SCF Domain	SCF Control	SCF Control #	Secure Controls Framework (SCF) Control Description	CDPP Standard #	ISO 27001 v2013	ISO 27001 v2022	ISO 27002 v2013	ISO 27002 v2022

Cybersecurity & Privacy Governance	Digital Security Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and privacy governance controls.	**GOV-01**	4.3
					4.4
					5.1
					6.1.1
						4.4
						5.1
						5.1(a)
						5.1(b)
						5.1(c)
						5.1(d)
						5.1(e)
						5.1(f)
						5.1(g)
						5.1(h)
						6.1
						6.1.1
						6.1.1(a)
						6.1.1(b)
						6.1.1(c)
						6.1.1(d)
						6.1.1(e)(1)
						6.1.1(e)(2)
						8.1
						10.1
							5.1
							5.1.1
								5.1
								5.4
								5.37

Cybersecurity & Privacy Governance	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprised of key cybersecurity, privacy and business executives, which meets formally and on a regular basis.	**GOV-01.1**	4.3
					5.1
					6.2
					7.4
					9.3
					10.2
						4.4
						5.3
						5.3(a)
						5.3(b)
						9.3
						9.3.1
						9.3.2(a)
						9.3.2(b)
						9.3.2(c)
						9.3.2(d)
						9.3.2(d)(1)
						9.3.2(d)(2)
						9.3.2(d)(3)
						9.3.2(d)(4)
						9.3.2(e)
						9.3.2(f)
						9.3.2(g)
						9.3.3
						10.1		

Cybersecurity & Privacy Governance	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 privacy program.	**GOV-01.2**		7.4
						7.4(a)
						7.4(b)
						7.4(c)
						7.4(d)
						9.1
						9.1(a)
						9.1(b)
						9.1(c)
						9.1(d)
						9.1(e)
						9.1(f)
						9.3
						9.3.1
						9.3.2(a)
						9.3.2(b)
						9.3.2(c)
						9.3.2(d)
						9.3.2(d)(1)
						9.3.2(d)(2)
						9.3.2(d)(3)
						9.3.2(d)(4)
						9.3.2(e)
						9.3.2(f)
						9.3.2(g)
						9.3.3		

SCF Domain	SCF Control	SCF Control #	Secure Controls Framework (SCF) Control Description	CDPP Standard #	ISO 27001 v2013	ISO 27001 v2022	ISO 27002 v2013	ISO 27002 v2022

Cybersecurity & Privacy Governance	Publishing Cybersecurity & Privacy Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and privacy policies, standards and procedures.	**GOV-02**	4.3
					5.2
					7.5.1
					7.5.2
					7.5.3
						5.1(a)
						5.2
						5.2(a)
						5.2(b)
						5.2(c)
						5.2(d)
						5.2(e)
						5.2(f)
						5.2(g)
						7.5
						7.5.1
						7.5.1(a)
						7.5.1(b)
						7.5.2
						7.5.2(a)
						7.5.2(b)
						7.5.2(c)
						7.5.3
						7.5.3(a)
						7.5.3(b)
						7.5.3(c)
						7.5.3(d)
						7.5.3(e)
						7.5.3(f)
							5.1.1
							6.2.1
							9.1.1
								5.1
								5.37

Cybersecurity & Privacy Governance	Periodic Review & Update of Cybersecurity & Privacy Program	GOV-03	Mechanisms exist to review the cybersecurity and privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	**GOV-03**	6.1.1
					7.4
						7.5.2
						7.5.2(a)
						7.5.2(b)
						7.5.2(c)
							5.1.2	5.1
								5.37

Cybersecurity & Privacy Governance	Assigned Cybersecurity & Privacy Responsibilities	GOV-04	Mechanisms exist to assign a qualified individual with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.	**GOV-04**	5.3	5.1(f)
						5.1(h)
						5.3
						5.3(a)
						5.3(b)
								5.2

Cybersecurity & Privacy Governance	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and privacy program measures of performance.	**GOV-05**	9.1	9.1
						9.1(a)
						9.1(b)
						9.1(c)
						9.1(d)
						9.1(e)
						9.1(f)		

Cybersecurity & Privacy Governance	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	**GOV-06**			6.1.3	5.5
Cybersecurity & Privacy Governance	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the cybersecurity & privacy communities to: ▪ Facilitate ongoing cybersecurity and privacy education and training for organizational personnel; ▪ Maintain currency with recommended cybersecurity and privacy practices, techniques and technologies; and ▪ Share current security-related information including threats, vulnerabilities and incidents.	**GOV-07**			6.1.4	5.6
Cybersecurity & Privacy Governance	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the mission of the organization.	**GOV-08**	4.1 4.2			

Cybersecurity & Privacy Governance	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	**GOV-09**	5.1	4.1
						4.2
						4.2(b)
						4.2(c)
						5.2(b)
						6.2
						6.2(a)
						6.2(b)
						6.2(c)
						6.2(d)
						6.2(e)
						6.2(f)
						6.2(g)
						6.2(h)
						6.2(i)
						6.2(j)
						6.2(k)
						6.2(l)
								4.2

Asset Management	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	**AST-01**			11.2.6	5.30 5.31 7.9
Asset Management	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of technology assets that support more than one critical business function.	**AST-01.1**				5.9 5.30

SCF Domain	SCF Control	SCF Control #	Secure Controls Framework (SCF) Control Description	CDPP Standard #	ISO 27001 v2013	ISO 27001 v2022	ISO 27002 v2013	ISO 27002 v2022
Asset Management	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical systems, applications and services to support the ongoing secure management of those assets.	**AST-01.2**	4.2	4.2 4.2(a)		5.9
Asset Management	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and reporting; ▪ Includes organization-defined information deemed necessary to achieve effective property accountability; and ▪ Is available for review and audit by designated organizational personnel.	**AST-02**			8.1.1	5.9
Asset Management	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	**AST-02.7**			18.1.2	5.32 6.2
Asset Management	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of technology assets where sensitive/regulated data is stored, transmitted or processed.	**AST-02.8**				5.9
Asset Management	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.	**AST-03**			8.1.2	5.9
Asset Management	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.	**AST-03.1**				5.9
Asset Management	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to systems, system components and associated data.	**AST-03.2**				5.21
Asset Management	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: ▪ Contain sufficient detail to assess the security of the network's architecture; ▪ Reflect the current architecture of the network environment; and ▪ Document all sensitive/regulated data flows.	**AST-04**				5.9 8.20
Asset Management	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity and privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties).	**AST-04.1**		4.3		
Asset Management	Security of Assets & Media	AST-05	Mechanisms exist to maintain strict control over the internal or external distribution of any kind of sensitive/regulated media.	**AST-05**			11.2.6	7.9
Asset Management	Unattended End-User Equipment	AST-06	Mechanisms exist to implement enhanced protection measures for unattended systems to protect against tampering and unauthorized access.	**AST-06**			11.2.6 11.2.8	7.9 8.1
Asset Management	Kiosks & Point of Interaction (PoI) Devices	AST-07	Mechanisms exist to appropriately protect devices that capture sensitive/regulated data via direct physical interaction from tampering and substitution.	**AST-07**			11.2.8	8.1
Asset Management	Tamper Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	**AST-08**			11.2.6	7.9
Asset Management	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	**AST-09**			11.2.7	7.14 8.10
Asset Management	Return of Assets	AST-10	Mechanisms exist to ensure that employees and third-party users return all organizational assets in their possession upon termination of employment, contract or agreement.	**AST-10**			8.1.4	5.11
Asset Management	Removal of Assets	AST-11	Mechanisms exist to authorize, control and track technology assets entering and exiting organizational facilities.	**AST-11**			11.2.5	7.10
Asset Management	Use of Personal Devices	AST-12	Mechanisms exist to restrict the possession and usage of personally-owned technology devices within organization-controlled facilities.	**AST-12**				7.10 8.1

SCF Domain	SCF Control	SCF Control #	Secure Controls Framework (SCF) Control Description	CDPP Standard #	ISO 27001 v2013	ISO 27001 v2022	ISO 27002 v2013	ISO 27002 v2022
Asset Management	Tamper Protection	AST-15	Mechanisms exist to verify logical configuration settings and the physical integrity of critical technology assets throughout their lifecycle.	**AST-15**			11.2.6	7.9
Business Continuity & Disaster Recovery	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services.	**BCD-01**			17.1.1 17.1.2	5.29 5.30
Business Continuity & Disaster Recovery	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	**BCD-01.1**				5.29 5.30
Business Continuity & Disaster Recovery	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	**BCD-01.2**				5.29 5.30
Business Continuity & Disaster Recovery	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	**BCD-04**			17.1.3	5.29 5.30
Business Continuity & Disaster Recovery	Alternate Storage Site	BCD-08	Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.	**BCD-08**			17.2.1	8.14
Business Continuity & Disaster Recovery	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	**BCD-09**			17.2.1	8.14
Business Continuity & Disaster Recovery	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	**BCD-11**			12.3.1	8.13
Business Continuity & Disaster Recovery	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	**BCD-11.1**			12.3.1	8.13
Business Continuity & Disaster Recovery	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	**BCD-11.2**			12.3.1	8.13
Business Continuity & Disaster Recovery	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	**BCD-11.4**			12.3.1	8.13
Business Continuity & Disaster Recovery	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover system, that is not collocated with the primary system, application and/or service, which can be activated with little-to-no loss of information or disruption to operations.	**BCD-11.7**			17.2.1	8.14
Capacity & Performance Planning	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	**CAP-01**			12.1.3	8.6
Capacity & Performance Planning	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	**CAP-03**			12.1.3	8.6
Change Management	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	**CHG-01**		6.3	12.1.2	8.19 8.32
Change Management	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	**CHG-02**			12.1.2 14.2.2	8.19 8.32
Change Management	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	**CHG-02.2**			14.2.3	8.19 8.32
Cloud Security	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	**CLD-01**				5.23
Cloud Security	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	**CLD-02**				5.23
Cloud Security	Application & Program Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application & Program Interfaces (APIs).	**CLD-04**				5.23 8.26

SCF Domain	SCF Control	SCF Control #	Secure Controls Framework (SCF) Control Description	CDPP Standard #	ISO 27001 v2013	ISO 27001 v2022	ISO 27002 v2013	ISO 27002 v2022
Cloud Security	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	**CLD-06**				5.23
Cloud Security	Customer Responsibility Matrix (CRM)	CLD-06.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for controls between the Cloud Service Provider (CSP) and its customers.	**CLD-06.1**		4.3(c)		5.23
Cloud Security	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	**CLD-09**				5.23
Compliance	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	**CPL-01**		4.1 9.1 9.2 9.2.1 9.2.2	18.1.1	5.31 8.34

Compliance	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	**CPL-01.1**	10.1	9.1
						9.1(a)
						9.1(b)
						9.1(c)
						9.1(d)
						9.1(e)
						9.1(f)
						10.2
						10.2(a)
						10.2(a)(1)
						10.2(a)(2)
						10.2(b)
						10.2(b)(1)
						10.2(b)(2)
						10.2(b)(3)
						10.2(c)
						10.2(d)
						10.2(e)
						10.2(f)
						10.2(g)		

Compliance	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity and privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	**CPL-01.2**		4.3
						4.3(a)
						4.3(b)
						4.3(c)		

Compliance	Security & Privacy Controls Oversight	CPL-02	Mechanisms exist to provide a security & privacy controls oversight function that reports to the organization's executive leadership.	**CPL-02**	9.1 9.3 10.2	8.1 10.1	12.7.1 18.2.2 18.2.3	5.31 5.36 6.8 8.8 8.34

Compliance	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	**CPL-02.1**	9.1	9.2
						9.2.1
						9.2.1(a)(1)
						9.2.1(a)(2)
						9.2.1(b)
						9.2.2
						9.2.2(a)
						9.2.2(b)
						9.2.2(c)
							12.7.1	5.35
								8.34

Compliance	Security Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate security policies, standards and other applicable requirements.	**CPL-03**	9.2	8.1
						9.1
						9.1(a)
						9.1(b)
						9.1(c)
						9.1(d)
						9.1(e)
						9.1(f)
							18.2.2	5.35
								5.36
								8.34

Compliance	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security & privacy controls at planned intervals or when the system, service or project undergoes significant changes.	**CPL-03.1**	9.2		18.2.1	5.35
Compliance	Functional Review Of Security Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity and privacy policies and standards.	**CPL-03.2**	9.1		18.2.3	5.35 5.36 8.8
Compliance	Audit Activities	CPL-04	Mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations.	**CPL-04**	9.2		12.7.1	5.35 8.34
Configuration Management	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	**CFG-01**			9.4.1	8.3 8.9 8.12

SCF Domain	SCF Control	SCF Control #	Secure Controls Framework (SCF) Control Description	CDPP Standard #	ISO 27001 v2013	ISO 27001 v2022	ISO 27002 v2013	ISO 27002 v2022
Configuration Management	Assignment of Responsibility	CFG-01.1	Mechanisms exist to implement a segregation of duties for configuration management that prevents developers from performing production configuration management duties.	**CFG-01.1**				8.9
Configuration Management	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	**CFG-02**			9.4.1 14.1.1	8.3 8.5 8.9 8.12 8.25 8.26
Configuration Management	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: ▪ At least annually; ▪ When required due to so; or ▪ As part of system component installations and upgrades.	**CFG-02.1**				8.9
Configuration Management	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes.	**CFG-02.4**				8.25
Configuration Management	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	**CFG-02.5**				8.12
Configuration Management	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	**CFG-03**			9.4.1	8.3 8.9 8.12
Configuration Management	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	**CFG-03.1**			9.2.5 9.2.6 12.6.1 14.2.5	5.18 8.8 8.27
Continuous Monitoring	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	**MON-01**			12.4.1	8.15 8.16
Continuous Monitoring	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	**MON-01.1**				8.16
Continuous Monitoring	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	**MON-01.2**				8.16
Continuous Monitoring	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	**MON-01.3**				8.16
Continuous Monitoring	System Generated Alerts	MON-01.4	Mechanisms exist to monitor, correlate and respond to alerts from physical, cybersecurity, privacy and supply chain activities to achieve integrated situational awareness.	**MON-01.4**			12.4.1	8.15
Continuous Monitoring	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	**MON-01.8**				8.16
Continuous Monitoring	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	**MON-02**				8.15
Continuous Monitoring	Correlate Monitoring Information	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) or similar automated tool, to enhance organization-wide situational awareness.	**MON-02.1**				8.15
Continuous Monitoring	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	**MON-02.2**			12.4.1	6.8 8.15 8.16
Continuous Monitoring	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce audit records that contain sufficient information to, at a minimum: ▪ Establish what type of event occurred; ▪ When (date and time) the event occurred; ▪ Where the event occurred; ▪ The source of the event; ▪ The outcome (success or failure) of the event; and ▪ The identity of any user/subject associated with the event.	**MON-03**			12.4.1	8.15

SCF Domain	SCF Control	SCF Control #	Secure Controls Framework (SCF) Control Description	CDPP Standard #	ISO 27001 v2013	ISO 27001 v2022	ISO 27002 v2013	ISO 27002 v2022
Continuous Monitoring	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	MON-03.3			12.4.3	8.15
Continuous Monitoring	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	MON-06				6.8 8.15
Continuous Monitoring	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	MON-08			12.4.2	8.15
Continuous Monitoring	Monitoring For Information Disclosure	MON-11	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.	MON-11				5.7
Continuous Monitoring	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	MON-11.3				5.7
Cryptographic Protections	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	CRY-01			10.1.1 14.1.2	8.24 8.26
Cryptographic Protections	Export-Controlled Technology	CRY-01.2	Mechanisms exist to address the exporting of cryptographic technologies in compliance with relevant statutory and regulatory requirements.	CRY-01.2			18.1.5	5.31
Cryptographic Protections	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	CRY-03			10.1.1 13.2.3 14.1.2 14.1.3	5.14 8.24 8.26
Cryptographic Protections	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	CRY-04			10.1.1 14.1.3	8.24 8.26
Cryptographic Protections	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	CRY-05			10.1.1	8.24
Cryptographic Protections	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	CRY-09			10.1.2	8.24
Cryptographic Protections	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	CRY-09.3			10.1.2	8.24
Cryptographic Protections	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	CRY-09.4			10.1.2	8.24
Data Classification & Handling	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	DCH-01			8.2 8.2.3 8.3	5.9 5.10 5.12 5.33 7.10 8.12
Data Classification & Handling	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	DCH-02			8.2.1	5.9 5.12
Data Classification & Handling	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	DCH-03				7.10
Data Classification & Handling	Masking Displayed Data	DCH-03.2	Mechanisms exist to apply data masking to sensitive information that is displayed or printed.	DCH-03.2				8.11
Data Classification & Handling	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	DCH-04			8.2.2	5.10 5.13
Data Classification & Handling	Media Storage	DCH-06	Mechanisms exist to: ▪ Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and ▪ Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	DCH-06				7.10
Data Classification & Handling	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	DCH-07			8.3.3	5.14 7.10
Data Classification & Handling	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	DCH-07.1			8.2.3	5.10 5.14
Data Classification & Handling	Encrypting Data In Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	DCH-07.2				7.10
Data Classification & Handling	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	DCH-08			8.3.2	7.10 8.10

SCF Domain	SCF Control	SCF Control #	Secure Controls Framework (SCF) Control Description	CDPP Standard #	ISO 27001 v2013	ISO 27001 v2022	ISO 27002 v2013	ISO 27002 v2022
Data Classification & Handling	Digital Media Sanitization	DCH-09	Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	**DCH-09**				8.10
Data Classification & Handling	Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify media sanitization and disposal actions.	**DCH-09.1**				8.10
Data Classification & Handling	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	**DCH-09.3**				8.10
Data Classification & Handling	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	**DCH-10**			8.3.1	7.10
Data Classification & Handling	Limitations on Use	DCH-10.1	Mechanisms exist to restrict the use and distribution of sensitive / regulated data.	**DCH-10.1**				7.10
Data Classification & Handling	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	**DCH-12**			8.3.1	7.10
Data Classification & Handling	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	**DCH-14**			13.2 13.2.1 13.2.2	5.14
Data Classification & Handling	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	**DCH-17**			13.2.1	5.14
Data Classification & Handling	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	**DCH-18**			8.3 18.1.3	5.33 8.10
Data Classification & Handling	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	**DCH-21**				8.10
Data Classification & Handling	De-Identification (Anonymization)	DCH-23	Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.	**DCH-23**				8.33
Data Classification & Handling	Removal, Masking, Encryption, Hashing or Replacement of Direct Identifiers	DCH-23.4	Mechanisms exist to remove, mask, encrypt, hash or replace direct identifiers in a dataset.	**DCH-23.4**				8.11
Endpoint Security	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	**END-01**			11.2.9	7.7 8.1 8.5
Endpoint Security	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	**END-02**				8.1 8.5
Endpoint Security	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	**END-03**			12.5.1 12.6.2	8.19
Endpoint Security	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to systems.	**END-03.2**			12.5.1	8.19
Endpoint Security	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	**END-04**			12.2.1	8.7
Endpoint Security	Automatic Antimalware Signature Updates	END-04.1	Mechanisms exist to automatically update antimalware technologies, including signature definitions.	**END-04.1**			12.2.1	8.7

Human Resources Security	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	**HRS-01**		7.3
						7.3(a)
						7.3(b)
						7.3(c)
						7.2(d)
								5.4

Human Resources Security	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	**HRS-02**		7.2(a)		
Human Resources Security	Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.	**HRS-03**		7.3 7.3(b)	6.1.1 7.2	5.2

Human Resources Security	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	**HRS-03.1**		7.3
						7.3(a)
						7.3(b)
						7.3(c)		

Human Resources Security	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	**HRS-03.2**	7.2	7.2
						7.2(a)
						7.2(b)
						7.2(c)
						7.2(d)		

Human Resources Security	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	**HRS-04**		7.2(b)
						7.2(c)
							7.1
							7.1.1
								6.1

SCF Domain	SCF Control	SCF Control #	Secure Controls Framework (SCF) Control Description	CDPP Standard #	ISO 27001 v2013	ISO 27001 v2022	ISO 27002 v2013	ISO 27002 v2022
Human Resources Security	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	**HRS-04.1**				5.2 6.1

Human Resources Security	Formal Indoctrination	HRS-04.2	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information are formally indoctrinated for all the relevant types of information to which they have access on the system.	**HRS-04.2**		7.3
						7.3(a)
						7.3(b)
						7.3(c)
								5.4

Human Resources Security	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and privacy principles in their daily work.	**HRS-05**		7.3
						7.3(a)
						7.3(b)
						7.3(c)
							7.1.2
							7.2
							7.2.1
							13.2.1
								5.4
								5.14
								6.2

Human Resources Security	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.	**HRS-05.1**		7.3
						7.3(a)
						7.3(b)
						7.3(c)
							7.2
							7.2.1
							8.1.3
							13.2.1
								5.4
								5.10
								5.14
								6.2

Human Resources Security	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	**HRS-05.2**		7.3
						7.3(a)
						7.3(b)
						7.3(c)
							8.1.3	5.4
								5.10
								6.2

Human Resources Security	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	**HRS-05.3**		7.3
						7.3(a)
						7.3(b)
						7.3(c)
							8.1.3	5.4
								5.10
								6.2

Human Resources Security	Use of Critical Technologies	HRS-05.4	Mechanisms exist to govern usage policies for critical technologies.	**HRS-05.4**		7.3
						7.3(a)
						7.3(b)
						7.3(c)
							8.1.3	

Human Resources Security	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	**HRS-05.5**		7.3
						7.3(a)
						7.3(b)
						7.3(c)
							8.1.3	6.2

Human Resources Security	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization’s cybersecurity and privacy policies and provide acknowledgement.	**HRS-05.7**		7.3 7.3(c)		
Human Resources Security	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	**HRS-06**			13.2.2	5.10 5.14
Human Resources Security	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	**HRS-06.1**			13.2.2 13.2.4	5.14 6.6
Human Resources Security	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	**HRS-07**			7.2.3 7.3	6.4
Human Resources Security	Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.	**HRS-07.1**				6.4
Human Resources Security	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to systems and facilities upon personnel reassignment or transfer, in a timely manner.	**HRS-08**			7.3.1	6.5
Human Resources Security	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	**HRS-09**			7.3.1	6.5
Human Resources Security	Post-Employment Requirements	HRS-09.3	Mechanisms exist to govern former employee behavior by notifying terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information.	**HRS-09.3**				6.5
Human Resources Security	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	**HRS-11**				5.3 5.18
Human Resources Security	Incompatible Roles	HRS-12	Mechanisms exist to avoid incompatible development-specific roles through limiting and reviewing developer privileges to change hardware, software and firmware components within a production/operational environment.	**HRS-12**			6.1.2	5.3
Identification & Authentication	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	**IAC-01**			9.1 9.1.1	5.15 5.18
Identification & Authentication	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.	**IAC-02**				5.15