NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2025.3
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: NIST Cybersecurity Framework (CSF) version 2.0
https://m/gubs.nist.gov/nistpubs/CSWP/NIST.CSWP/29.pdfi
https://securecontrolstramework.com/content/atrm/scf-stm-general-nist-csf-2-0.pdf

## 1940			FID.	STRM	STRM	0000		Secure Controls Framework (SCF)	Strength of	
## 100 Part	FDE#	FDE Name	Focal Document Element (FDE) Description	Rationale	Relationship		SCF#		Relationship (optional)	Notes (optional)
Part					subset of	Protection Governance Program	GOV-01	protection governance controls.	10	
March   Marc	GV	N/A		Functional	intersects with		GOV-05	protection program measures of performance.	8	
1	J.			cuolidi	subset of		RSK-01		10	
No.					intersects with		PRM-01.1		5	
Part					auboat of	Defining Business	001/09		10	
## 100 Part   Pa					subset of	Context & Mission	GOV-08		10	
March   Marc			The sign metapose mission stakeholder expectations		intersects with		AST-01.1	Applications and/or Services (TAAS), Applications and/or Services (TAAS) that support more than one critical business function.	5	
1400   1400	GV.OC	N/A	dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management	Functional	intersects with	Identification &	AST-01.2	Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
March   Marc					intersects with	Contractual Compliance	CPL-01	statutory, regulatory and contractual controls.	5	
March   Marc					intersects with	Accountable, Supportive, Consulted & Informed	TPM-05.4	Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between	5	
100   100					subset of	Defining Business	GOV-08	Mechanisms exist to define the context of its business model and document the	10	
Marchane   Park   Processed and Control of								Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring;		
March   Marc	GV.OC-01	N/A		Functional	intersects with	Risk Framing	RSK-01.1	(3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing	5	
March   100					intersects with	Threat Modeling	TDA-06.2		4	
March   Part						Stakeholder		accounted for.  Mechanisms exist to identify and involve pertinent stakeholders of critical		
Manual					intersects with	Involvement	AST-01.2	ongoing secure management of those assets.  Mechanisms exist to require contractual requirements for cybersecurity and data	5	
## 100-00-00  *****************************	GV.OC-02	N/A	expectations regarding cybersecurity risk management are understood	Functional	intersects with	Requirements	TPM-05	protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
March   Marc					intersects with	Accountable, Supportive, Consulted & Informed	TPM-05.4	Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	
March   Marc					subset of		CPL-01		10	
March   1904   1905				intersects with	Protection Controls	CPL-02		5		
Market Ma			cybersecurity — including privacy and civil liberties obligations — are		intersects with		PRI-01		8	
Marcanian and Part	GV.OC-03	N/A		Functional		Third-Party Contract		Data (PD) are processed lawfully, fairly and transparently.  Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to	5	
Processor International Inte					intercents with	Contract Flow-Down	TPM_05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are	5	
OUT-MET  NAT  Profession and except the new exceptions, updations, and workers that will be extended to general own one operation on proceed from the operations of the second of the se								Mechanisms exist to define the context of its business model and document the		
OV. PM NA  PARA  Chical objectives, capabilities, and services the reference of the referen				Functional	intersects with		GOV-08		5	
OV.00-10  NA  Procedure of the processor	CV OC 04	N/A		Functional	intersects with	-	BCD-02	business functions.	5	
Processor NA  NA  Outcomes, coasibilities, and services that the organization depends on any subject to the complete service that the organization depends on any subject to the complete service that the organization depends on any subject to the complete service that the organization depends on any subject to the complete service that the organization depends on any subject to the complete service that the organization depends on any subject to the complete service that the organization depends on any subject to the complete service that the organization depends on any subject to the complete service that the organization depends on any subject to the complete service that the organization depends on any subject to the complete service that the organization depends on the service that the organization of the service that the organization of the service that the organization depends on the service that the organization of the service that the organization of the service that the organization of the organization depends on the service that the organization of the organization of the service that the organization of the organi	31.33 34	TWA		Functional	intersects with		PRM-01.1	specific business plan and set of objectives to achieve that plan.	5	
OV.DOS  NAS  Outcomes, capacitations, and services that the organization depend on an understood and communicated.  Functional  Functional				Functional	intersects with		TPM-02	critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the	5	
Outcomes, capabilities, and services that the organization depends of an understood and communicated.  Punctional  Intersects with Punch Principles  Intersects with Punctional  Intersects with Punct					intersects with	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets,	5	
Functional  OV.PM  NA  Risk management objectives are established and agreed to by organization at stakeholders.  Functional  NA  Risk management objectives are established and agreed to by organizations at stakeholders.  Functional  NA  Risk management objectives are established and agreed to by organizations at stakeholders.  Functional  Risk management objectives are established and agreed to by organizations distakeholders.  Functional  Risk management objectives are established and agreed to by organizations distakeholders.  Functional  Risk management objectives are established and agreed to by organizations distakeholders.  Functional  Risk management objectives are established and agreed to by organizations distakeholders.  Functional  Risk management objectives are established and agreed to by organizations distakeholders.  Functional  Risk management objectives are established and agreed to by organizations distakeholders.  Functional  Risk management objectives are established and agreed to by organizations distakeholders.  Functional  Risk management objectives are established and agreed to by organizations at stakeholders.  Functional  Risk management objectives are established and agreed to by organizations at stakeholders.  Functional  Risk management objectives are established and agreed to by organizations at stakeholders.  Functional  Risk management objectives are established and agreed to by organizations and stakeholders.  Functional  Risk management objectives are established and agreed to by organizations and stakeholders.  Functional  Risk management objectives are established and agreed to by organizations and stakeholders.  Functional  Risk management objectives are established and agreed to by organizations and stakeholders.  Functional  Risk management objectives are established and agreed to by organizations and stakeholders.  Functional  Risk management objectives are established and agreed to by organizations and stakeholders.  Functional  Risk management objectives are establishe	GV.OC-05	N/A		Functional	intersects with	Software Bill of Materials	TDA-04.2	Technology Assets, Applications and/or Services (TAAS) that lists software	4	
Assigned Cylemencum by Analysin Cylemencum by			are understood and communicated.	I NA	intersects with	Third-Party Criticality	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	5	
OV.RM NA  Risk Management  Ov.RM-O1  NA  Risk Management objectives are established and agreed to by organizational state shortly september of a subserver of protection with severe or a subserver of a					intersects with	Data Protection	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	5	
Washingsment (and protection objectives a restallation of the protection objectives and protection objectives are settlements, and assumptions are established, communicated, and used to support operational risk decisions.  Which then organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.  Functional  Functional  N/A  N/A  N/A  Risk management Cobjectives are established and agreed to by organization at stakeholders.  Functional  Functional  Analysis of the protection downship of the protection objectives are established and agreed to by organization at stakeholders.  Functional  Functional  Analysis of the protection downship of the protection objectives are established and agreed to by organization at stakeholders.  Functional  Functional  Functional  Analysis of the protection objectives are established and agreed to by organization at stakeholders.  Functional  Functional  Functional  Analysis of the protection objectives are established and agreed to by organization at stakeholders.  Functional					intersects with	Cybersecurity & Data	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity and data	5	
OV.RM  NA  The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.  Functional  Functional  OV.RM-01  N/A  Risk management controls.  Functional  F						Management		achieving cybersecurity and data protection objectives.  Mechanisms exist to establish a strategic cybersecurity and data protection-		
The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.  Functional  Functi					intersects with	Objectives	rnm-01.1		,	
Used to support operational risk decisions.    Functional   N/A	GV RM	N/A	The organization's priorities, constraints, risk tolerance and appetite	Functional	intersects with		RSK-01	tactical risk management controls.	5	
Intersects with   Risk Tolerance   Risk-Claimance   Ris	Ov.ne1	IVA		, anduorist	intersects with	Risk Framing	RSK-01.1	(1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing	8	
Functional  N/A  Risk management objectives are established and agreed to by organizational stakeholders.  Functional  Intersects with  Financional  Functional  F					intersects with	Risk Tolerance	RSK-01.3		8	
GV.RM-01  N/A  Risk management objectives are established and agreed to by organizational stakeholders.  Functional  Steering Committee & Program Oversight  OOV-01.  10  OOV-01.  OOV-01.  OOV-01.  Steering Committee or advisory board, comprised or key of persecurity, data protection and business executives, which meets formally and on a regular beals.  Mechanisms exist to develop, report and monitor Key Risk Indicators (Risk) to every and data protection program.  Risk Management In performance monitoring and tread analysis of the 3 cybersecurity and data protection program.  Risk Management In performance monitoring and tread analysis of the 3 cybersecurity and data protection program.  Risk Management In performance monitoring and tread analysis of the 3 cybersecurity and data protection program.  Risk Management In performance monitoring and tread analysis of the 3 cybersecurity and data protection program.  Risk Management In performance monitoring and tread analysis of the 3 cybersecurity and data protection program.					intersects with	Risk Appetite	RSK-01.5		8	
Risk management objectives are established and agreed to by organizational stakeholders.  Functional					subset of	Protection Governance	GOV-01		10	
Risk management objectives are established and agreed to by organizational stakeholders.  Functional								Mechanisms exist to coordinate cybersecurity, data protection and business		
intersects with Key Risk Indicators (KRIs) GOV-05.2 assist senior management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring and trend analysis of the 3 cybersective management in performance monitoring management in performance	GV.RM-01	N/A		Functional	intersects with		GOV-01.1	cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	10	
intersects with Risk Management Risk Management RSK-nt Mechanisms exist to facilitate the implementation of strategic, operational and 5					intersects with	Key Risk Indicators (KRIs)	GOV-05.2	assist senior management in performance monitoring and trend analysis of the	3	
					intersects with		RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and	5	



1 of 16

March   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 (optional)	Notes (optional)
March   Marc	GV RM-02	N/A		Functional	intersects with	Risk Tolerance	RSK-01.3	acceptable results.	10	
March   1900			communicated, and maintained.		intersects with		RSK-01.5	the organization is willing to accept in anticipation of a reward.	10	
## 14 Page 14					subset of	Protection Governance	GOV-01		10	
March   Marc	GV.RM-03	N/A		Functional						
## 14 Part			in enterprise risk management processes.		intersects with	Program Oversight	GOV-01.1	cybersecurity, data privacy and business executives, which meets formally and on	5	
March   1906					subset of	Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
March   Marc					subset of		RSK-01	tactical risk management controls.	10	
Mathematical   Math								(1) Assumptions affecting risk assessments, risk response and risk monitoring;		
March   Marc					intersects with	Risk Framing	RSK-01.1	(3) The organizational risk tolerance; and	5	
March   Marc	GV.RM-04	N/A		Functional						
Marchan   Marc					intersects with	Risk Remediation	RSK-06		5	
100   100					superset of	Risk Response	RSK-06.1	assessments, incidents and audits to ensure proper remediation has been	5	
Part					intersects with	Countermeasures	RSK-06.2	reduce risk and exposure to threats.	5	
Part					intersects with	Data Protection	GOV-04	resources to centrally-manage, coordinate, develop, implement and maintain an	5	
March   Marc					intersects with	Stakeholder	GOV-04 1	Mechanisms exist to enforce an accountability structure so that appropriate teams	5	
The column   The	GV.RM-05	N/A		Functional				and managing data and technology-related risks.	-	
Part			parties.		intersects with	Responsibilities	HRS-03		5	
March   Marc					intersects with	Accountable, Supportive,	TPM-05.4	Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to	5	
March   Marc						(RASCI) Matrix		internal stakeholders and External Service Providers (ESPs).		
Manual   M					subset of		RSK-01	tactical risk management controls.	10	
Part								(1) Assumptions affecting risk assessments, risk response and risk monitoring;		
March   March   Property   Prop					intersects with	Risk Framing	RSK-01.1	(3) The organizational risk tolerance; and	5	
Part	GV.RM-06	N/A		Functional						
Math					intersects with	Rick Accessment	B&K-UV	likelihood and magnitude of harm, from unauthorized access, use, disclosure,	5	
March   Marc					III.OI OCCIO WIGH	THUK PUDGUSTION	HOR 64	Applications, Services and/or Data (TAASD).	J	
## Part					intersects with	Risk Register	RSK-04.1		5	
18								Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring;		
March   Marc	GV.RM-07	N/A		Functional	subset of	Risk Framing	RSK-01.1	(2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and	10	
Company   Comp			, , , , , , , , , , , , , , , , , , , ,							
OCARGO NA PART OCARGO NA PACTOR OF THE PART OCARGO NA PACTOR OCARGO NA PAC					intersects with		HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
OURSES  NA  Operation in terms of any operation of control showers any of the protection control showers in a control showers in a control showers in the contro	GV.RR	N/A	accountability, performance assessment, and continuous	Functional		Responsible,				
A Marie of M			improvement are established and communicated.		intersects with	Consulted & Informed	TPM-05.4	delineate assignment for cybersecurity and data protection controls between	8	
Marco					subset of	Cybersecurity & Data	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data	10	
Organizational inaderative in reportation of inaderative in reportation in reportation in reportation in reportation in report						Program		Mechanisms exist to coordinate cybersecurity, data protection and business		
August Communication of the season and secondary of the communication of					intersects with		GOV-01.1	cybersecurity, data privacy and business executives, which meets formally and on		
Operation is selected by an expension of selected by an ex					intersects with			Mechanisms exist to assign one or more qualified individuals with the mission and	5	
OVER 21  NA PARTICIPATION AND PRODUCT OF THE PARTICIPATION AND PRO						Responsibilities		enterprise-wide cybersecurity and data protection program.  Mechanisms exist to enforce an accountability structure so that appropriate teams	-	
Wild of Nin do Nin A Colora color in the form results and overtextually improved.  Interacts with Plas Tolerance Plas Colorance Plas Coloranc			Organizational leadership is responsible and accountable for		intersects with		GOV-04.1	and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	
OVAN-GS  NA  Adequate resources are allocated commensurals with the cybersourly fall strength of the particular of the p	GV.RR-01	N/A		Functional	intersects with		RSK-01		5	
OV.RP-02 NA Appetite set and authorities related to operandum/risk management are established, communicated, understood, and enforced.  NA Adaptate resources are allocated commensurate with the operandum set and authorities related to operandum set and process of the operandum set of person and personal commensurate with the operandum set of the operandum set of personal set operandum set of personal set operandum set of personal set operandum set operandum set of personal set operandum set of personal set operandum set operandu					intersects with	Risk Tolerance	RSK-01.3		5	
W.R-G2  N/A  Roles, responsibilities, and purcharises designed to operance are allocated communicated, understood, and enforced.  Purctional  Adequate resources are allocated communicates are allocated communicates are allocated communicates, and policies.  Purctional  OV.RR-G3  N/A  Adequate resources are allocated communicates are allocated communicates. Purctional  Purctional  OV.RR-G4  N/A  Overlandourly is included in human resources practices.  Functional  OV.RR-G4  N/A  Overlandourly is included in human resources practices.  Functional  OV.RR-G4  N/A  Overlandourly is included in human resources practices.  Functional  OV.RR-G4  N/A  Overlandourly is included in human resources practices.  Functional  Intersects with  Functional  Intersects with  Overlandourly is included in human resources practices.  Functional  Overlandourly is included in human resources practices.  Functional  Overlandourly is included in human resources practices.  Functional  Intersects with  Overlandourly is included in human resources practices.  Functional  Overlandourly is included in human resources practices.  Functional  Functional  Overlandourly is included in human resources practices.  Functional  Functional								Mechanisms exist to define organizational risk threshold, the level of risk exposure		
Main					intersects with	Risk Threshold	RSK-01.4		5	
OV.RR-02 NA Roles, responsibilities, and authorities related to operacurity risk management are established, communicated, understood, and enforced.  Functional OV.RR-03 NA Adequate resources are allocated commensustate with the cycles-recurity risk strategy, roles, responsibilities.  OV.RR-04 NA Organizational Cycles-recurity risk strategy, roles, responsibilities.  OV.RR-05 NA Organizational Cycles-recurity risk strategy roles, responsibilities.  OV.RR-06 NA Organizational Cycles-recurity risk strategy roles, responsibilities.  Intersects with Peacle Na Na Organizational Cycles-recurity risk strategy roles, responsibilities.  OV.RR-06 NA Organizational Cycles-recurity risk strategy roles, responsibilities, and policies.  Functional Intersects with Peacle Na Na Organizational Cycles-recurity risk strategy roles, responsibilities, and policies.  Functional Intersects with Peacle Na Na Organizational Cycles-recurity risk strategy roles, responsibilities, and policies.  Functional Intersects with Peacle Na Na Organizational Cycles-recurity risk strategy roles, responsibilities, and policies.  Functional Intersects with Peacle Na Na Organizational Cycles-recurity risk strategy roles, responsibilities, and policies.  Functional Intersects with Peacle Na Na Organizational Cycles-recurity role and strategy related risk with resource planning controls that define a viable plan for schedule plan for schedule resource responsibilities to responsibilities and factorities to replications to replications of this subgesteron.  OV.RR-05					intersects with	Risk Appetite	RSK-01.5	the organization is willing to accept in anticipation of a reward.	5	
Rodes, responsibilities and authorities related to rijhorascurity risk management are established, communicated, understood, and enforced.  Rodes, responsibilities and authorities related to rijhorascurity risk passings of six management are established, communicated, understood, and enforced.  Defined Roles & Responsibilities Intersects with Postion Categorization  Planting Roles & Responsibilities Intersects with Postion Categorization  Procedure Responsibilities Intersects with Postion Categorization  Responsibilities Intersects with Postion Categorization  Responsibilities Intersects with Postion Responsibilities Intersects with Postion Responsibilities Intersects with Postion Responsibilities Intersects with Postion Responsibilities  Responsibilities Intersects with Postion Responsibilities Intersects with Postion Postion Responsibilities Intersects with Postion Responsibilities Intersects with Postion Responsibilities  Rectanting exist to decimat					intersects with	Risk Culture	RSK-12		5	
Responsibilities   Responsibilit					intersects with	Assigned Cybersecurity &			5	
Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.  Functional entersects with Position Categorization   HiS-SQ designation to all positions and establishing scoreoning criteria for individuals filling these positions.  Defined Roles & Intersects with Position Categorization   HiS-SQ separative, consulted with the propositions and established, communicated, and enforced.  Pinctional entersects with Position Categorization   HiS-SQ separative, consulted with the positions and established communicated, and enforced.  Pinctional entersects with Position Categorization   HiS-SQ separative, consulted separation to all positions and established for individuals filling these positions.  Pinctional entersects with Position Categorization   HiS-SQ separative, consulted separation   HiS-SQ separative, consulted separation   HiS-SQ separative, consulted services   HiS-SQ separ					soots with	Responsibilities		enterprise-wide cybersecurity and data protection program.		
enforced.    Intersects with   Defined Roles & Personsibilities   HRS-03   Feature   Functional   Functional	OV PP	N/*		Francis	intersects with	Position Categorization	HRS-02	designation to all positions and establishing screening criteria for individuals filling those positions.		
Adequate resources are allocated commensurate with the cybersecurity in intersects with  Adequate resources are allocated commensurate with the cybersecurity in intersects with  Adequate resources are allocated commensurate with the cybersecurity in intersects with  Adequate resources are allocated commensurate with the cybersecurity and star protection objectives.  Functional  GV.RR-04  N/A  Cybersecurity is included in human resources practices.  Functional  OV.RR-04  N/A  Organizational cybersecurity policy is established, communicated, and enforced.  Functional  Functiona	GV.RR-02	N/A		runctional	intersects with		HRS-03	mecnanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.  WA Cybersecurity is included in human resources practices.  Functional  OV.PO  NIA  Organizational cybersecurity policy is established, communicated, and enforced.  NIA  Organizational cybersecurity policy is established, communicated, and enforced.  Intersects with  Functional  Functional							TOLL		_	
Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.  GV.RR-04  N/A  Cybersecurity is included in human resources practices.  Functional  GV.PO  N/A  Organizational cybersecurity policy is established, communicated, and enforced.  Functional  Funct					intersects with	Consulted & Informed (RASCI) Matrix	IPM-05.4	delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	
Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.  Functional  GV.RR-04  N/A  A Cybersecurity is included in human resources practices.  Functional					intersects with	Protection Portfolio	PRM-01	protection-related resource planning controls that define a viable plan for	5	
GV.RP-04 N/A Organizational cybersecurity policy is established, communicated, and enforced.    Management   Subscript Amagement   S	GV.RR-03	N/A		Functional	intersects with	Cybersecurity & Data	PRM-02	Mechanisms exist to address all capital planning and investment requests,	5	
GV.RR-04 N/A Cybersecurity is included in human resources practices.  Functional Cybersecurity is included in human resources practices.  Functional Functional Cybersecurity and communicated, and enforced.  Functional Functional Cybersecurity policy is established, communicated, and enforced.  Functional Functional Functional Cybersecurity policy is established, communicated, and enforced.  GV.PO N/A Organizational cybersecurity policy is established, communicated, and enforced.  Functional Functional Functional Approaches the first of the functional intersects with processing the functional processing to functional processing to consider the implementation of personnel security controls. 10  Mechanisms exist to establish, mentitain as safe and secure working environment. Mechanisms exist to establish, mentitain as and secure working environment. Mechanisms exist to establish, mentitain as defensional expenses curity and data procedures. 10  Mechanisms exist to establish, mentitain and disseminate cybersecurity and data procedures and provide procedures and procedures and expenses and the implementation of personnel security controls. 10  Mechanisms exist to establish, mentitain as safe and secure working environment. Mechanisms exist to establish, mentitain as and security controls. 10  Mechanisms exist to establish, mentitain as safe and security controls. 10  Mechanisms exist to establish, mentitain as safe and security controls. 10  Mechanisms exist to establish, mentitain as safe and security controls. 10  Mechanisms exist to ensure personnel security controls. 10  Mechanisms exist			сурывесилку risk strategy, roles, responsibilities, and policies.			Management		protection programs and document all exceptions to this requirement.		
GV.RP-04 N/A Cybersecurity is included in human resources practices.  Functional intersects with leaves about their roles and seponsibilities to communicate with users about their roles and seponsibilities to communicate with users about their roles and seponsibilities to maintain a safe and secure working environment.  Mechanisms exist to communicate with users about their roles and seponsibilities to maintain a safe and secure working environment.  Mechanisms exist to establish, maintain and disseminate cybersecurity and data procedures.  Mechanisms exist to establish, maintain and disseminate cybersecurity and data procedures.  The communication of					equal		PRM-03	technical and data protection requirements within business process planning for projects / initiatives.	10	
GV.PO  N/A  Organizational cybersecurity policy is established, communicated, and enforced.  Functional  Functiona	GV.RR-04	N/A	Cybersecurity is included in human resources practices.	Functional		Security Management				
GV.PO  N/A  Organizational cybersecurity policy is established, communicated, and enforced.  Functional  Functiona					intersects with		HRS-03.1	responsibilities to maintain a safe and secure working environment.	5	
GV.PO  N/A  Organizational cybersecurity policy is established, communicated, and enforced.  Functional functional enforced.  Functional functional intersects with additional enforced intersects with additional					subset of	& Data Protection	GOV-02		10	
intersects with Acknowledgement HRS-05.7   organization's cybersecurity and data protection policies and provide 5	GV.PO	N/A		Functional			LIDO 1		_	
јаланитецернен.					intersects with		HKS-05.7	organization's cybersecurity and data protection policies and provide acknowledgement.	5	



FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
				intersects with	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
				subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	10	
GV.PO-01	N/A	Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.	Functional	intersects with	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's cybersecurity and data protection policies and provide acknowledgement.	5	
				intersects with	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
				intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
GV.PO-02	N/A	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.	Functional	intersects with	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's cybersecurity and data protection policies and provide acknowledgement.	8	
				intersects with	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	8	
				intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecunity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
GV.OV	N/A	Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program.	5	
		management strategy.		intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5	
				intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
				intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
				intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection	5	
GV.OV-01	N/A	Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.	Functional	intersects with	Measures of Performance	GOV-05	program.  Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5	
				intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
				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	
				intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity and data protection- specific business plan and set of objectives to achieve that plan.	5	
				subset of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	10	
GV.OV-02	N/A	N/A  The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.	Functional	subset of	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	10	
			intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5		
				intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
GV.OV-03	N/A	Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed.	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program.	5	
				intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5	
				intersects with	Risk Management Program Cybersecurity & Data	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.  Mechanisms exist to facilitate the implementation of cybersecurity and data	5	
				subset of	Protection Governance Program	GOV-01	protection governance controls.  Mechanisms exist to coordinate cybersecurity, data protection and business	10	
				intersects with	Steering Committee & Program Oversight	GOV-01.1	alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
				intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program.	5	
GV.SC	N/A	Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5	
64.30	IWA	stakeholders.	runctional	intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
				equal	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 Teachardoly Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	10	
				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).	5	
				intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets,	8	
				subset of	Cybersecurity & Data Protection Governance	GOV-01	Applications and/or Services (TAAS) supply chains; and Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
				intersects with	Program  Steering Committee &  Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on	5	
GV.SC-01	N/A	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by	Functional	intersects with	Publishing Cybersecurity & Data Protection	GOV-02	Cyberisecurity, data privacy and business executives, which meets formatly and on a regular basis.  Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	
		organizational stakeholders.		intersects with	Documentation  Risk Management	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
					Program  Supply Chain Risk  Management (SCRM)		Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of		
				equal	Management (SCRM) Plan	RSK-09	Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.  Mechanisms exist to require contractual requirements for cyberse	10	
		Cybersecurity roles and responsibilities for suppliers, customers, and		intersects with	Third-Party Contract Requirements	TPM-05	protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).  Mechanisms exist to ensure cybersecurity and data protection requirements are	8	
GV.SC-02	N/A	partners are established, communicated, and coordinated internally and externally.	Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	included in contracts that flow-down to applicable sub-contractors and suppliers.	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 (optional)	Notes (optional)
				intersects with	Responsible, Accountable, Supportive, Consulted & Informed	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between	8	
				subset of	(RASCI) Matrix Cybersecurity & Data Protection Governance	GOV-01	internal stakeholders and External Service Providers (ESPs).  Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
				intersects with	Program  Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on	5	
					Publishing Cybersecurity		cybersecurity, data privacy and business executives, which meets formally and on a regular basis.  Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.		
		Cybersecurity supply chain risk management is integrated into		intersects with	& Data Protection Documentation  Defining Business	GOV-02	Mechanisms exist to define the context of its business model and document the	5	
GV.SC-03	N/A	cybersecurity and enterprise risk management, risk assessment, and improvement processes.	Functional	intersects with	Context & Mission	GOV-08	organization's mission.  Mechanisms exist to establish control objectives as the basis for the selection,	5	
				intersects with	Objectives Risk Management	GOV-09 RSK-01	implementation and management of the organization's internal control system.  Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
				intersects with	Program Supply Chain Risk	RSK-U1	Tactical risk management controls.  Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of	•	
				intersects with	Management (SCRM) Plan	RSK-09	Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
				intersects with	Asset Governance Asset-Service	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.  Mechanisms exist to identify and assess the security of Technology Assets,	5	
				intersects with	Dependencies Third-Party Management	AST-01.1	Applications and/or Services (TAAS), Applications and/or Services (TAAS) that support more than one critical business function.  Mechanisms exist to facilitate the implementation of third-party management	5	
GV.SC-04	N/A	Suppliers are known and prioritized by criticality.	Functional				controls.  Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity.		
				intersects with	Third-Party Inventories	TPM-01.1	Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).  Mechanisms exist to identify, prioritize and assess suppliers and partners of	8	
				intersects with	Third-Party Criticality Assessments	TPM-02	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	
				intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.  Mechanisms exist to document and validate the scope of cybersecurity and data	5	
				intersects with	Compliance Scope	CPL-01.2	protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
				intersects with	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive / regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
				intersects with	Data Privacy Requirements for Contractors & Service	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
GV.SC-05	N/A	Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties.	Functional	intersects with	Providers  Risk Management  Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
				intersects with	Supply Chain Risk	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of	5	
				intersects with	Management (SCRM) Plan	RSK-09	Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.  Mechanisms exist to require contractual requirements for cybersecurity and data		
				intersects with	Third-Party Contract Requirements	TPM-05	protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
				intersects with	Contract Flow-Down Requirements	TPM-05.2		5	
				intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.  Mechanisms exist to identify, prioritize and assess suppliers and partners of	5	
				intersects with	Third-Party Criticality Assessments	TPM-02	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.	5	
				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	5	
				intersects with	Limit Potential Harm	TPM-03.2	to those risks and threats, as necessarv.  Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5	
				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	5	
				intersects with	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
				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).	5	
				intersects with	Conflict of Interests Third-Party Processing,	TPM-04.3	Services (1945).  Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.  Mechanisms exist to restrict the location of information processing/storage based	5	
				intersects with	Storage and Service Locations	TPM-04.4	on business requirements.	5	
GV.SC-06	N/A	Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
				intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
				intersects with	Third-Party Authentication Practices	TPM-05.3	Mechanisms exist to ensure External Service Providers (ESPs) use unique authentication factors for each of its customers.	5	
				intersects with	Responsible, Accountable, Supportive, Consulted & Informed	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between	5	
				intersects with	(RASCI) Matrix Third-Party Scope Review	TDM OF C	Internal stakeholders and External Service Providers (ESPs). Mechanisms exist to perform recurring validation of the Responsible, Accountable Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity and data protection control assignments accurately reflect	5	
					arry acope neview		ensure cybersecurity and data protection control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.  Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable		
				intersects with	First-Party Declaration (1PD)	TPM-05.6	External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to	5	
				intersects with	Break Clauses	TPM-05.7	subcontractors.  Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data privacy controls.	5	
				intersects with	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
				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.	5	
				intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
		I	l			ļ		1	



FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)		
				intersects with	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets,	5			
				intersects with	Third-Party Criticality Assessments	TPM-02	Applications, Services and/or Data (TAASD).  Applications, Services and/or Data (TAASD).  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 or high-ralus services.	5			
				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	5			
GV.SC-07	N/A	The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed,	Functional	intersects with	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5			
		responded to, and monitored over the course of the relationship.		intersects with	Processes To Address Weaknesses or	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	5			
				intersects with	Deficiencies Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5			
				intersects with	Third-Party Risk Assessments &	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or	5			
				intersects with	Approvals  Review of Third-Party  Services	TPM-08	Services (TAAS).  Mechanisms exist to monitor, regularly review and assess External Service  Providers (ESPs) for compliance with established contractual requirements for	5			
				intersects with	Third-Party Deficiency Remediation	TPM-09	cybersecurity and data protection controls.  Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5			
					Business Continuity		Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services				
				intersects with	Management System (BCMS)	BCD-01	(TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).  Mechanisms exist to coordinate internal contingency plans with the contingency	5			
				intersects with	Coordinate With External Service Providers	BCD-01.2	plans of external service providers to ensure that contingency requirements can be satisfied.	5			
				intersects with	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.  Mechanisms exist to cover:  (1) Preparation;	5			
				intersects with	Incident Handling	IRO-02	(2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment;	5			
							(5) Eradication; and (6) Recovery.  Mechanisms exist to coordinate with approved third-parties to achieve a cross-				
GV.SC-08	N/A	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities.	Functional	Functional	Functional	intersects with	Correlation with External Organizations	IRO-02.5	organization perspective on incident awareness and more effective incident responses.	5	
				intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.  Mechanisms exist to maintain a current, accurate and complete list of External	5			
				intersects with	Third-Party Inventories	TPM-01.1	Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications. Services and/or Data (TAASD).	5			
				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.	5			
			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.	5				
				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.	5			
				intersects with	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5			
				subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10			
				intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecunity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5			
				intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection	5			
				intersects with	Measures of Performance	GOV-05	program.  Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5			
		Supply chain security practices are integrated into cybersecurity and		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			
GV.SC-09	N/A	enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle.	Functional	intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5			
					Supply Chain Risk		Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of				
				intersects with	Management (SCRM) Plan	RSK-09	Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5			
				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).	5			
				intersects with	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.  Mechanisms exist to design and implement product management processes to	5			
				intersects with	Product Management	TDA-01.1	Mechanisms exist to essign and implement product management processes proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:  Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM)	5			
				subset of	Supply Chain Risk Management (SCRM) Plan	RSK-09	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.	10			
GV.SC-10	N/A	Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5			
		-g		intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5			
				intersects with	Third-Party Authentication Practices	TPM-05.3	Mechanisms exist to ensure External Service Providers (ESPs) use unique authentication factors for each of its customers.	5			
				subset of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	10			
				intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program.	5			
				intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5			



				Relationship		SCF#	Control Description	Relationship (optional)	Notes (optional)
ID	N/A	The organization's current cybersecurity risks are understood.	Functional	intersects with	Risk Framing	RSK-01.1	(4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
				intersects with	Risk Identification Risk Catalog	RSK-03.1	Mechanisms exist to identify and document risks, both internal and external.  Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	
				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, Exprise and/or Data (T/ASD).	5	
				intersects with	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
				intersects with	Risk Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.	5	
				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.	5	
				subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
				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.	5	
				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.	5	
				intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TASE) 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.	5	
				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.	5	
				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.	5	
				intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
		Assets (e.g., data, hardware, software, systems, facilities, services,		intersects with	Defined Roles &	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
ID.AM	N/A	people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Functional	intersects with	Responsibilities  Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work.	5	
				intersects with	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
				intersects with	Physical & Environmental	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
					Protections		Mechanisms exist to categorize Technology Assets, Applications, Services and/or		
				intersects with	Risk-Based Security Categorization	RSK-02	Data (TASD) in accordance with applicable laws, regulations and contractual obligations that:  (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and  (2) Ensure the security categorization decision is reviewed and approved by the	5	
				intersects with	Third-Party Management	TPM-01	asset owner.  Mechanisms exist to facilitate the implementation of third-party management controls.	5	
				intersects with	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPe) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CLS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
				intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	
				intersects with	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
ID.AM-01	N/A	Inventories of hardware managed by the organization are maintained.	Functional	subset of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (IAASD) in use; (1) Accurately reflects the current TAASD in use; (2) identifies authorized software products, including business justification details; (3) is a 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 organizations) personnel.	10	
				intersects with	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TIASD).	5	
ID.AM-02	N/A	Inventories of software, services, and systems managed by the organization are maintained.	Functional	subset of	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.	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 (optional)	Notes (optional)
				intersects with	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPa) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
		Representations of the organization's authorized network		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/regulated data flows.	5	
ID.AM-03	N/A	communication and internal and external network data flows are maintained.	Functional	intersects with	Control Applicability Boundary Graphical Representation	AST-04.2	Mechanisms exist to ensure control applicability is appropriately-determined for Technology Assets, Applications and/or Services (TAAS) and third parties by graphically representing applicable boundaries.	5	
				intersects with	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	5	
ID.AM-04	N/A	Inventories of services provided by suppliers are maintained.	Functional	equal	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10	
				intersects with	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity and data protection 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).	5	
ID.AM-05	N/A	Assets are prioritized based on classification, criticality, resources, and impact on the mission.	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.	5	
				intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.  Mechanisms exist to identify, prioritize and assess suppliers and partners of	5	
				intersects with	Third-Party Criticality Assessments	TPM-02	rechainsms exist to identify, prioritize and assess suppliers and partners or 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.	5	
				intersects with	Media Storage	DCH-06	Universe or Ingervature services.  Michanisms sold sold in an securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using sapproved equipment, schniques and procedures.	5	
				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	
				intersects with	Periodic Scans for Sensitive / Regulated Data	DCH-06.3	Mechanisms exist to periodically scan unstructured data sources for sensitive/regulated data or data requiring special protection measures by	5	
ID.AM-07	N/A	Inventories of data and corresponding metadata for designated data types are maintained.	Functional	intersects with	Personal Data (PD) Retention & Disposal	PRI-05	statutory, regulator or contractual obligations.  (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to Idlit the purposely identified in the notice or as required by low;  (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and  (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
				intersects with	Inventory of Personal	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store,	5	
				subset of	Data (PD) Asset Governance	AST-01	transmit. update and/or share Personal Data (PD). Mechanisms exist to facilitate an IT Asset Management (ITAM) program to	10	
				intersects with	Stakeholder Identification &	AST-01.2	implement and manage asset management controls.  Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the	5	
					Involvement  Data Protection	DCH-01	ongoing secure management of those assets.  Mechanisms exist to facilitate the implementation of data protection controls.		
ID.AM-08	N/A Systems, hardware, software, services, and data are managed throughout their life cycles.	Functional	intersects with	Data Protection  Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and	5		
			intersects with	Secure Development Life Cycle (SDLC)	PRM-07	communicated.  Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled	5		
			intersects with	Management Predictable Failure	SEA-07	through formal change control procedures.  Mechanisms exist to determine the Mean Time to Failure (MTTF) for system	5		
				intersects with	Analysis Technology Lifecycle	SEA-07.1	components in specific environments of operation.  Mechanisms exist to manage the usable lifecycles of technology assets.	5	
				subset of	Management Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.  Mechanisms exist to coordinate cybersecurity, data protection and business	10	
				intersects with	Steering Committee & Program Oversight	GOV-01.1	alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
ID.RA	N/A	The cybersecurity risk to the organization, assets, and individuals is understood by the organization.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation Risk Management	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.  Mechanisms exist to facilitate the implementation of strategic, operational and	5	
				intersects with	Program Program	RSK-01	rechanisms exist to racinitate the implementation of strategic, operational and tactical risk management controls.  Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM)	5	
				intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	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.	5	
				intersects with	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.  Mechanisms exist to formally assess the cybersecurity and data protection	5	
				intersects with	Assessments	IAO-02	controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extant to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
				intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or declicincies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities. Mechanisms exist to conduct recurring assessments of risk that includes the	5	
ID.RA-01	N/A	Vulnerabilities in assets are identified, validated, and recorded.	Functional	intersects with	Risk Assessment	RSK-04	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).  Mechanisms exist to maintain a risk register that facilitates monitoring and	5	
				intersects with	Risk Register	RSK-04.1	reporting of risks.  Mechanisms exist to require system developers/integrators consult with	5	
					Cybersecurity & Data		cybersecurity and data protection personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar		
				intersects with	Protection Testing Throughout Development	TDA-09	capability.  [2] Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	
				subset of	Vulnerability & Patch Management Program	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
				intersects with	(VPMP) Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
							vunnerability scanning of systems and applications.  Mechanisms exist to establish contact with selected groups and associations within the cybersecurity and data protection communities to:		
ID.RA-02	N/A	Cyber threat intelligence is received from information sharing forums and sources.	Functional	intersects with	Contacts With Groups & Associations	GOV-07	(1) Facilitate ongoing cybersecurity and data protection education and training for organizational personnel; (2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and (3) Share currency bersecurity and/of data privacy-related information including	5	
					Threat Intelligence Feeds		threats, vulnerabilities and incidents. Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and		
				intersects with	Feeds	THR-03	threats by severaging the knowledge of attacker factics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	



FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
				subset of	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
				intersects with	Indicators of Exposure (IOE)	THR-02	Mechanisms exist to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.  Mechanisms exist to maintain situational awareness of vulnerabilities and evolving	5	
ID.RA-03	N/A	Internal and external threats to the organization are identified and	Functional	intersects with	Threat Intelligence Feeds Feeds	THR-03	threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
		recorded.		intersects with	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross- discipline insider threat incident handling team.	5	
				intersects with	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.  Mechanisms exist to perform cyber threat hunting that uses Indicators of	5	
				intersects with	Threat Hunting Threat Catalog	THR-07	Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.  Mechanisms exist to develop and keep current a catalog of applicable internal and	5	
ID RA-04	N/A	Potential impacts and likelihoods of threats exploiting vulnerabilities	Functional	intersects with	Threat Catalog	THR-09	external threats to the organization, both natural and manmade.  Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
15.104-04	IVA	are identified and recorded.	runcuonat	intersects with	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats. Mechanisms exist to identify:	5	
				intersects with	Risk Framing	RSK-01.1	(1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
				intersects with	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.  Mechanisms exist to conduct recurring assessments of risk that includes the	5	
		Threats, vulnerabilities, likelihoods, and impacts are used to		intersects with	Risk Assessment	RSK-04	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).	5	
ID.RA-05	N/A	understand inherent risk and inform risk response prioritization.	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. Mechanisms exist to remediate risks to an acceptable level.	5	
				intersects with	Risk Remediation	RSK-06	Mechanisms exist to respond to findings from cybersecurity and data protection	5	
				intersects with	Risk Response  Indicators of Exposure	RSK-06.1 THR-02	assessments, incidents and audits to ensure proper remediation has been performed.  Mechanisms exist to develop indicators of Exposure (IOE) to understand the	5	
				intersects with	(IOE) Threat Catalog	THR-02	potential attack vectors that attackers could use to attack the organization.  Mechanisms exist to develop and keep current a catalog of applicable internal and	5	
				intersects with	Threat Analysis	THR-10	external threats to the organization, both natural and manmade.  Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5	
				intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify:  (1) Assumptions affecting risk assessments, risk response and risk monitoring;  (2) Constraints affecting risk assessments, risk response and risk monitoring;  (3) The organizational risk tolerance; and  (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
ID.RA-06	N/A	Risk responses are chosen, prioritized, planned, tracked, and	Functional	intersects with	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	5	
		communicated.		intersects with	Risk Ranking	RSK-05 RSK-06	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices. Mechanisms exist to remediate risks to an acceptable level.	5	
			intersects with	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity and data protection assessments, incidents and audits to ensure proper remediation has been	5		
				intersects with	Compensating	RSK-06.2	performed.  Mechanisms exist to identify and implement compensating countermeasures to	5	
				subset of	Countermeasures Change Management Program	CHG-01	reduce risk and exposure to threats.  Mechanisms exist to facilitate the implementation of a change management program.	10	
				intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.  Mechanisms exist to prohibit unauthorized changes, unless organization-approved	5	
				intersects with	Prohibition Of Changes Test, Validate &	CHG-02.1	change requests are received.  Mechanisms exist to appropriately test and document proposed changes in a non-	5	
ID.RA-07	N/A	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked.	Functional	intersects with	Document Changes Security Impact Analysis	CHG-02.2	production environment before changes are implemented in a production environment.  Mechanisms exist to analyze proposed changes for potential security impacts,	5	
				intersects with	for Changes Access Restriction For	CHG-03 CHG-04	prior to the implementation of the change.  Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
				intersects with	Change Exception Management	GOV-02.1	soming of users to conduct unanomored cranges.  Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	5	
				intersects with	Threat Intelligence Feeds	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross organization information-sharing capability that can influence the development of	5	
					Program  Indicators of Exposure		the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.  Mechanisms exist to develop indicators of Exposure (IOE) to understand the		
				intersects with	(IOE)	THR-02	potential attack vectors that attackers could use to attack the organization. Mechanisms exist to maintain situational awareness of vulnerabilities and evolving	5	
ID.RA-08	N/A	Processes for receiving, analyzing, and responding to vulnerability disclosures are established.	Functional	intersects with	Threat Intelligence Feeds Feeds	THR-03	threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
				intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
				intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.  Mechanisms exist to identify and assign a risk ranking to newly discovered security	5	
				intersects with	Vulnerability Ranking	VPM-03	vulnerabilities using reputable outside sources for security vulnerability information.	5	
				intersects with	Logical Tampering Protection	AST-15	Mechanisms exist to verify logical configuration settings and the physical integrity of critical technology assets throughout their lifecycle.  Mechanisms exist to provision and protect the confidentiality, integrity and	5	
				intersects with	Roots of Trust Protection Technology	AST-18	authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification.  Mechanisms exist to facilitate the implementation of tailored development and	5	
				intersects with	Development & Acquisition	TDA-01	acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
ID.RA-09	N/A	The authenticity and integrity of hardware and software are assessed prior to acquisition and use.	Functional	intersects with	Integrity Mechanisms for Software / Firmware Updates	TDA-01.2	Mechanisms exist to utilize integrity validation mechanisms for security updates.	5	
				intersects with	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	5	
				intersects with	Software / Firmware Integrity Verification	TDA-14.1	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware	5	
				intersects with	Hardware Integrity Verification	TDA-14.2	components.  Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of hardware components.	5	
				intersects with	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets,	5	
ID.RA-10	N/A	Critical suppliers are assessed prior to acquisition.	Functional	intersects with	Third-Party Criticality Assessments	TPM-02	Applications, Services and/or Data (TAASD).  Mechanisms exist to identity, 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.	5	
				intersects with	Third-Party Risk Assessments &	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or	5	
				intersects with	Approvals Operations Security	OPS-01	Services (TAAS).  Mechanisms exist to facilitate the implementation of operational security controls.	5	
			l		, , ,				



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (ontional)	Notes (optional)									
				intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	(,	(optional) 5										
ID.IM	N/A	Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions.	Functional	subset of	Risk Management Program	RSK-01	assigned tasks.  Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10										
		Fullctions.			Supply Chain Risk		Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of											
				intersects with	Management (SCRM) Plan	RSK-09	Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5										
				intersects with	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection	5										
				intersects with	Functional Review Of Cybersecurity & Data	CPL-03.2	policies, standards and other applicable requirements.  Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity and data protection policies and standards.	5										
					Protection Controls		Mechanisms exist to formally assess the cybersecurity and data protection											
				intersects with	Assessments	IAO-02	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	5										
							desired outcome with respect to meeting expected requirements.  Mechanisms exist to produce a Security Assessment Report (SAR) at the											
				intersects with	Security Assessment Report (SAR)	IAO-02.4	conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	5										
				intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or	5										
ID.IM-01	N/A	Improvements are identified from evaluations.	Functional				eliminate known vulnerabilities.  Mechanisms exist to require system developers/integrators consult with cybersecurity and data protection personnel to:											
					Cybersecurity & Data Protection Testing		<ol> <li>Create and implement a Security Testing and Evaluation (ST&amp;E) plan, or similar capability;</li> </ol>											
				intersects with	Throughout Development	TDA-09	(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation	5										
							processes.  Mechanisms exist to require the developers of Technology Assets, Applications											
				intersects with	Continuous Monitoring Plan Third-Party Risk	TDA-09.1	and/or Services (TAAS) to produce a plan for the continuous monitoring of cybersecurity and data protection control effectiveness.	5										
				intersects with	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).	5										
				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 cybersecurity and data protection controls.	5										
				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.	5										
				intersects with	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection	5										
				intersects with	Functional Review Of Cybersecurity & Data	CPL-03.2	policies, standards and other applicable requirements.  Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity and data protection policies and standards.	5										
					Protection Controls		Mechanisms exist to formally assess the cybersecurity and data protection											
				intersects with	Assessments	IAO-02	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	5										
							desired outcome with respect to meeting expected requirements.  Mechanisms exist to produce a Security Assessment Report (SAR) at the											
				intersects with	Security Assessment Report (SAR)	IAO-02.4	conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	5										
		Improvements are identified from security tests and exercises,		intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or	5										
ID.IM-02	N/A	including those done in coordination with suppliers and relevant third parties.	Functional	intersects with	Root Cause Analysis	IRO-13	eliminate known vulnerabilities.  Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of	5										
						(RCA) & Lessons Learned		future incidents.  Mechanisms exist to require system developers/integrators consult with cybersecurity and data protection personnel to:										
												intersects with	Cybersecurity & Data Protection Testing		(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;			
																		intersects with
										processes.  Mechanisms exist to require the developers of Technology Assets, Applications								
				intersects with	Continuous Monitoring Plan Third-Party Risk	TDA-09.1	and/or Services (TAAS) to produce a plan for the continuous monitoring of cybersecurity and data protection control effectiveness.	5										
				intersects with	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).	5										
				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 cybersecurity and data protection controls.	5										
				intersects with	Measures of Performance Contingency Plan Root	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5										
ID.IM-03	N/A	Improvements are identified from execution of operational processes, procedures, and activities.	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.	5										
				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.	5										
				intersects with	Business Continuity Management System	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 &	5										
		Incident response plans and other cybersecurity plans that affect		latara ( 6)	(BCMS) Ongoing Contingency	noc -:	Disaster Recovery (BC/DR) playbooks).  Mechanisms exist to update contingency plans due to changes affecting:	_										
ID.IM-04	N/A	operations are established, communicated, maintained, and improved.	Functional	intersects with	Planning Incident Response Plan	BCD-06	(1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including Mechanisms exist to maintain and make available a current and viable incident	5										
				intersects with	(IRP)	IRO-04	Response Plan (IRP) to all stakeholders.  Mechanisms exist to regularly review and modify incident response practices to	5										
				intersects with	IRP Update	IRO-04.2	incorporate lessons learned, business process changes and industry developments, as necessary.	5										
				subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10										
				intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on	5										
PR	N/A	Safeguards to manage the organization's cybersecurity risks are used.	Functional	intersects with	Statutory, Regulatory &	CPL-01	a regular basis.  Mechanisms exist to facilitate the identification and implementation of relevant	5										
	IV/A	Suregumes to manage the organization is cybersecurity fisks are used.	runctionat	intersects with	Contractual Compliance Risk Management	CPL-01	statutory, regulatory and contractual controls.  Mechanisms exist to facilitate the implementation of strategic, operational and	5										
				wood will	Program Supply Chain Risk		tactical risk management controls.  Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of											
				intersects with	Management (SCRM) Plan	RSK-09	Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5										
				intersects with	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5										
				intersects with	Authenticate, Authorize	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service	5										
		I	l		and Audit (AAA)		Provider (ESP).											



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
PR.AA	N/A	Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the	Functional	intersects with	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
		assessed risk of unauthorized access.		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	5	
							the facility officially designated as publicly accessible).  Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit		
				intersects with	Physical Access Control	PES-03	points) to facilities (excluding those areas within the facility officially designated as publicly accessible).  Mechanisms exist to uniquely identify and centrally Authenticate. Authorize and	5	
				intersects with	Authentication for Organizational Users	IAC-02	Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
				intersects with	Identification & Authentication for Non- Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5	
PR.AA-01	N/A	Identities and credentials for authorized users, services, and hardware are managed by the organization.	Functional	intersects with	Identification & Authentication for	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional	5	
					Devices Identification & Authentication for Third-		authentication that is cryptographically- based and replay resistant.  Mechanisms exist to identify and authenticate third-party Technology Assets,  Applications and/or Services (TAAS).		
				intersects with	Party Technology Assets, Applications and/or Services (TAAS)	IAC-05		5	
PR.AA-02	N/A	Identities are proofed and bound to credentials based on the context of interactions.	Functional	equal	Identity Proofing (Identity Verification)	IAC-28	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.	10	
				subset of	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	10	
				intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
				intersects with	Identification & Authentication for Non-	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the	5	
PR.AA-03	N/A	Users, services, and hardware are authenticated.	Functional	intersects with	Organizational Users Identification & Authentication for	IAC-04	organization.  Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional	5	
					Devices Identification & Authentication for Third-		authentication that is cryotographically-based and replay resistant.  Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).		
				intersects with	Party Technology Assets, Applications and/or	IAC-05	repriorition dilutal Statutes (IPPo).	5	
				intersects with	Services (TAAS)  Authenticate, Authorize	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service	5	
PR.AA-04	N/A	Identity assertions are protected, conveyed, and verified.	Functional	intersects with	and Audit (AAA) Replay-Resistant	IAC-02.2	Provider (ESP). Automated mechanisms exist to employ replay-resistant authentication.	5	
				intersects with	Authentication  Acceptance of External Authenticators	IAC-03.5	Mechanisms exist to restrict the use of external authenticators to those that are National Institute of Standards and Technology (NIST)-compliant and maintain a	5	
				intersects with	Position Categorization	HRS-02	list of accepted external authenticators.  Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling	5	
					Separation of Duties		those positions.  Mechanisms exist to implement and maintain Separation of Duties (SoD) to		
				intersects with	(SoD)	HRS-11	prevent potential inappropriate activity without collusion.  Mechanisms exist to facilitate the implementation of identification and access	5	
				subset of	Identity & Access Management (IAM)	IAC-01	management controls.  Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit	10	
				intersects with	Authenticate, Authorize and Audit (AAA)	IAC-01.2	(AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
				intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
PR.AA-05	N/A	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.	Functional	intersects with	Identification & Authentication for Non- Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the	5	
				intersects with	Identification & Authentication for	IAC-04	organization.  Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional	5	
					Devices Identification & Authentication for Third-		authentication that is cryptographically-based and replay resistant.  Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).		
				intersects with	Party Technology Assets, Applications and/or Services (TAAS)	IAC-05		5	
				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	5	
				intersects with	Least Privilege	IAC-21	individuals assigned specific roles with legitimate business needs.  Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with	5	
				subset of	Physical & Environmental	PES-01	organizational business functions.  Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
					Protections  Physical Access		Physical access control mechanisms exist to maintain a current list of personnel		
PR.AA-06	N/A	Physical access to assets is managed, monitored, and enforced commensurate with risk.	Functional	intersects with	Authorizations  Role-Based Physical	PES-02	with authorized access to organizational facilities (except for those areas within the facility officially designated as <u>oublicly accessible</u> ).  Physical access control mechanisms exist to authorize physical access to	5	
		*****		intersects with	Access	PES-02.1	facilities based on the position or role of the individual.  Physical access control mechanisms exist to enforce physical access	5	
				intersects with	Physical Access Control	PES-03	authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
				subset of	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
20.47	N/4	The organization's personnel are provided with cybersecurity	Europia :	intersects with	Cybersecurity & Data Protection Awareness	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
PR.AT	N/A	awareness and training so that they can perform their cybersecurity- related tasks.	Functional		Training Role-Based		Mechanisms exist to provide role-based cybersecurity and data protection-related training:		
				intersects with	Cybersecurity & Data Protection Training	SAT-03	Before authorizing access to the system or performing assigned duties;     When required by system changes; and     Annually thereafter.	5	
				intersects with	Cybersecurity & Data Protection Awareness	SAT-02	(3) Annuativ thereafter.  Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
		Personnel are provided with awareness and training so that they			Training Role-Based		Mechanisms exist to provide role-based cybersecurity and data protection-related training:		
PR.AT-01	N/A	possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.	Functional	intersects with	Cybersecurity & Data Protection Training	SAT-03	(1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and	5	
				intersects with	Cyber Threat Environment	SAT-03.6	(3) Annually thereafter.  Mechanisms exist to provide role-based cybersecurity and data protection awareness training that is current and relevant to the cyber threats that users	5	
					Role-Based		might encounter in day-to-day business operations.  Mechanisms exist to provide role-based cybersecurity and data protection-related training:		
				intersects with	Cybersecurity & Data Protection Training	SAT-03	(1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and	5	
		Individuals in specialized roles are provided with awareness and		intersects with	Privileged Users	SAT-03.5	(3) Annually thereafter.  Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities	5	
PR.AT-02	N/A	training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind.	Functional	intersects with	Cyber Threat	SAT-02 C	Mechanisms exist to provide role-based cybersecurity and data protection awareness training that is current and relevant to the cyber threats that users	5	
				c.sects with	Environment  Continuing Professional	un1-03.6	might encounter in day-to-day business operations.  Mechanisms exist to ensure cybersecurity and data protection personnel receive	,	
				intersects with	Education (CPE) - Cybersecurity & Data Protection Personnel	SAT-03.7	Continuing Professional Education (CPE) training to maintain currency and proficiency with industry-recognized secure practices that are pertinent to their assigned roles and responsibilities.	5	
				subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
		I	i .		1	1		1	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
				intersects with	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	
				intersects with	Sensitive / Regulated	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
		Data are managed consistent with the organization's risk strategy to		intersects with	Data Protection Sensitive / Regulated	DOLLOS O	Mechanisms exist to ensure media records for sensitive/regulated data contain	5	
PR.DS	N/A	protect the confidentiality, integrity, and availability of information.	Functional	intersects with	Media Records  Defining Access	DCI1-01.3	sufficient information to determine the potential impact in the event of a data loss incident.  Mechanisms exist to explicitly define authorizations for specific individuals and/or		
				intersects with	Authorizations for Sensitive/Regulated Data	DCH-01.4	roles for logical and /or physical access to sensitive/regulated data.	5	
				intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
				intersects with	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
				subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
		The confidentiality, integrity, and availability of data-at-rest are		intersects with	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
PR.DS-01	N/A	protected.	Functional	intersects with	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards.	5	
				intersects with	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
				subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.  Mechanisms exist to facilitate the implementation of cryptographic protections	10	
PR.DS-02	N/A	The confidentiality, integrity, and availability of data-in-transit are protected.	Functional	intersects with	Use of Cryptographic Controls	CRY-01	controls using known public standards and trusted cryptographic technologies.	5	
				intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.  Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
				intersects with	Transmission Integrity  Data Protection	CRY-04 DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
				intersects with	Use of Cryptographic	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
PR.DS-10	N/A	The confidentiality, integrity, and availability of data-in-use are protected.	Functional		Controls Secure Baseline		Mechanisms exist to develop, document and maintain secure baseline		
		,		intersects with	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. Mechanisms exist to utilize the concept of least privilege, allowing only authorized	5	
				intersects with	Least Privilege	IAC-21	access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
				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	5	
				intersects with	Testing for Reliability &	BCD-11.1	(RPOs).  Mechanisms exist to routinely test backups that verify the reliability of the backup	5	
PR.DS-11	N/A	Backups of data are created, protected, maintained, and tested.	Functional	intersects with	Integrity Test Restoration Using Sampling	BCD-11.5	process, as well as the integrity and availability of the data.  Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	5	
				intersects with	Transfer to Alternate Storage Site	BCD-11.6	Capationices as part of business continuity plan results; Mechanisms exist to transfer backup data to the alternate storage site at a rate that is capable of meeting both Recovery Time Objectives (RTOs) and Recovery	5	
					Configuration		Point Objectives (RPOs).  Mechanisms exist to facilitate the implementation of configuration management controls.		
				intersects with	Management Program	CFG-01	controls.	5	
				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.	5	
		The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are		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	5	
PR.PS	N/A	managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability.	Functional	intersects with	Configure Technology Assets, Applications and/or Services (TAAS)	CFG-02.5	(3) As oart of system component installations and upgrades. Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	
				intersects with	for High-Risk Areas  Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	5	
							Mechanisms exist to conduct controlled maintenance activities throughout the		
				intersects with	Controlled Maintenance	MNT-02	lifecycle of the system, application or service.	5	
PR.PS-01	N/A	Configuration management practices are established and applied.	Functional	equal	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
				intersects with	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise. Mechanisms exist to conduct controlled maintenance activities throughout the	5	
				intersects with	Controlled Maintenance	MNT-02	lifecycle of the system, application or service.  Mechanisms exist to obtain maintenance support and/or spare parts for	5	
				intersects with	Timely Maintenance  Preventative	MNT-03.1	Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).  Mechanisms exist to perform preventive maintenance on critical Technology	5	
					Maintenance Secure Development Life		Assets, Applications and/or Services (TAAS).  Mechanisms exist to ensure changes to Technology Assets, Applications and/or	-	
				intersects with	Cycle (SDLC)  Management  Technology Lifecycle	PRM-07	Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.  Mechanisms exist to manage the usable lifecycles of technology assets.	5	
PR.PS-02	N/A	Software is maintained, replaced, and removed commensurate with risk.	Functional	intersects with	Management	SEA-07.1	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or	5	
				intersects with	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Services (TAAS) by:  (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of	5	
				intersects with	Vulnerability & Patch Management Program	VPM-01	unsupported TAAS required to satisfy mission/business needs.  Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
				intersects with	(VPMP) Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface	5	
	PR.PS-03 N/A Hardware is maintained, replaced, and removed commensurate with risk.		intersects with	Vulnerability Remediation Process	VPM-02	management activities.  Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		
			intersects with	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		
			intersects with	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise. Mechanisms exist to conduct controlled maintenance activities throughout the	5		
			intersects with	Controlled Maintenance	MNT-02	lifecycle of the system, application or service.  Mechanisms exist to obtain maintenance support and/or spare parts for	5		
				intersects with	Timely Maintenance  Preventative	MNT-03	Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).  Mechanisms exist to perform preventive maintenance on critical Technology	5	
PR.PS-03			Functional	intersects with	Maintenance Secure Development Life	MNT-03.1	Assets, Applications and/or Services (TAAS).  Mechanisms exist to ensure changes to Technology Assets, Applications and/or	5	
			intersects with	Cycle (SDLC)  Management  Technology Lifecycle	PRM-07	Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.  Mechanisms exist to manage the usable lifecycles of technology assets.	5		
			intersects with	Management	SEA-07.1	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or	5		
			intersects with	Unsupported Technology Assets, Applications	TDA-17	Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and	5		
					and/or Services (TAAS)		(2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.		



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (ontional)	Notes (optional)
				subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	(optional)	
				intersects with	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve	5	
							integrated situational awareness.  Mechanisms exist to configure Technology Assets, Applications and/or Services		
PR.PS-04	N/A	Log records are generated and made available for continuous monitoring.	Functional				(TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred;		
				intersects with	Content of Event Logs	MON-03	(2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event;	5	
							(5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.		
				intersects with	Configuration	CFG-01	Mechanisms exist to facilitate the implementation of configuration management	5	
				intersects with	Management Program Secure Baseline	CFG-02	controls.  Mechanisms exist to develop, document and maintain secure baseline	5	
				intersects with	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. Mechanisms exist to configure systems to provide only essential capabilities by	5	
PR.PS-05	N/A	Installation and execution of unauthorized software are prevented.	Functional	intersects with	Least Functionality	CFG-03	specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
				intersects with	Prevent Unauthorized Software Execution	CFG-03.2	Mechanisms exist to configure systems to prevent the execution of unauthorized software programs.	5	
				intersects with	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software. Automated mechanisms exist to prohibit software installations without explicitly	5	
				intersects with	Prohibit Installation Without Privileged Status	END-03	assigned privileged status.	5	
				intersects with	Technology Development &	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique	5	
					Acquisition		business needs.  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:		
				intersects with	Product Management	TDA-01.1	(1) Improve functionality; (2) Enhance security and resiliency capabilities;	5	
							(3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.		
				intersects with	Secure Software	TDA-06	Mechanisms exist to develop applications based on Secure Software Development	5	
		Secure software development practices are integrated, and their		antersects with	Development Practices (SSDP)	1DA-06	Practices (SSDP).  Mechanisms exist to require the developer of the system, system component or		
PR.PS-06	N/A	performance is monitored throughout the software development life cycle.	Functional	intersects with	Criticality Analysis	TDA-06.1	service to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	
				intersects with	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and	5	
				intersects with	Software Assurance	TDA-06 3	accounted for.  Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets,	5	
				III.CI GOOG WILL	Maturity Model (SAMM)	15/1 00.0	Applications and/or Services (TAAS).  Mechanisms exist to require system developers/integrators consult with		
					Cybersecurity & Data		cybersecurity and data protection personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar		
				intersects with	Protection Testing Throughout	TDA-09	capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and	5	
					Development		deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation		
					Cybersecurity & Data		processes.  Mechanisms exist to facilitate the implementation of cybersecurity and data		
			subset of	Protection Governance Program	GOV-01	protection governance controls.	10		
			intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on	5		
							cybersecurity, data privacy and business executives, which meets formally and on a regular basis.  Mechanisms exist to facilitate the implementation of strategic, operational and		
				intersects with	Risk Management Program	RSK-01	tactical risk management controls.	5	
PR.IR	N/A	Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and	Functional	subset of	Secure Engineering	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design,	10	
FR.IN	IVA	organizational resilience.	runctional		Principles		development, implementation and modification of Technology Assets, Applications and/or Services (TAAS). Mechanisms exist to centrally-manage the organization-wide management and		
				intersects with	Centralized Management of Cybersecurity & Data Protection Controls	SEA-01.1	implementation of cybersecurity and data protection controls and related processes.	5	
				intersects with	Achieving Resilience	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse	5	
				intersects with	Requirements	SEA-01.2	situations.  Mechanisms exist to develop an enterprise architecture, aligned with industry-	5	
				intersects with	Alignment With Enterprise Architecture	SEA-02	recognized leading practices, with consideration for cybersecurity and data protection principles that addresses risk to organizational operations, assets,	5	
				subset of	Network Security Controls (NSC)	NET-01	individuals, other organizations.  Mechanisms exist to develop, govern & update procedures to facilitate the	10	
					Controls (NSC)  Layered Network		implementation of Network Security Controls (NSC).  Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence		
				intersects with	Defenses	NET-02	by lower layers on the functionality or correctness of higher layers.	5	
PR.IR-01	N/A	Networks and environments are protected from unauthorized logical access and usage.	Functional	intersects with	Secure Engineering	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design,	5	
					Principles		development, implementation and modification of Technology Assets, Applications and/or Services (TAAS). Mechanisms exist to develop an enterprise architecture, aligned with industry-		
				intersects with	Alignment With Enterprise Architecture	SEA-02	recognized leading practices, with consideration for cybersecurity and data protection principles that addresses risk to organizational operations, assets,	5	
					Business Continuity		individuals, other organizations.  Mechanisms exist to facilitate the implementation of contingency planning	-	
				intersects with	Management System (BCMS)	BCD-01	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).	5	
				subset of	Physical & Environmental Protections	PES-01	Disaster Recovery (CC/DN) playbooks).  Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
				intersects with	Protections  Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling	5	
PR.IR-02	N/A	The organization's technology assets are protected from	Functional	intersects with	Water Damage	PES-07.5	for the system from damage and destruction.  Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working	5	
		environmental threats.			Protection	7.20-07.5	water teakage by providing master shutch valves that are accessible, working property and known to key personnel.  Facility security mechanisms exist to utilize and maintain fire suppression and		
				intersects with	Fire Protection	PES-08	detection devices/systems for the system that are supported by an independent energy source.	5	
				intersects with	Temperature & Humidity Controls	PES-09	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.  Machanisms suits to achieve serilipses or pour months in permal and achieves.	5	
				intersects with	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.  Mechanisms exist to develop and keep current a catalog of applicable internal and	5	
				intersects with	Threat Catalog  Business Continuity	THR-09	external threats to the organization, both natural and manmade.  Mechanisms exist to facilitate the implementation of contingency planning	5	
				subset of	Management System (BCMS)	BCD-01	controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity &	10	
					Secure Engineering		Disaster Recovery (BC/DR) playbooks). Mechanisms exist to facilitate the implementation of industry-recognized		
PR.IR-03	N/A	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	Functional	intersects with	Principles	SEA-01	cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Apolications and/or Services (TAAS).	5	
				intersects with	Alignment With	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry- recognized leading practices, with consideration for cybersecurity and data	5	
				soots will	Enterprise Architecture	-27.02	protection principles that addresses risk to organizational operations, assets, individuals, other organizations.		



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
				intersects with	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	(optional) 5	
PR.IR-04				subset of	Capacity & Performance	CAP-01	situations.  Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated	10	
					Management		Tuture capacity requirements.  Mechanisms exist to control resource utilization of Technology Assets,		
				intersects with	Resource Priority	CAP-02	Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	
	N/A	Adequate resource capacity to ensure availability is maintained.	Functional	intersects with	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist	5	
							during contingency operations.  Automated mechanisms exist to centrally-monitor and alert on the operating state		
				intersects with	Performance Monitoring	CAP-04	and health status of critical Technology Assets, Applications and/or Services (TAAS).	5	
				intersects with	Elastic Expansion	CAP-05	Mechanisms exist to automatically scale the resources available for Technology Assets, Applications and/or Services (TAAS), as demand conditions change.	5	
							Mechanisms exist to implement a threat intelligence program that includes a cross		
			subset of	Threat Intelligence Feeds Program	THR-01	organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring,	10		
		Possible cybersecurity attacks and compromises are found and analyzed.	Functional	intersects with	Indicators of Exposure	THR-02	threat hunting, response and recovery activities.  Mechanisms exist to develop Indicators of Exposure (IOE) to understand the	5	
					(IOE)		potential attack vectors that attackers could use to attack the organization.  Mechanisms exist to maintain situational awareness of vulnerabilities and evolving		
DE	N/A			intersects with	Threat Intelligence Feeds Feeds	THR-03	threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating	5	
				intersects with	Threat Hunting	THR-07	controls.  Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security	5	
							controls.  Mechanisms exist to develop and keep current a catalog of applicable internal and		
				intersects with	Threat Catalog	THR-09	external threats to the organization, both natural and mammade.  Mechanisms exist to identify, assess, prioritize and document the potential	5	
				intersects with	Threat Analysis  Monitoring for Indicators	THR-10	impact(s) and likelihood(s) of applicable internal and external threats.  Automated mechanisms exist to identify and alert on Indicators of Compromise	5	
				intersects with	of Compromise (IOC)	MON-11.3	(IoC).  Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User	5	
DE.CM	N/A	Assets are monitored to find anomalies, indicators of compromise,	Functional	intersects with	Anomalous Behavior	MON-16	Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
DE.OH	INA	and other potentially adverse events.	, uncoonst	intersects with	Indicators of	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the	5	
				intersects with	Compromise (IOC) Indicators of Exposure	THR-02	signs of potential cybersecurity events. Mechanisms exist to develop Indicators of Exposure (IOE) to understand the	5	
				subset of	(IOE) Continuous Monitoring	MON-01	potential attack vectors that attackers could use to attack the organization.  Mechanisms exist to facilitate the implementation of enterprise-wide monitoring	10	
					Intrusion Detection &		controls.  Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS /		
			Functional	intersects with	Prevention Systems (IDS & IPS)	MON-01.1	IPS) technologies on critical systems, key network segments and network choke points.	5	
DE.CM-01	N/A	Networks and network services are monitored to find potentially adverse events.		intersects with	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	
				intersects with	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve	5	
				intersects with	Security Event Monitoring	MON-01.8	integrated situational awareness.  Mechanisms exist to review event logs on an ongoing basis and escalate incidents	5	
				intersects with	Physical & Environmental	PES-01	in accordance with established timelines and procedures.  Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
					Protections	. 23-01	protection controls.  Physical access control mechanisms exist to enforce physical access		
DE.CM-02	N/A	The physical environment is monitored to find potentially adverse events.	Functional	intersects with	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	5	
			ranctional				points) to lacenties (excluding those areas within the facility officially designated as publicly accessible).  Physical access control mechanisms generate a log entry for each access attempt		
			intersects with	Physical Access Logs Monitoring Physical	PES-03.3	through controlled ingress and egress points.  Physical access control mechanisms exist to monitor for, detect and respond to	5		
			-	intersects with	Access	PES-05 MON-01	physical security incidents.  Mechanisms exist to facilitate the implementation of enterprise-wide monitoring	5	
			Functional	intersects with	Continuous Monitoring	MON-01	controls.  Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User	5	
				intersects with	Anomalous Behavior	MON-16	Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
DE.CM-03	N/A	Personnel activity and technology usage are monitored to find		intercepts with	Incider Threats	MON 16 1	Mechanisms exist to monitor internal personnel activity for potential security	5	
JE.GP-03	INA	potentially adverse events.	, uncoonst	intersects with	Insider Threats Unauthorized Activities	MON-16.1	incidents.  Mechanisms exist to monitor for unauthorized activities, accounts, connections,	5	
					STRUCTURES ACTIVITIES	. 1014-10.3	devices and software.  Mechanisms exist to force Internet-bound network traffic through a proxy device		
				intersects with	DNS & Content Filtering	NET-18	(e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
				intersects with	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring	5	
DE.CM-06	N/A	External service provider activities and services are monitored to find	Functional	intersects with	Third-Party Threats	MON-16.2	controls.  Mechanisms exist to monitor third-party personnel activity for potential security	5	
		potentially adverse events.		intersects with	Account Creation and	MON-16.4	incidents. Automated mechanisms exist to generate event logs for permissions changes to	5	
				intersects with	Modification Logging  Continuous Monitoring	MON-01	privileged accounts and/or groups.  Mechanisms exist to facilitate the implementation of enterprise-wide monitoring	5	
					File Integrity Monitoring		controls.  Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-		
				intersects with	(FIM) Enterprise Device	MUN-01.7	detection technology, on critical assets to generate alerts for unauthorized modifications.  Mechanisms exist to facilitate the implementation of Enterprise Device	5	
DE.CM-09	N/A	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events.	Functional	intersects with	Enterprise Device Management (EDM) Malicious Code	END-01	Mechanisms exist to facilitate the implementation of Enterprise Device  Management (EDM) controls.  Mechanisms exist to utilize antimalware technologies to detect and eradicate	5	
				intersects with	Protection (Anti- Malware)	END-04	maticious code.	5	
				intersects with	Endpoint File Integrity	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration	5	
					Monitoring (FIM)		settings.  Mechanisms exist to facilitate the implementation of enterprise-wide monitoring		
				intersects with	Continuous Monitoring	MON-01	controls.	5	
	N/A	Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect	Functional	intersects with	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
						MON-	Mechanisms exist to automatically alert incident response personnel to		
				intersects with	Automated Alerts	01.12	inappropriate or anomalous activities that have potential security incident implications.	5	
DE.AE				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	10	
		cybersecurity incidents.					protection-related incidents. Mechanisms exist to cover:		
					tooldest '' '''	IDC	(1) Preparation; (2) Automated event detection or manual incident report intake;	_	
				intersects with	Incident Handling	IRO-02	(3) Analysis; (4) Containment;	5	
							(5) Eradication; and (6) Recovery.		
				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.	5	
							Mechanisms exist to cover:		
DE.AE-02	N/A	Potentially adverse events are analyzed to better understand associated activities.	Functional	intersects with	Incident Handling	IRO-02	(1) Preparation; (2) Automated event detection or manual incident report intake; (3) Another in the control of	5	
					aencriandung	0-02	(3) Analysis; (4) Containment; (5) Eradication; and		
					Incident Classification &		(s) Eradication; and (6) Recovery. Mechanisms exist to identify classes of incidents and actions to take to ensure the		
				intersects with	Prioritization	IRO-02.4	continuation of organizational missions and business functions.  Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar	5	
				intersects with	Centralized Collection of Security Event Logs	MON-02	automated tool, to support the centralized collection of security-related event logs.	8	
		1	1		1		Man.		



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
				intersects with	Correlate Monitoring	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM)	10	
					Information		or similar automated tool, to enhance organization-wide situational awareness.		
DE.AE-03	N/A	Information is correlated from multiple sources.	Functional				Mechanisms exist to cover: (1) Preparation;		
				intersects with	Incident Handling	IRO-02	(2) Automated event detection or manual incident report intake;     (3) Analysis;     (4) Containment;	3	
							(6) Eradication; and (6) Recovery.		
				intersects with	Correlation with External Organizations	IRO-02.5	Mechanisms exist to coordinate with approved third-parties to achieve a cross- organization perspective on incident awareness and more effective incident	5	
					Organizations		responses. Mechanisms exist to cover:		
	N/A	The estimated impact and scope of adverse events are understood.	Functional	intersects with	Incident Handling	IRO-02	(1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis:	5	
DE.AE-04					incident Handling	INO-02	(4) Containment; (5) Eradication; and	3	
				intersects with	Incident Classification &	IRO-02.4	(6) Recovery.  Mechanisms exist to identify classes of incidents and actions to take to ensure the	5	
				intersects with	Prioritization  Materiality Determination	GOV-16	continuation of organizational missions and business functions.  Mechanisms exist to define materiality threshold criteria capable of designating an	5	
				intersects with	Security Event Monitoring	MON-01.8	incident as material.  Mechanisms exist to review event logs on an ongoing basis and escalate incidents	5	
				intersects with	Automated Alerts	MON-	in accordance with established timelines and procedures.  Mechanisms exist to automatically slert incident response personnel to inappropriate or anomalous activities that have potential security incident	5	
					Centralized Collection of	01.12	implications.  Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar		
				intersects with	Security Event Logs	MON-02	automated tool, to support the centralized collection of security-related event logs.	5	
		<u>'</u>		intersects with	Correlate Monitoring	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM)	5	
					Information		or similar automated tool, to enhance organization-wide situational awareness.  Mechanisms exist to cover:		
			. Functional		Incident Handling		rechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake;		
DE.AE-06	N/A	Information on adverse events is provided to authorized staff and tools.		intersects with		IRO-02	(3) Analysis; (4) Containment;	5	
		·					(5) Eradication; and (6) Recovery.		
				intersects with	Incident Classification & Prioritization Incident Response Plan	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions. Mechanisms exist to maintain and make available a current and viable Incident	5	
				intersects with	(IRP) Integrated Security	IRO-04	Response Plan (IRP) to all stakeholders.  Mechanisms exist to establish an integrated team of cybersecurity, IT and	5	
				intersects with	Incident Response Team (ISIRT)	IRO-07	business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5	
				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	5	
					Incident Stakeholder		resolution of the incident.  Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders;		
				intersects with	Reporting	IRO-10	(2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
			Functional	subset of	Threat Intelligence Feeds	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross organization information-sharing capability that can influence the development of	10	
		Cyber threat intelligence and other contextual information are integrated into the analysis.			Program		the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.		
DE.AE-07	N/A			intersects with	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating	5	
				intersects with	Threat Analysis	THR-10	controls.  Mechanisms exist to identify, assess, prioritize and document the potential	5	
				intersects with	Intreat Anatysis	IHK-10	impact(s) and likelihood(s) of applicable internal and external threats.  Mechanisms exist to cover:	5	
		Incidents are declared when advense events meet the defined incident criteria.	Functional	intersects with	Incident Handling	IRO-02	(1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis;	5	
DE.AE-08	N/A				modern runding		(d) Containment; (5) Eradication; and	3	
				intersects with	Incident Classification &	IRO-02.4	(6) Recovery.  Mechanisms exist to identify classes of incidents and actions to take to ensure the	5	
		Actions regarding a detected cybersecurity incident are taken.		subset of	Prioritization Incident Response	IRO-01	continuation of organizational missions and business functions.  Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data	10	
	N/A			subset of	Operations	INO-01	facultate an organization-wide response capability for cybersecurity and data protection-related incidents.  Mechanisms exist to cover:	10	
				intersects with			(1) Preparation; (2) Automated event detection or manual incident report intake;		
					Incident Handling	IRO-02	(3) Analysis; (4) Containment;	5	
					Incident Response Plan		(5) Eradication; and (6) Recovery.		
RS				intersects with	(IRP) Integrated Security	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders. Mechanisms exist to establish an integrated team of cybersecurity, IT and	5	
				intersects with	Incident Response Team (ISIRT)	IRO-07	business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5	
				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.	5	
					Incident Stakeholder		resolution of the incident.  Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders;	_	
				intersects with	Reporting	IRO-10	(2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
							Mechanisms exist to cover: (1) Preparation;		
	N/A	Responses to detected cybersecurity incidents are managed.		intersects with	Incident Handling	IRO-02	(2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment:	5	
RS.MA			Functional				(4) Containment; (5) Eradication; and (6) Recoverv.		
				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.	5	
				intersects with	Integrated Security Incident Response Team	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity	5	
		The incident response plan is executed in coordination with relevant third parties once an incident is declared.	Functional		(ISIRT)		and data protection incident response operations.  Mechanisms exist to cover:  (1) Preparation:		
	N/A			intersects with	Incident Handling	IRO-02	(1) rreparation; (2) Automatted event detection or manual incident report intake; (3) Analysis;	5	
					som radiumg		(4) Containment; (5) Eradication; and		
				inter	Correlation with External	IDO CO C	(6) Recovery.  Mechanisms exist to coordinate with approved third-parties to achieve a cross-	-	
RS.MA-01				intersects with	Organizations Incident Response Plan	IRO-02.5	organization perspective on incident awareness and more effective incident responses.  Mechanisms exist to maintain and make available a current and viable Incident	5	
				intersects with	(IRP) Integrated Security	IRO-04	Response Plan (IRP) to all stakeholders.  Mechanisms exist to establish an integrated team of cybersecurity, IT and	5	
				intersects with	Incident Response Team (ISIRT)	IRO-07	business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5	
				intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and	5	
					neporung		(2) Affected clients & third-parties; and (3) Regulatory authorities.		



Rationale Relationship Screening Rationale (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (5) Recover.  Incident Response Plan IRO-04 (RP) Redaminance sets to maintain and make available a current and vine Response Plan IRO-04 (Response Plan IRO-04) Response Plan (IRP) to all stakeholders.	(optional)
RS.MA-02 N/A Incident reports are triaged and validated.  Functional Intersects with Incident Handling IRO-02 (3) Analysis: (4) Containment; (5) Endication; and (6) Recovery.  Incident Response Plan (IRP) and Intersects with Intersects with Intersects with Intersects with Incident Response Plan (IRP) to all stakeholders. Response Plan (IRP) to all stakeholders.	
Signal category   Signal cat	5
intersects with (IRP)   RC-04   Response Plan (IRP) to all stakeholders.	
12 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	5
RS.MA-03 N/A Incidents are categorized and prioritized. Functional equal Incident Classification & Prioritization   Incident Classification   Incident Classification   Incident Classification   Incident Classification   Incident Classificat	ake to ensure the 10
Mechanisms exist to cover: (1) Preparation: (2) Automated event detection or manual incident report intake;	
intersects with Incident Handling IRO-02 (3) Analysis; (4) Containment;	5
RS.MA-04 N/A Incidents are escalated or elevated as needed. Functional (5) Eradication; and (6) Recovery.	lights Insident
Intersects will   (RP)   Introduced   Response Plant (RP) to all stakeholders.   Integrated Security   Mechanisms exist to establish an integrated team of cybersecurity.	5
intersects with Incident Response Team IRO-07 business function representatives that are capable of addressing (ISIRT) and data protection incident response operations.	
Business Continuity intersects with  Business Continuity Management System (TAS) (e.g., Continuity of Operations Plan (COOP) or Business Co	and/or Services
RS.MA-05 NA The criteria for initiating incident recovery are applied. Functional (LOCPHS) Disaster Recovery (EC/DR) plut-phocks. Mechanisms wait to define spefic criteria necessary that must be	met to execute
intersects with intersects with Recovery Operations Criteria BCD-01.5 BcD-0	
(Into sign recovery Point Objectives (PPUs).  Mechanisms exist to cover:  (1) Preparation;  (1) Preparation;	
(2) Automated event detection or manual incident report intake; Incident Handling Irrestigations are conducted to ensure effective response and support	5
RS.AN N/A Investigations are conducted to ensure effective response and support forensics and recovery activities.  Functional (4) Containment; (5) Eradication; and (6) Recovery.	
Intersects with Chain of Custody & IRO-08 Intersects with Forensics IRO-08 Incomplete IRO-08 Intersects with Forensics IRO-08 IR	tegrity of the and industry- 5
PS AMPS N/A Analysis is performed to establish what has taken place during an Euroritinal equal Root Cause Analysis   19-13	and resolving
Incident and the root cause of the incident.    Purcuonal equal (RCA) & Lessons Learned   Incident   Purcuonal equal (RCA) & Lessons Learned   Purcuonal eq	oo or impose UI
(1) Preparation; (2) Automated event detection or manual incident report intake;	
intersects with Incident Handling IRO-02 (3) Analysis; (4) Containment; (5) Endication; and	5
RS.AN-06 N/A records integrity and provenance are preserved.  Functional (6) Recovery.  (6) Recovery.  (6) Recovery.	
intersects with Forensics III-U-U clargo of custory, in accentance with appreciate usws, regulations	
intersects with Situational Awareness For Incidents   For Incidents   For Incidents   For Incidents   For Incidents   For Incident   For Inci	
ncident data and metadata are collected, and their integrity and subsect of N/A s	
RS.AN-08 N/A An incident's magnitude is estimated and validated. Functional equal incident Classification & Prioritization Prioritization   Ho-02.4   Mechanisms exist to identify classes of incidents and actions to teach	ake to ensure the 10
Mechanisms exist to cover: (1) Preparation;	
intersects with Incident Handling (2) Automated event detection or manual incident report intake; IRO-02 (3) Analysis; IRO-02 (3) Containment;	5
(5) Endication; and (6) Recovery.	
intersects with  Correlation with External Organizations  Organizations  Re-0-12.5 Mechanisms exist to coordinate with approved third-parties to act provided the	hieve a cross- ve incident 5
intersects with Bedauting the Coordination with Related Plans (Fig. 2) in 100-06.1 (Mechanisms exist to coordinate incident response testing with or gleament responsible for related plans.	8
RS.CO N/A Response activities are coordinated with internal and external stakeholders are cupilations, or policies. Functional stakeholders are cupilations, or policies. Status of the status of t	
Reporting HKU-11 (2) Affected clients & third-parties; and (3) Regulatory exhibition.	5
intersects with Cyber Incident Reporting for Sensitive Data IRO-10.2	timely manner.
Mechanisms exist to provide cybersecurity and data protection in intersects with Supply Chain IRO-10.4 IRO-10.4	
Coordination (IAAS) and other organizations involved in the supply chain for IAA incident.	AS related to the
Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake;	
intersects with Incident Handling IRO-02 (3) Analysis; (4) Containment;	5
(5) Eradication; and (6) Recovery.  Mechanisms exist to timely-report incidents to applicable:	
RS.CO-02 N/A Internal and external stakeholders are notified of incidents. Functional intersects with Incident Stakeholder Reporting (1) Internal stakeholders; (2) Affected clients & third-parties; and	5
(3) Regulatory authorities.  Cyber Incident Reporting Intersects with Intersect with Intersects with Intersect	a timely manner.
for Sensitive Data  Mechanisms exist to provide cybersecurity and data protection in	cident
Supply Chain Coordination  Supply Chain Coordination  IRO-10.4  IR	
Mechanisms exist to cover: (1) Preparation;	
(2) Automated event detection or manual incident report intake; intersects with Incident Handling IRO-02 (3) Analysis;	5
(4) Containment; (5) Eradication; and (6) Recovery.	
BS COLORS N/A Information is shared with designated internal and external Functional Information is shared with designated internal and external Functional Information is shared with designated internal and external Functional Information is shared with designated internal and external Information is shared with the information in the information in the information is shared with the information in the inform	5
stakeholders. Reporting (2) Affected clients & third-parties; and (3) Regulatory authorities.	
intersects with Continue to the Continue to th	5
Mechanisms exist to provide cybersecurity and data protection in intersects with Coordination Coordination (TAXs) and other organizations involved in the supply chain for TAY	s and/or Services
incident Beasses Medianisms exist to implement and govern processes and docur	mentation to
intersects with Operations (IRO-01 (IR	ity and data 5
Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; Functional  Functional	
Its effects.  Its effects.  Incident Handling IRO-02 (3) Analysis; (4) Containment;	5
(5) Eradication; and (6) Recovery.	



RS.MI-01  N/A Incidents are contained.  Functional subset of Incident Handling Incident Handling Incident report intake;  (3) Analysis; (4) Containment; (5) Endication; and (6) Renower Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (6) Renower Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (6) Renower Mechanisms exist to cover: (1) Preparation; (2) Endication; and (6) Renower Mechanisms exist to cover: (1) Preparation; (2) Endication; and (6) Renower Mechanisms exist to cover: (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Endication; and (7) Renower Mechanisms exist to cover: (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Endication; and (7) Renower Mechanisms exist to cover: (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (7) Renower Mechanisms e	5 10 10 10 5 5
RS.MI-01  N/A Incidents are contained.  Functional subset of Incident Handling Incident Handling Incident report intake;  (3) Analysis; (4) Containment; (5) Endication; and (6) Renower Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (6) Renower Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (6) Renower Mechanisms exist to cover: (1) Preparation; (2) Endication; and (6) Renower Mechanisms exist to cover: (1) Preparation; (2) Endication; and (6) Renower Mechanisms exist to cover: (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Endication; and (7) Renower Mechanisms exist to cover: (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Endication; and (7) Renower Mechanisms exist to cover: (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (7) Renower Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Endication; and (7) Renower Mechanisms e	10
RS.MI-02 N/A Incidents are eradicated.  Functional subset of Incident Handling IRO-02 (3) Automated event detection or manual incident report intake; (4) Containment; (4) Containment; (5) Eradication; and (5) Feradication; and (6) Recovery.  Business Continuity Management System (BCD-01 (ASS) (e.g., Continuity of Operations Plan (COOP) of Business Continuity & Observed (COM) (17AS) (e.g., Continuity of Operations Plan (COOP) of Business Continuity & Observed (COM) (17AS) (e.g., Continuity of Operations Plan (COOP) of Business Continuity & Observed (COM) (17AS) (e.g., Continuity of Operations Plan (COOP) of Business Continuity & Observed (COM) (17AS) (e.g., Continuity of Operations Plan (COOP) of Business Continuity & Observed (COM) (17AS) (e.g., Continuity of Operations Plan (COOP) of Business Continuity & Observed (COOM) (17AS) (e.g., Continuity of Operations Plan (COOP) of Business Continuity & Observed (COOM) (17AS) (e.g., Continuity of Operations Plan (COOP) of Business Continuity & Observed (COOM) (17AS) (e.g., Continuity of Operations Plan (COOP) of Business Continuity & Observed (COOM) (17AS) (e.g., Continuity of Operations Plan (COOP) (17AS) (e.g., COOP) (17AS) (	10
Business Continuity subset of Management System (BCMS)  Management Sys	
Mechanisms exist to ensure the secure recovery and reconstitution of Jechnology I	5
restored.  Technology Assets, Applications and/or Applications and/or Services (TAAS) to a known state after a disruption, Assets, Applications and/or Services (TAAS) to a known state after a disruption, Services (TAAS) Recovery Assets, Applications and/or Services (TAAS) to a known state after a disruption, Compromise or failure.	
Business Continuity subset of Management System (BCMS)  Become Visual Page 1 Page 1 Page 1 Page 2 Pa	10
RC.RP N/A Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents.  Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents.  Functional intersects with Dejectives (RITO / RPO)  Mechanisms exist to identify and document the critical Technology Assets,	5
intersects with Identify Critical Assets BCD-02 Applications, Services and/or Data (TAASD) that support essential missions and business functions.  Machanisms update to narrow all missions and business functions.	5
Resume All Missions & Business Functions  Resume All Missions & Business Functions  Bu	5
Recovery Operations Criteria  The recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once  In the recovery portion of the incident response plan is executed once and the recovery portion of the incident response plan is executed once and	5
initiated from the incident response process.  Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, Services (TAAS) Recovery & Reconstitution  Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5
(BCMS) (BCMS) Disaster Recovery (BC/PD) playbooks).	10
NCA RECOVERY actions are selected, scoped, prioritized, and performed.    No   Compared to the control of the c	5
business functions.    intersects with   Resume All Missions & RCD21   Mechanisms exist to resume all missions and business functions within Recovery	5
intercontouith Backup & Restoration Backup & Restoration Backup & Restoration Backup & Mechanisms exist to protect backup and restoration hardware and software.	5
RC.RP-03 N/A The integrity of backups and other restoration assets is verified before using them for restoration.  The integrity of backups and other restoration assets is verified before using them for restoration.  Functional Functional Functional Verification Provided Functional Verification Provided Functional Provided F	5
Business Continuity  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning  Machanisms exist to facilitate the implementation of contingency planning	10
	5
Mechanisms exist to identify and document the critical Technology Assets, intersects with Identify Critical Assets 8CD-2a Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5
Business Functions Time Objectives (RTOs) of the contingency plan's activation.	5
RC.RP-05 N/A The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed.  Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, Services (TAAS) Recovery & Reconstitution	10
RC.RP-06 N/A The end of incident recovery is declared based on criteria, and incident related documentation is completed.  Functional  Functional  (4) Containment; (5) Endication; and (6) Recovery.	5
Situational Awareness For Incidents  Situational Awareness For Incidents  Situational Awareness For Incidents  IRO-09 Incidents or Incidents to internal stakeholders all the way through the resolution of the incident.	5
RecCO N/A Restoration activities are coordinated with internal and external external elements responsible for related plans. Functional Functional Pulsars external elements responsible for related plans and the contingency plans with the	5
Intersects with Service Providers Service Providers Service Providers a service providers to ensure that contingency requirements can be statisfied.	5
Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders.  Functional equal Procovery Operations Communications  Recovery Operations CD-0.16 restoring operational capabilities to designated internal and external stakeholders. 1  Mechanisms exist to communicate the status of recovery activities and progress in recovery Operations CD-0.16 restoring operational capabilities to designated internal and external stakeholders. 1  Mechanisms exist to communicate the status of recovery activities and progress in restoring operational capabilities or designated internal and external stakeholders. 1  Mechanisms exist to communicate the status of recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders. 1	10
Public protection in incident recognitions of percel using appropriate	10

