets and the data management strategy is implemented and maintained in an effective and sustainable manner.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	8	
AP014.01	Define and communicate the organization's data management strategy and roles and responsibilities	Define how to manage and improve the organization's data assets, in line with enterprise strategy and objectives. Communicate the data management strategy to all stakeholders. Assign roles and responsibilities to ensure that corporate data are managed as critical assets and the data management strategy is implemented and maintained in an effective and sustainable manner.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
AP014.02	Define and maintain a consistent business glossary	Create, approve, update and promote consistent business terms and definitions to foster shared data usage across the organization.	Functional	Subset Of	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	10	
AP014.03	Establish the processes and infrastructure for metadata management	Establish the processes and infrastructure for specifying and extending metadata about the organization's data assets, fostering and supporting data sharing, ensuring compliant use of data, improving responsiveness to business changes and reducing data-related risk.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
AP014.04	Define a data quality strategy	Define an integrated, organizationwide strategy to achieve and maintain the level of data quality (such as complexity, integrity, accuracy, completeness, validity, traceability and timeliness) required to support the business goals and objectives.	Functional	Subset Of	Quality Management System (QMS)	GOV-18	Mechanisms exist to govern a Quality Management System (QMS) to ensure security, compliance and resilience processes conform with applicable statutory, regulatory and/or contractual obligations.	10	
AP014.05	Establish data profiling methodologies, processes and tools	Implement standardized data profiling methodologies, processes, practices, tools and templates that can be applied across multiple data repositories and data stores.	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	3	
AP014.05	Establish data profiling methodologies, processes and tools	Implement standardized data profiling methodologies, processes, practices, tools and templates that can be applied across multiple data repositories and data stores.	Functional	Subset Of	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	10	
AP014.06	Ensure a data quality assessment approach	Provide a systematic approach to measure and evaluate data quality according to processes and techniques, and against data quality rules.	Functional	Subset Of	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	10	
AP014.07	Define the data cleansing approach	Define the mechanisms, rules, processes, and methods to validate and correct data according to predefined business rules.	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	8	
AP014.07	Define the data cleansing approach	Define the mechanisms, rules, processes, and methods to validate and correct data according to predefined business rules.	Functional	Intersects With	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	5	
AP014.08	Manage the life cycle of data assets	Ensure that the organization understands, maps, inventories and controls its data flows through business processes over the data life cycle, from creation or acquisition to retirement.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	
AP014.08	Manage the life cycle of data assets	Ensure that the organization understands, maps, inventories and controls its data flows through business processes over the data life cycle, from creation or acquisition to retirement.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulate data flows.	8	
AP014.08	Manage the life cycle of data assets	Ensure that the organization understands, maps, inventories and controls its data flows through business processes over the data life cycle, from creation or acquisition to retirement.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
AP014.09	Support data archiving and retention	Ensure that data maintenance satisfies organizational and regulatory requirements for availability of historical data. Ensure that legal and regulatory requirements for data archiving and retention are met.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
AP014.09	Support data archiving and retention	Ensure that data maintenance satisfies organizational and regulatory requirements for availability of historical data. Ensure that legal and regulatory requirements for data archiving and retention are met.	Functional	Subset Of	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	10	
AP014.10	Manage data backup and restore arrangements	Manage availability of critical data to ensure operational continuity.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BCDR) playbooks).	10	
AP014.10	Manage data backup and restore arrangements	Manage availability of critical data to ensure operational continuity.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	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
AP014.10	Manage data backup and restore arrangements	Manage availability of critical data to ensure operational continuity.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	8	
BAI01.01	Maintain a standard approach for program management	Maintain a standard approach for program management that enables governance and management review, decision-making and delivery management activities. These activities should focus consistently on business value and goals (i.e., requirements, risk, costs, schedule and quality targets).	Functional	Subset Of	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.	10	
BAI01.01	Maintain a standard approach for program management	Maintain a standard approach for program management that enables governance and management review, decision-making and delivery management activities. These activities should focus consistently on business value and goals (i.e., requirements, risk, costs, schedule and quality targets).	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	
BAI01.02	Initiate a program	Initiate a program to confirm expected benefits and obtain authorization to proceed. This includes agreeing on program sponsorship, confirming the program mandate through approval of the conceptual business case, appointing program board or committee members, producing the program brief, reviewing and updating the business case, developing a benefits realization plan, and obtaining approval from sponsors to proceed.	Functional	Subset Of	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.	10	
BAI01.02	Initiate a program	Initiate a program to confirm expected benefits and obtain authorization to proceed. This includes agreeing on program sponsorship, confirming the program mandate through approval of the conceptual business case, appointing program board or committee members, producing the program brief, reviewing and updating the business case, developing a benefits realization plan, and obtaining approval from sponsors to proceed.	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	
BAI01.03	Manage stakeholder engagement	Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information for all relevant stakeholders. This includes planning, identifying and engaging stakeholders and managing their expectations.	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	
BAI01.03	Manage stakeholder engagement	Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information for all relevant stakeholders. This includes planning, identifying and engaging stakeholders and managing their expectations.	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	
BAI01.03	Manage stakeholder engagement	Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information for all relevant stakeholders. This includes planning, identifying and engaging stakeholders and managing their expectations.	Functional	Subset Of	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.	10	
BAI01.03	Manage stakeholder engagement	Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information for all relevant stakeholders. This includes planning, identifying and engaging stakeholders and managing their expectations.	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	
BAI01.04	Develop and maintain the program plan	Formulate a program to lay the initial groundwork. Position it for successful execution by formalizing the scope of the work and identifying deliverables that will satisfy goals and deliver value. Maintain and update the program plan and business case throughout the full economic life cycle of the program, ensuring alignment with strategic objectives and reflecting the current status and insights gained to date.	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	
BAI01.04	Develop and maintain the program plan	Formulate a program to lay the initial groundwork. Position it for successful execution by formalizing the scope of the work and identifying deliverables that will satisfy goals and deliver value. Maintain and update the program plan and business case throughout the full economic life cycle of the program, ensuring alignment with strategic objectives and reflecting the current status and insights gained to date.	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	
BAI01.04	Develop and maintain the program plan	Formulate a program to lay the initial groundwork. Position it for successful execution by formalizing the scope of the work and identifying deliverables that will satisfy goals and deliver value. Maintain and update the program plan and business case throughout the full economic life cycle of the program, ensuring alignment with strategic objectives and reflecting the current status and insights gained to date.	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	
BAI01.05	Launch and execute the program	Launch and execute the program to acquire and direct the resources needed to accomplish the goals and benefits of the program as defined in the program plan. In accordance with stage-gate or release review criteria, prepare for stage-gate, iteration or release reviews to report progress and make the case for funding up to the following stage-gate or release review.	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	
BAI01.05	Launch and execute the program	Launch and execute the program to acquire and direct the resources needed to accomplish the goals and benefits of the program as defined in the program plan. In accordance with stage-gate or release review criteria, prepare for stage-gate, iteration or release reviews to report progress and make the case for funding up to the following stage-gate or release review.	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	
BAI01.06	Monitor, control and report on the program outcomes	Monitor and control performance against plan throughout the full economic life cycle of the investment, covering solution delivery at the program level and value/outcome at the enterprise level. Report performance to the program steering committee and the sponsors.	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 (SCRIP).	5	
BAI01.06	Monitor, control and report on the program outcomes	Monitor and control performance against plan throughout the full economic life cycle of the investment, covering solution delivery at the program level and value/outcome at the enterprise level. Report performance to the program steering committee and the sponsors.	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	
BAI01.07	Manage program quality	Prepare and execute a quality management plan, processes and practices that align with quality management standards (QMS). Describe the approach to program quality and implementation. The plan should be formally reviewed and agreed on by all parties concerned and incorporated into the program plan.	Functional	Intersects With	Quality Management System (QMS)	GOV-18	Mechanisms exist to govern a Quality Management System (QMS) to ensure security, compliance and resilience processes conform with applicable statutory, regulatory and/or contractual obligations.	5	
BAI01.07	Manage program quality	Prepare and execute a quality management plan, processes and practices that align with quality management standards (QMS). Describe the approach to program quality and implementation. The plan should be formally reviewed and agreed on by all parties concerned and incorporated into the program plan.	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.	8	
BAI01.08	Manage program risk	Eliminate or minimize specific risk associated with programs through a systematic process of planning, identifying, analyzing, responding to, monitoring and controlling the areas or events with the potential to cause unwanted change. Define and record any risk faced by program management.	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	
BAI01.08	Manage program risk	Eliminate or minimize specific risk associated with programs through a systematic process of planning, identifying, analyzing, responding to, monitoring and controlling the areas or events with the potential to cause unwanted change. Define and record any risk faced by program management.	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.	8	
BAI01.09	Close a program	Remove the program from the active investment portfolio when there is agreement that the desired value has been achieved or when it is clear it will not be achieved within the value criteria set for the program.	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	
BAI01.09	Close a program	Remove the program from the active investment portfolio when there is agreement that the desired value has been achieved or when it is clear it will not be achieved within the value criteria set for the program.	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.	8	
BAI02.01	Define and maintain business functional and technical requirements	Based on the business case, identify, prioritize, specify and agree on business information, functional, technical and control requirements covering the scope/understanding of all initiatives required to achieve the expected outcomes of the proposed IoT-enabled business solution.	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	
BAI02.01	Define and maintain business functional and technical requirements	Based on the business case, identify, prioritize, specify and agree on business information, functional, technical and control requirements covering the scope/understanding of all initiatives required to achieve the expected outcomes of the proposed IoT-enabled business solution.	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	
BAI02.02	Perform a feasibility study and formulate alternative solutions	Perform a feasibility study of potential alternative solutions, assess their viability and act on the preferred option. If appropriate, implement the selected option as a pilot to determine possible improvements.	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	
BAI02.03	Manage requirements risk	Identify, document, prioritize and mitigate functional, technical and information processing-related risks associated with the enterprise requirements, assumptions and proposed solution.	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.	8	
BAI02.04	Obtain approval of requirements and solutions	Coordinate feedback from affected stakeholders. At predetermined key stages, obtain approval and sign-off from the business sponsor or product owner regarding functional and technical requirements, feasibility studies, risk analyses and recommended solutions.	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	
BAI02.04	Obtain approval of requirements and solutions	Coordinate feedback from affected stakeholders. At predetermined key stages, obtain approval and sign-off from the business sponsor or product owner regarding functional and technical requirements, feasibility studies, risk analyses and recommended solutions.	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	
BAI03.01	Design high-level solutions	Develop and document high-level designs for the solution in terms of technology, business processes and workflows. Use agreed and appropriate phased or rapid Agile development techniques. Ensure alignment with the IoT strategy and enterprise architecture. Reassess and update the designs when significant issues occur during detailed design or building phases, or as the solution evolves. Apply a user-centric approach, ensure that stakeholders actively participate in the design and approve each version.	Functional	Subset Of	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.	10	
BAI03.01	Design high-level solutions	Develop and document high-level designs for the solution in terms of technology, business processes and workflows. Use agreed and appropriate phased or rapid Agile development techniques. Ensure alignment with the IoT strategy and enterprise architecture. Reassess and update the designs when significant issues occur during detailed design or building phases, or as the solution evolves. Apply a user-centric approach, ensure that stakeholders actively participate in the design and approve each version.	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	

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
BAI03.01	Design high-level solution	Develop and document high-level designs for the solution in terms of technology, business processes and workflows. Use agreed and appropriate phased or rapid Agile development techniques. Ensure alignment with the I&T strategy and enterprise architecture. Reassess and update the designs when significant issues surface or the solution evolves, or as the solution evolves. Apply a user-centric approach; ensure that stakeholders actively participate in the design and approve each version.	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	
BAI03.02	Design detailed solution components	Develop, document and elaborate detailed designs progressively. Use agreed and appropriate phased or rapid Agile development techniques, addressing all components (business processes and related automated and manual controls, supporting I&T applications, infrastructure services and technology products, and partners/suppliers). Ensure that the detailed design includes internal and external service level agreements (SLAs) and operational level agreements (OLAs).	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	
BAI03.02	Design detailed solution components	Develop, document and elaborate detailed designs progressively. Use agreed and appropriate phased or rapid Agile development techniques, addressing all components (business processes and related automated and manual controls, supporting I&T applications, infrastructure services and technology products, and partners/suppliers). Ensure that the detailed design includes internal and external service level agreements (SLAs) and operational level agreements (OLAs).	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
BAI03.03	Develop solution components	Develop solution components progressively in a separate environment, in accordance with detailed designs following standards and requirements for development and documentation, quality assurance (QA), and approval. Ensure that all control requirements in the business processes, supporting I&T applications and infrastructure services, services and technology products, and partner/vendor services are addressed.	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	
BAI03.03	Develop solution components	Develop solution components progressively in a separate environment, in accordance with detailed designs following standards and requirements for development and documentation, quality assurance (QA), and approval. Ensure that all control requirements in the business processes, supporting I&T applications and infrastructure services, services and technology products, and partner/vendor services are addressed.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
BAI03.03	Develop solution components	Develop solution components progressively in a separate environment, in accordance with detailed designs following standards and requirements for development and documentation, quality assurance (QA), and approval. Ensure that all control requirements in the business processes, supporting I&T applications and infrastructure services, services and technology products, and partner/vendor services are addressed.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
BAI03.04	Procure solution components	Procure solution components, based on the acquisition plan, in accordance with requirements and detailed designs, architecture principles and standards, and the enterprise's overall procurement and contract procedures. QA requirements, and approval standards. Ensure that all legal and contractual requirements are identified and addressed by the vendor.	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	
BAI03.04	Procure solution components	Procure solution components, based on the acquisition plan, in accordance with requirements and detailed designs, architecture principles and standards, and the enterprise's overall procurement and contract procedures. QA requirements, and approval standards. Ensure that all legal and contractual requirements are identified and addressed by the vendor.	Functional	Subset Of	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	10	
BAI03.05	Build solutions	Install and configure solutions and integrate with business process activities. During configuration and integration of hardware and infrastructure software, implement control, security, privacy and auditability measures to protect resources and ensure availability and data integrity. Update the product or services catalogue to reflect the new solutions.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
BAI03.05	Build solutions	Install and configure solutions and integrate with business process activities. During configuration and integration of hardware and infrastructure software, implement control, security, privacy and auditability measures to protect resources and ensure availability and data integrity. Update the product or services catalogue to reflect the new solutions.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	8	
BAI03.06	Perform quality assurance (QA)	Develop, resource and execute a QA plan aligned with the QMS to obtain the quality specified in the requirements definition and in the enterprise's quality policies and procedures.	Functional	Subset Of	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	10	
BAI03.06	Perform quality assurance (QA)	Develop, resource and execute a QA plan aligned with the QMS to obtain the quality specified in the requirements definition and in the enterprise's quality policies and procedures.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	8	
BAI03.07	Prepare for solution testing	Establish a test plan and required environments to test the individual and integrated solution components. Include the business processes and supporting services, applications and infrastructure.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	8	
BAI03.08	Execute solution testing	During development, execute testing continually (including control testing), in accordance with the defined test plan and development practices in the appropriate environment. Engage business process owners and end users in the test team. Identify, log and prioritize errors and issues identified during testing.	Functional	Subset Of	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	10	
BAI03.08	Execute solution testing	During development, execute testing continually (including control testing), in accordance with the defined test plan and development practices in the appropriate environment. Engage business process owners and end users in the test team. Identify, log and prioritize errors and issues identified during testing.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	8	
BAI03.09	Manage changes to requirements	Track the status of individual requirements (including all rejected requirements) throughout the project life cycle. Manage the approval of changes to requirements.	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	
BAI03.09	Manage changes to requirements	Track the status of individual requirements (including all rejected requirements) throughout the project life cycle. Manage the approval of changes to requirements.	Functional	Subset Of	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.	10	
BAI03.10	Maintain solutions	Develop and execute a plan for the maintenance of solution and infrastructure components. Include periodic reviews against business needs and operational requirements.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	8	
BAI03.11	Define IT products and services and maintain the service portfolio	Define and agree on new or changed IT products or services and service level options. Document new or changed product and service definitions and service level options to be updated in the products and services portfolio.	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	
BAI03.11	Define IT products and services and maintain the service portfolio	Define and agree on new or changed IT products or services and service level options. Document new or changed product and service definitions and service level options to be updated in the products and services portfolio.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
BAI03.12	Design solutions based on the defined development methodology	Design, develop and implement solutions with the appropriate development methodology (i.e., waterfall, Agile or bimodal I&T), in accordance with the overall strategy and requirements.	Functional	Subset Of	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	10	
BAI04.01	Assess current availability, performance and capacity and create a baseline	Assess availability, performance and capacity of services and resources to ensure that cost-justifiable capacity and performance are available to support business needs and deliver against service level agreements (SLAs). Create availability, performance and capacity baselines for future comparison.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	3	
BAI04.02	Assess business impact	Identify important services to the enterprise. Map services and resources to business processes and identify business dependencies. Ensure that the impact of unavailable resources is fully agreed on and accepted by the customer. For vital business functions, ensure that availability requirements can be satisfied per service level agreement (SLA).	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	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
BAI04.02	Assess business impact	Identify important services to the enterprise. Map services and resources to business processes and identify business dependencies. Ensure that the impact of unavailable resources is fully agreed on and accepted by the customer. For vital business functions, ensure that availability requirements can be satisfied per service level agreement (SLA).	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8	
BAI04.02	Assess business impact	Identify important services to the enterprise. Map services and resources to business processes and identify business dependencies. Ensure that the impact of unavailable resources is fully agreed on and accepted by the customer. For vital business functions, ensure that availability requirements can be satisfied per service level agreement (SLA).	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	8	
BAI04.03	Plan for new or changed service requirements	Plan and prioritize availability, performance and capacity implications of changing business needs and service requirements.	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	
BAI04.03	Plan for new or changed service requirements	Plan and prioritize availability, performance and capacity implications of changing business needs and service requirements.	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	
BAI04.04	Monitor and review availability and capacity	Monitor, measure, analyze, report and review availability, performance and capacity. Identify deviations from established baselines. Review trend analysis reports identifying any significant issues and variances. Initiate actions where necessary and ensure that all outstanding issues are addressed.	Functional	Subset Of	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	10	
BAI04.05	Investigate and address availability, performance and capacity issues	Address deviations by investigating and resolving identified availability, performance and capacity issues.	Functional	Subset Of	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	10	
BAI05.01	Establish the desire to change	Understand the scope and impact of the desired change. Assess stakeholder readiness and willingness to change. Identify actions that will motivate stakeholder acceptance and participation to make the change work successfully.	Functional	Subset Of	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.	10	
BAI05.02	Form an effective implementation team	Establish an effective implementation team by assembling appropriate members, creating trust, and establishing common goals and effectiveness measures.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
BAI05.03	Communicate desired vision	Communicate the desired vision for the change in the language of those affected by it. The communication should be made by senior management and include the rationale for, and benefits of, the change; the impacts of not making the change; and the vision, the road map and the involvement required of the various stakeholders.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
BAI05.04	Empower role players and identify short-term wins	Empower those with implementation roles by assigning accountability. Provide training and align organizational structures and HR processes. Identify and communicate short-term wins that are important from a change-enabler perspective.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
BAI05.05	Enable operation and use	Plan and implement all technical, operational and usage aspects so all those who are involved in the future state environment can exercise their responsibility.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
BAI05.06	Embed new approaches	Embed new approaches by tracking implemented changes, assessing the effectiveness of the operation and use plan, and sustaining ongoing awareness through regular communication. Take corrective measures as appropriate (which may include enforcing compliance).	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
BAI05.07	Sustain changes	Sustain changes through effective training of new staff, ongoing communication campaigns, continued commitment of top management, monitoring of adoption and sharing of lessons learned across the enterprise.	Functional	Subset Of	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.	10	
BAI06.01	Evaluate, prioritize and authorize change requests	Evaluate all requests for change to determine the impact on business processes and I&T services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Ensure that changes are logged, prioritized, categorized, assessed, authorized, planned and scheduled.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
BAI06.02	Manage emergency changes	Carefully manage emergency changes to minimize further incidents. Ensure the emergency change is controlled and takes place securely. Verify that emergency changes are appropriately assessed and authorized after the change.	Functional	Subset Of	Emergency Changes	CHG-07	Mechanisms exist to govern change management procedures for "emergency" changes.	10	
BAI06.03	Track and report change status	Maintain a tracking and reporting system to document rejected changes and communicate the status of approved, in-process and complete changes. Make certain that approved changes are implemented as planned.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
BAI06.03	Track and report change status	Maintain a tracking and reporting system to document rejected changes and communicate the status of approved, in-process and complete changes. Make certain that approved changes are implemented as planned.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	
BAI06.04	Close and document the changes	Whenever changes are implemented, update the solution, user documentation and procedures affected by the change.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	
BAI07.01	Establish an implementation plan	Establish an implementation plan that covers system and data conversion, acceptance testing criteria, communication, training, release preparation, promotion to production, early production support, a fallback/back-up plan, and a post-implementation review. Obtain approval from relevant parties.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	
BAI07.02	Plan business process, system and data conversion	Prepare for business process, I&T service data and infrastructure migration as part of the enterprise's development methods. Include audit trails and a recovery plan should the migration fail.	Functional	Subset Of	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	10	
BAI07.04	Establish a test environment	Define and establish a secure test environment representative of the planned business process and IT operations environment in terms of performance, capacity, security, internal controls, operational practices, data quality, privacy requirements and workloads.	Functional	Intersects With	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	8	
BAI07.04	Establish a test environment	Define and establish a secure test environment representative of the planned business process and IT operations environment in terms of performance, capacity, security, internal controls, operational practices, data quality, privacy requirements and workloads.	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	8	
BAI07.05	Perform acceptance tests	Test changes independently, in accordance with the defined test plan, prior to migration to the live operational environment.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	8	
BAI07.06	Promote to production and manage releases	Promote the accepted solution to the business and operations. Where appropriate, run the solution as a pilot implementation or in parallel with the old solution for a defined period and compare behavior and results. If significant problems occur, revert to the original environment based on the fallback/back-up plan. Manage releases of solution components.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	
BAI07.06	Promote to production and manage releases	Promote the accepted solution to the business and operations. Where appropriate, run the solution as a pilot implementation or in parallel with the old solution for a defined period and compare behavior and results. If significant problems occur, revert to the original environment based on the fallback/back-up plan. Manage releases of solution components.	Functional	Intersects With	Secure Migration Practices	TDA-08.1	Mechanisms exist to ensure secure migration practices purge Technology Assets, Applications and/or Services (TAAS) of test/development/staging data and accounts before it is migrated into a production environment.	8	
BAI07.07	Provide early production support	For an agreed period of time, provide early support to users and I&T operations to resolve issues and help stabilize the new solution.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
BAI07.08	Perform a post-implementation review	Conduct a post-implementation review to confirm outcome and results, identify lessons learned, and develop an action plan. Evaluate actual performance and outcomes of the new or changed service against expected performance and outcomes anticipated by the user or customer.	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5	
BAI08.01	Identify and classify sources of information for governance and management of I&T	Identify, validate and classify diverse sources of internal and external information required to enable governance and management of I&T, including strategy documents, incident reports and configuration information that progresses from development to operations before going live.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	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
BAI08.02	Organize and contextualize information into knowledge	Organize information based on classification criteria. Identify and create meaningful relationships among information elements and enable use of information. Identify owners, and leverage and implement enterprise-defined information levels of access to management information and knowledge resources.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
BAI08.03	Use and share knowledge	Propagate available knowledge resources to relevant stakeholders and communicate how these resources can be used to address different needs (e. problem solving, learning, strategic planning and decision making).	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
BAI08.04	Evaluate and update or retire information	Measure the use and evaluate the currency and relevance of information. Update information or retire obsolete information.	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	8	
BAI09.01	Identify and record current assets	Maintain an up-to-date, accurate record of all I&T assets that are required to deliver services and that are owned or controlled by the organization with an expectation of future benefits (including resources with economic value, such as hardware or software). Ensure alignment with configuration management and financial management.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	
BAI09.02	Manage critical assets	Identify assets that are critical in providing service capability. Maximize their reliability and availability to support business needs.	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	8	
BAI09.02	Manage critical assets	Identify assets that are critical in providing service capability. Maximize their reliability and availability to support business needs.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8	
BAI09.02	Manage critical assets	Identify assets that are critical in providing service capability. Maximize their reliability and availability to support business needs.	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	8	
BAI09.03	Manage the asset life cycle	Manage assets from procurement to disposal. Ensure that assets are utilized as effectively and efficiently as possible and are accounted for and physically protected until appropriately retired.	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	
BAI09.03	Manage the asset life cycle	Manage assets from procurement to disposal. Ensure that assets are utilized as effectively and efficiently as possible and are accounted for and physically protected until appropriately retired.	Functional	Subset Of	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	10	
BAI09.04	Optimize asset value	Regularly review the overall asset base to identify ways to optimize value in alignment with business needs.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
BAI09.04	Optimize asset value	Regularly review the overall asset base to identify ways to optimize value in alignment with business needs.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	8	
BAI09.05	Manage licenses	Manage software licenses to maintain the optimal number of licenses and support business requirements. Ensure that the number of licenses owned is sufficient to cover the installed software in use.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	8	
BAI09.05	Manage licenses	Manage software licenses to maintain the optimal number of licenses and support business requirements. Ensure that the number of licenses owned is sufficient to cover the installed software in use.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	
BAI09.05	Manage licenses	Manage software licenses to maintain the optimal number of licenses and support business requirements. Ensure that the number of licenses owned is sufficient to cover the installed software in use.	Functional	Intersects With	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	8	
BAI10.01	Establish and maintain a configuration model	Establish and maintain a logical model of the services, assets, infrastructure and recording of configuration items (CIs), including the relationships among them. Include the CIs considered necessary to manage services effectively and to provide a single, reliable description of the assets in a service.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
BAI10.02	Establish and maintain a configuration repository and baseline	Establish and maintain a configuration management repository and create controlled configuration baselines.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	8	
BAI10.02	Establish and maintain a configuration repository and baseline	Establish and maintain a configuration management repository and create controlled configuration baselines.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
BAI10.02	Establish and maintain a configuration repository and baseline	Establish and maintain a configuration management repository and create controlled configuration baselines.	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	8	
BAI10.03	Maintain and control configuration items	Maintain an up-to-date repository of configuration items (CIs) by populating any configuration changes.	Functional	Subset Of	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	10	
BAI10.04	Produce status and configuration reports	Define and produce configuration reports on status changes of configuration items.	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	8	
BAI10.05	Verify and review integrity of the configuration repository	Periodically review the configuration repository and verify completeness and correctness against the desired target.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	8	
BAI10.05	Verify and review integrity of the configuration repository	Periodically review the configuration repository and verify completeness and correctness against the desired target.	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	8	
BAI11.01	Maintain a standard approach for project management	Maintain a standard approach for project management that enables governance and management review, decision-making and delivery management activities. These activities should focus consistently on business value and goals (i. requirements, risk, costs, schedule and quality targets).	Functional	Subset Of	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.	10	
BAI11.02	Start up and initiate a project	Define and document the nature and scope of the project to confirm and develop a common understanding of project scope among stakeholders. The definition should be formally approved by the project sponsors.	Functional	Subset Of	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.	10	
BAI11.03	Manage stakeholder engagement	Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information that reaches all relevant stakeholders. This includes planning, identifying and engaging stakeholders and managing their expectations.	Functional	Subset Of	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.	10	
BAI11.04	Develop and maintain the project plan	Establish and maintain a formal, approved, integrated project plan covering business and IT resources) to guide project execution and control throughout the life of the project. The scope of projects should be clearly defined and tied to building or enhancing business capability.	Functional	Subset Of	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.	10	
BAI11.05	Manage project quality	Prepare and execute a quality management plan, processes and practices that align with quality management standards (QMS). Describe the approach to project quality and implementation. The plan should be formally reviewed and agreed on by all parties concerned and incorporated into the integrated project plans.	Functional	Subset Of	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.	10	
BAI11.06	Manage project risk	Eliminate or minimize specific risk associated with projects through a systematic process of planning, identifying, analyzing, responding to, monitoring and controlling the areas or events with potential to cause unwanted change. Define and record any risk faced by project management.	Functional	Intersects With	Prioritization To Address Evolving Risks & Threats	PRM-02.1	Mechanisms exist to integrate foundational cybersecurity practices with advanced techniques to maintain situation awareness of and minimize the organization's exposure to evolving risks and threats.	8	
BAI11.06	Manage project risk	Eliminate or minimize specific risk associated with projects through a systematic process of planning, identifying, analyzing, responding to, monitoring and controlling the areas or events with potential to cause unwanted change. Define and record any risk faced by project management.	Functional	Subset Of	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.	10	
BAI11.07	Monitor and control projects	Measure project performance against key project performance criteria such as schedule, quality, cost and risk. Identify any deviations from expected targets. Assess the impact of deviations on the project and overall program and report results to key stakeholders.	Functional	Subset Of	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.	10	
BAI11.08	Manage project resources and work packages	Manage project work packages by placing formal requirements on authorizing and accepting work packages and assigning and coordinating appropriate business and IT resources.	Functional	Subset Of	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.	10	
BAI11.09	Close a project or iteration	At the end of each project, release or iteration, require the project stakeholders to ascertain whether the project, release or iteration delivered the required results in terms of capabilities and contributed as expected to program benefits. Identify and communicate any outstanding activities required to achieve planned results of the project and/or benefits of the program. Identify and document lessons learned for future projects, releases, iterations and programs.	Functional	Subset Of	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.	10	
DSS01.01	Perform operational procedures	Maintain and perform operational procedures and operational tasks reliably and consistently.	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	
DSS01.02	Manage outsourced I&T services	Manage the operation of outsourced I&T services to maintain the protection of enterprise information and reliability of service delivery.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
DSS01.03	Monitor I&T infrastructure	Monitor the I&T infrastructure and related events. Store sufficient chronological information in operations logs to reconstruct and review time sequences of operations and other activities surrounding or supporting operations.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring 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
DSS01.04	Manage the environment	Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
DSS01.04	Manage the environment	Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	Functional	Intersects With	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	8	
DSS01.04	Manage the environment	Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	Functional	Intersects With	Automatic Voltage Controls	PES-07.1	Facility security mechanisms exist to utilize automatic voltage controls for critical system components.	8	
DSS01.04	Manage the environment	Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	Functional	Intersects With	Emergency Shutoff	PES-07.2	Facility security mechanisms exist to shut off power in emergency situations by: (1) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and (2) Protecting emergency power shutoff capability from unauthorized activation.	8	
DSS01.04	Manage the environment	Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	Functional	Intersects With	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	8	
DSS01.04	Manage the environment	Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	Functional	Intersects With	Emergency Lighting	PES-07.4	Facility security mechanisms exist to utilize and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	8	
DSS01.04	Manage the environment	Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	Functional	Intersects With	Water Damage Protection	PES-07.5	Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key personnel.	8	
DSS01.04	Manage the environment	Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	Functional	Intersects With	Automation Support for Water Damage Protection	PES-07.6	Facility security mechanisms exist to detect the presence of water in the vicinity of critical systems and alert facility maintenance and IT personnel.	8	
DSS01.04	Manage the environment	Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	Functional	Intersects With	Fire Protection	PES-08	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	8	
DSS01.04	Manage the environment	Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	Functional	Intersects With	Fire Detection Devices	PES-08.1	Facility security mechanisms exist to utilize and maintain fire detection devices/systems that activate automatically and notify organizational personnel and emergency responders in the event of a fire.	8	
DSS01.04	Manage the environment	Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	Functional	Intersects With	Fire Suppression Devices	PES-08.2	Facility security mechanisms exist to utilize fire suppression devices/systems that provide automatic notification of any activation to organizational personnel and emergency responders.	8	
DSS01.04	Manage the environment	Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	Functional	Intersects With	Automatic Fire Suppression	PES-08.3	Facility security mechanisms exist to employ an automatic fire suppression capability for critical systems when the facility is not staffed on a continuous basis.	8	
DSS01.04	Manage the environment	Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	Functional	Intersects With	Temperature & Humidity Controls	PES-09	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	8	
DSS01.04	Manage the environment	Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	Functional	Intersects With	Monitoring with Alarms / Notifications	PES-09.1	Facility security mechanisms exist to trigger an alarm or notification of temperature and humidity changes that are potentially harmful to personnel or equipment.	8	
DSS01.05	Manage facilities	Manage facilities, including power and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
DSS02.01	Define classification schemes for incidents and service requests	Define classification schemes and models for incidents and service requests.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
DSS02.01	Define classification schemes for incidents and service requests	Define classification schemes and models for incidents and service requests.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8	
DSS02.01	Define classification schemes for incidents and service requests	Define classification schemes and models for incidents and service requests.	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	8	
DSS02.01	Define classification schemes for incidents and service requests	Define classification schemes and models for incidents and service requests.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	
DSS02.02	Record, classify and prioritize requests and incidents	Identify, record and classify service requests and incidents and assign a priority according to business criticality and service agreements.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8	
DSS02.02	Record, classify and prioritize requests and incidents	Identify, record and classify service requests and incidents and assign a priority according to business criticality and service agreements.	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	8	
DSS02.03	Verify, approve and fulfill service requests	Select the appropriate request procedures and verify that the service requests fulfill defined request criteria. Obtain approval, if required, and fulfill the requests.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8	
DSS02.04	Investigate, diagnose and allocate incidents	Identify and record incident symptoms, determine possible causes, and allocate for resolution.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8	
DSS02.05	Resolve and recover from incidents	Document, apply and test the identified solutions or workarounds. Perform recovery actions to restore the I&T-related service.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8	
DSS02.05	Resolve and recover from incidents	Document, apply and test the identified solutions or workarounds. Perform recovery actions to restore the I&T-related service.	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	8	
DSS02.06	Close service requests and incidents	Verify satisfactory incident resolution and/or fulfillment of requests, and close.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8	
DSS02.07	Track status and produce reports	Regularly track, analyze and report incidents and fulfillment of requests. Examine trends to provide information for continual improvement.	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	8	
DSS03.01	Identify and classify problems	Define and implement criteria and procedures to identify and report problems. Include problem classification, categorization and prioritization.	Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	8	
DSS03.02	Investigate and diagnose problems	Investigate and diagnose problems using relevant subject matter experts to assess and analyze root causes.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8	
DSS03.03	Raise known errors	As soon as root causes of problems are identified, create known-error records, document appropriate workarounds and identify potential solutions.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	8	
DSS03.04	Resolve and close problems	Identify and initiate sustainable solutions addressing the root cause. Raise change requests via the established change management process, if required, to resolve errors. Ensure that the personnel affected are aware of the actions taken and the plans developed to prevent future incidents from occurring.	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	8	
DSS03.04	Resolve and close problems	Identify and initiate sustainable solutions addressing the root cause. Raise change requests via the established change management process, if required, to resolve errors. Ensure that the personnel affected are aware of the actions taken and the plans developed to prevent future incidents from occurring.	Functional	Intersects With	Continuous Incident Response Improvements	IRO-04.3	Mechanisms exist to use qualitative and quantitative data from incident response testing to: (1) Determine the effectiveness of incident response processes; (2) Continuously improve incident response processes; and (3) Provide incident response measures and metrics that are accurate, consistent and in a reproducible format.	8	
DSS03.05	Perform proactive problem management	Collect and analyze operational data (especially incident and change records) to identify emerging trends that may indicate problems. Log problem records to enable assessment.	Functional	Intersects With	Continuous Incident Response Improvements	IRO-04.3	Mechanisms exist to use qualitative and quantitative data from incident response testing to: (1) Determine the effectiveness of incident response processes; (2) Continuously improve incident response processes; and (3) Provide incident response measures and metrics that are accurate, consistent and in a reproducible format.	8	
DSS04.01	Define the business continuity policy, objectives and scope	Define business continuity policy and scope, aligned with enterprise and stakeholder objectives, to improve business resilience.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
DSS04.02	Maintain business resilience	Evaluate business resilience options and choose a cost-effective and viable strategy that will ensure enterprise continuity, disaster recovery and incident response in the face of a disaster or other major incident or disruption.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
DSS04.03	Develop and implement a business continuity response	Develop a business continuity plan (BCP) and disaster recovery plan (DRP) based on the strategy. Document all procedures necessary for the enterprise to continue critical activities in the event of an incident.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
DSS04.04	Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP)	Test continually on a regular basis to exercise plans against predetermined outcomes, uphold business resilience and allow innovative solutions to be developed.	Functional	Subset Of	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	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
DS504.05	Review, maintain and improve the continuity plans	Conduct a management review of the continuity capability at regular intervals to ensure its continued suitability, adequacy and effectiveness. Manage changes to the plans in accordance with the change control process to ensure that continuity plans are kept up to date and continually reflect actual business requirements.	Functional	Subset Of	Ongoing Contingency Planning	BCD-06	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services); (3) Technologies (e.g., new, altered or decommissioned technologies); (4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or (6) Feedback from contingency plan testing activities.	10	
DS504.05	Review, maintain and improve the continuity plans	Conduct a management review of the continuity capability at regular intervals to ensure its continued suitability, adequacy and effectiveness. Manage changes to the plans in accordance with the change control process to ensure that continuity plans are kept up to date and continually reflect actual business requirements.	Functional	Intersects With	Contingency Planning Components	BCD-06.1	Mechanisms exist to identify components that potentially impact the organization's ability to execute contingency plans, including changes to: (1) Personnel roles; (2) Business processes (including the use of third-party services); (3) Deployed technologies; (4) Data repositories and/or data flows; and/or (5) Physical infrastructure.	8	
DS504.06	Conduct continuity plan training	Provide all concerned internal and external parties with regular training sessions regarding procedures and their roles and responsibilities in case of disruption.	Functional	Intersects With	Contingency Training	BCD-03	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	8	
DS504.07	Manage backup arrangements	Maintain availability of business-critical information.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
DS504.07	Manage backup arrangements	Maintain availability of business-critical information.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8	
DS504.07	Manage backup arrangements	Maintain availability of business-critical information.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	8	
DS504.08	Conduct post-resumption review	Assess the adequacy of the business continuity plan (BCP) and disaster response plan (DRP) following successful resumption of business processes and services after a disruption.	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	8	
DS505.01	Protect against malicious software	Implement and maintain preventive, detective and corrective measures (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malicious software (e. ransomware, malware, viruses, worms, spyware, spam).	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	8	
DS505.01	Protect against malicious software	Implement and maintain preventive, detective and corrective measures (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malicious software (e. ransomware, malware, viruses, worms, spyware, spam).	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update anti-malware technologies, including signature definitions.	8	
DS505.01	Protect against malicious software	Implement and maintain preventive, detective and corrective measures (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malicious software (e. ransomware, malware, viruses, worms, spyware, spam).	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	8	
DS505.02	Manage network and connectivity security	Use security measures and related management procedures to protect information over all methods of connectivity.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
DS505.03	Manage endpoint security	Ensure that endpoints (e. laptop, desktop, server, and other mobile and network devices or software) are secured at a level that is equal to or greater than the defined security requirements for the information processed, stored or transmitted.	Functional	Subset Of	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	10	
DS505.03	Manage endpoint security	Ensure that endpoints (e. laptop, desktop, server, and other mobile and network devices or software) are secured at a level that is equal to or greater than the defined security requirements for the information processed, stored or transmitted.	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	8	
DS505.04	Manage user identity and logical access	Ensure that all users have information access rights in accordance with business requirements. Coordinate with business units that manage their own access rights within business processes.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	8	
DS505.04	Manage user identity and logical access	Ensure that all users have information access rights in accordance with business requirements. Coordinate with business units that manage their own access rights within business processes.	Functional	Subset Of	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	10	
DS505.05	Manage physical access to I&T assets	Define and implement procedures (including emergency procedures) to grant, limit and revoke access to premises, buildings and areas, according to business need. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This requirement applies to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	
DS505.05	Manage physical access to I&T assets	Define and implement procedures (including emergency procedures) to grant, limit and revoke access to premises, buildings and areas, according to business need. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This requirement applies to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	8	
DS505.05	Manage physical access to I&T assets	Define and implement procedures (including emergency procedures) to grant, limit and revoke access to premises, buildings and areas, according to business need. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This requirement applies to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	8	
DS505.05	Manage physical access to I&T assets	Define and implement procedures (including emergency procedures) to grant, limit and revoke access to premises, buildings and areas, according to business need. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This requirement applies to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	Functional	Subset Of	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	10	
DS505.05	Manage physical access to I&T assets	Define and implement procedures (including emergency procedures) to grant, limit and revoke access to premises, buildings and areas, according to business need. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This requirement applies to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	Functional	Intersects With	Controlled Ingress & Egress Points	PES-03.1	Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.	8	
DS505.05	Manage physical access to I&T assets	Define and implement procedures (including emergency procedures) to grant, limit and revoke access to premises, buildings and areas, according to business need. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This requirement applies to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	Functional	Intersects With	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.	8	
DS505.05	Manage physical access to I&T assets	Define and implement procedures (including emergency procedures) to grant, limit and revoke access to premises, buildings and areas, according to business need. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This requirement applies to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	8	
DS505.06	Manage sensitive documents and output devices	Establish appropriate physical safeguards, accounting practices and inventory management regarding sensitive I&T assets, such as special forms, negotiable instruments, special-purpose printers or security tokens.	Functional	Intersects With	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	8	
DS505.07	Manage vulnerabilities and monitor the infrastructure for security-related events	Using a portfolio of tools and technologies (e. intrusion detection tools), manage vulnerabilities and monitor the infrastructure for unauthorized access. Ensure that security tools, technologies and detection are integrated with general event monitoring and incident management.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	8	
DS505.07	Manage vulnerabilities and monitor the infrastructure for security-related events	Using a portfolio of tools and technologies (e. intrusion detection tools), manage vulnerabilities and monitor the infrastructure for unauthorized access. Ensure that security tools, technologies and detection are integrated with general event monitoring and incident management.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	8	
DS505.07	Manage vulnerabilities and monitor the infrastructure for security-related events	Using a portfolio of tools and technologies (e. intrusion detection tools), manage vulnerabilities and monitor the infrastructure for unauthorized access. Ensure that security tools, technologies and detection are integrated with general event monitoring and incident management.	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	3	
DS505.07	Manage vulnerabilities and monitor the infrastructure for security-related events	Using a portfolio of tools and technologies (e. intrusion detection tools), manage vulnerabilities and monitor the infrastructure for unauthorized access. Ensure that security tools, technologies and detection are integrated with general event monitoring and incident management.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMPP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	8	
DS505.07	Manage vulnerabilities and monitor the infrastructure for security-related events	Using a portfolio of tools and technologies (e. intrusion detection tools), manage vulnerabilities and monitor the infrastructure for unauthorized access. Ensure that security tools, technologies and detection are integrated with general event monitoring and incident management.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	
DS506.01	Align control activities embedded in business processes with enterprise objectives	Continually assess and monitor the execution of business process activities and related controls (based on enterprise risk), to ensure that processing controls align with business needs.	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	
DS506.01	Align control activities embedded in business processes with enterprise objectives	Continually assess and monitor the execution of business process activities and related controls (based on enterprise risk), to ensure that processing controls align with business needs.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRPR) measures of performance.	8	
DS506.02	Control the processing of information	Operate the execution of the business process activities and related controls, based on enterprise risk. Ensure that information processing is valid, complete, accurate, timely and secure (i. reflects legitimate and authorized business use).	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
DS506.02	Control the processing of information	Operate the execution of the business process activities and related controls, based on enterprise risk. Ensure that information processing is valid, complete, accurate, timely and secure (i. reflects legitimate and authorized business use).	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	
DS506.02	Control the processing of information	Operate the execution of the business process activities and related controls, based on enterprise risk. Ensure that information processing is valid, complete, accurate, timely and secure (i. reflects legitimate and authorized business use).	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and/or physical access to sensitive/regulated data.	5	
DS506.02	Control the processing of information	Operate the execution of the business process activities and related controls, based on enterprise risk. Ensure that information processing is valid, complete, accurate, timely and secure (i. reflects legitimate and authorized business use).	Functional	Intersects With	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
DSS06.03	Manage roles, responsibilities, access privileges and levels of authority	Manage business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorize access to all information assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where the data are and who is handling data on its behalf.	Functional	Intersects With	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.	3	
DSS06.03	Manage roles, responsibilities, access privileges and levels of authority	Manage business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorize access to all information assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where the data are and who is handling data on its behalf.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
DSS06.03	Manage roles, responsibilities, access privileges and levels of authority	Manage business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorize access to all information assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where the data are and who is handling data on its behalf.	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	
DSS06.03	Manage roles, responsibilities, access privileges and levels of authority	Manage business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorize access to all information assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where the data are and who is handling data on its behalf.	Functional	Intersects With	Incompatible Roles	HRS-12	Mechanisms exist to avoid incompatible development-specific roles through limiting and reviewing developer privileges to change hardware, software and firmware components within a production/operational environment.	3	
DSS06.03	Manage roles, responsibilities, access privileges and levels of authority	Manage business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorize access to all information assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where the data are and who is handling data on its behalf.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	3	
DSS06.03	Manage roles, responsibilities, access privileges and levels of authority	Manage business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorize access to all information assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where the data are and who is handling data on its behalf.	Functional	Intersects With	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	3	
DSS06.04	Manage errors and exceptions	Manage business process exceptions and errors and facilitate remediation, executing defined corrective actions and escalating as necessary. This treatment of exceptions and errors provides assurance of the accuracy and integrity of the business information process.	Functional	Intersects With	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	8	
DSS06.04	Manage errors and exceptions	Manage business process exceptions and errors and facilitate remediation, executing defined corrective actions and escalating as necessary. This treatment of exceptions and errors provides assurance of the accuracy and integrity of the business information process.	Functional	Intersects With	Threat Analysis & Flow Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	3	
DSS06.04	Manage errors and exceptions	Manage business process exceptions and errors and facilitate remediation, executing defined corrective actions and escalating as necessary. This treatment of exceptions and errors provides assurance of the accuracy and integrity of the business information process.	Functional	Intersects With	Developer Threat Analysis & Flow Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	3	
DSS06.04	Manage errors and exceptions	Manage business process exceptions and errors and facilitate remediation, executing defined corrective actions and escalating as necessary. This treatment of exceptions and errors provides assurance of the accuracy and integrity of the business information process.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	3	
DSS06.04	Manage errors and exceptions	Manage business process exceptions and errors and facilitate remediation, executing defined corrective actions and escalating as necessary. This treatment of exceptions and errors provides assurance of the accuracy and integrity of the business information process.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	3	
DSS06.05	Ensure traceability and accountability for information events	Ensure that business information can be traced to an originating business event and associated with accountable parties. This discoverability provides assurance that business information is reliable and has been processed in accordance with defined objectives.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	8	
DSS06.05	Ensure traceability and accountability for information events	Ensure that business information can be traced to an originating business event and associated with accountable parties. This discoverability provides assurance that business information is reliable and has been processed in accordance with defined objectives.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	8	
DSS06.06	Secure information assets	Secure information assets accessible by the business through approved methods, including information in electronic form (e. portable media devices, user applications and storage devices, or other methods that create new assets in any form), information in physical form (e. source documents or output reports) and information during transit. This benefits the business by providing end-to-end safeguarding of information.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
DSS06.06	Secure information assets	Secure information assets accessible by the business through approved methods, including information in electronic form (e. portable media devices, user applications and storage devices, or other methods that create new assets in any form), information in physical form (e. source documents or output reports) and information during transit. This benefits the business by providing end-to-end safeguarding of information.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	8	
DSS06.06	Secure information assets	Secure information assets accessible by the business through approved methods, including information in electronic form (e. portable media devices, user applications and storage devices, or other methods that create new assets in any form), information in physical form (e. source documents or output reports) and information during transit. This benefits the business by providing end-to-end safeguarding of information.	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and/or physical access to sensitive/regulated data.	8	
DSS06.06	Secure information assets	Secure information assets accessible by the business through approved methods, including information in electronic form (e. portable media devices, user applications and storage devices, or other methods that create new assets in any form), information in physical form (e. source documents or output reports) and information during transit. This benefits the business by providing end-to-end safeguarding of information.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	3	
MEA01.01	Establish a monitoring approach	Engage with stakeholders to establish and maintain a monitoring approach to define the objectives, scope and method for measuring business solution and service delivery and contribution to enterprise objectives. Integrate this approach with the corporate performance management system.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MEA01.02	Set performance and conformance targets	Work with stakeholders to define, periodically review, update and approve performance and conformance targets within the performance measurement system.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
MEA01.02	Set performance and conformance targets	Work with stakeholders to define, periodically review, update and approve performance and conformance targets within the performance measurement system.	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-01.3	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5	
MEA01.02	Set performance and conformance targets	Work with stakeholders to define, periodically review, update and approve performance and conformance targets within the performance measurement system.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRMP) measures of performance.	8	
MEA01.03	Collect and process performance and conformance data	Collect and process timely and accurate data aligned with enterprise approaches.	Functional	Subset Of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRMP) measures of performance.	10	
MEA01.04	Analyze and report performance	Periodically review and report performance against targets. Use a method that provides a succinct all-around view of IS&T performance and fits within the enterprise monitoring system.	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	
MEA01.05	Ensure the implementation of corrective actions	Assist stakeholders in identifying, initiating and tracking corrective actions to address anomalies.	Functional	Subset Of	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.	10	
MEA02.01	Monitor internal controls	Continuously monitor, benchmark and improve the IS&T control environment and control framework to meet organizational objectives.	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	
MEA02.01	Monitor internal controls	Continuously monitor, benchmark and improve the IS&T control environment and control framework to meet organizational objectives.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	8	
MEA02.01	Monitor internal controls	Continuously monitor, benchmark and improve the IS&T control environment and control framework to meet organizational objectives.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	8	
MEA02.01	Monitor internal controls	Continuously monitor, benchmark and improve the IS&T control environment and control framework to meet organizational objectives.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	8	
MEA02.02	Review effectiveness of business process controls	Review the operation of controls, including monitoring and test evidence, to ensure that controls within business processes operate effectively. Include activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing, continuous monitoring, independent assessments, command and control centers, and network operation centers. This evidence assures the enterprise that controls meet requirements related to business, regulatory and social responsibilities.	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	
MEA02.02	Review effectiveness of business process controls	Review the operation of controls, including monitoring and test evidence, to ensure that controls within business processes operate effectively. Include activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing, continuous monitoring, independent assessments, command and control centers, and network operation centers. This evidence assures the enterprise that controls meet requirements related to business, regulatory and social responsibilities.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	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
MEA02.02	Review effectiveness of business process controls	Review the operation of controls, including monitoring and test evidence, to ensure that controls within business processes operate effectively. Include activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing, continuous monitoring, independent assessments, command and control centers, and network operation centers. This evidence assures the enterprise that controls meet requirements related to business, regulatory and social responsibilities.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	8	
MEA02.02	Review effectiveness of business process controls	Review the operation of controls, including monitoring and test evidence, to ensure that controls within business processes operate effectively. Include activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing, continuous monitoring, independent assessments, command and control centers, and network operation centers. This evidence assures the enterprise that controls meet requirements related to business, regulatory and social responsibilities.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	8	
MEA02.03	Perform control self-assessments	Encourage management and process owners to improve controls proactively through a continuing program of self-assessment that evaluates the completeness and effectiveness of management's control over processes, policies and contracts.	Functional	Intersects With	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	8	
MEA02.04	Identify and report control deficiencies	Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.	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	
MEA02.04	Identify and report control deficiencies	Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.	Functional	Intersects With	Periodic Audits	CPL-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.	5	
MEA03.01	Identify external compliance requirements	On a continuous basis, monitor changes in local and international laws, regulations and other external requirements and identify mandates for compliance from an I&T perspective.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
MEA03.02	Optimize response to external requirements	Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider adopting and adapting industry standards, codes of good practice, and good practice guidance.	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.	3	
MEA03.02	Optimize response to external requirements	Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider adopting and adapting industry standards, codes of good practice, and good practice guidance.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCR), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
MEA03.03	Confirm external compliance	Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements.	Functional	Subset Of	Ability To Demonstrate Conformity	CPL-01.3	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	10	
MEA03.04	Obtain assurance of external compliance	Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.	Functional	Intersects With	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	8	
MEA03.04	Obtain assurance of external compliance	Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.	Functional	Intersects With	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	8	
MEA03.04	Obtain assurance of external compliance	Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	(2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner).	5	
MEA04.01	Ensure that assurance providers are independent and qualified	Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards.	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	8	
MEA04.02	Develop risk-based planning of assurance initiatives	Determine assurance objectives based on assessments of the internal and external environment and context, the risk of not achieving enterprise goals, and the opportunities associated achievement of the same goals.	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.	8	
MEA04.02	Develop risk-based planning of assurance initiatives	Determine assurance objectives based on assessments of the internal and external environment and context, the risk of not achieving enterprise goals, and the opportunities associated achievement of the same goals.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	8	
MEA04.03	Determine the objectives of the assurance initiative	Define and agree with all stakeholders on the objectives of the assurance initiative.	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	
MEA04.04	Define the scope of the assurance initiative	Define and agree with all stakeholders on the scope of the assurance initiative, based on the assurance objectives.	Functional	Intersects With	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.	8	
MEA04.04	Define the scope of the assurance initiative	Define and agree with all stakeholders on the scope of the assurance initiative, based on the assurance objectives.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	8	
MEA04.05	Define the work program for the assurance initiative	Define a detailed work program for the assurance initiative, structured according to the management objectives and governance components in scope.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
MEA04.06	Execute the assurance initiative, focusing on design effectiveness	Execute the planned assurance initiative. Validate and confirm the design of the internal controls in place. Additionally, and specifically in internal audit assignments, consider the cost-effectiveness of the governance component design.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
MEA04.06	Execute the assurance initiative, focusing on design effectiveness	Execute the planned assurance initiative. Validate and confirm the design of the internal controls in place. Additionally, and specifically in internal audit assignments, consider the cost-effectiveness of the governance component design.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	8	
MEA04.07	Execute the assurance initiative, focusing on operating effectiveness	Execute the planned assurance initiative. Test whether the internal controls in place are appropriate and sufficient. Test the outcome of the key management objectives in scope of the assurance initiative.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	8	
MEA04.08	Report and follow up on the assurance initiative	Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control weaknesses.	Functional	Intersects With	Security Assessment Report (SAR)	IAO-02.4	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	5	
MEA04.09	Follow up on recommendations and actions	Agree on, follow up on and implement the identified recommendations for improvement.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	(2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner).	5	