NIST CSF 2.0 - Assessor Checklist

Requirement ID	Requirement Name	Requirement Description	In Compliance	References	Issues	Assessed By	Related Controls
DE.AE-02	Potentially Adverse Event Analysis	DE.AE-02: Potentially adverse events are analyzed to better understand associated activities.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, IT Security	CIS8.11
DE.AE-03	Event Information Correlation	DE.AE-03: Information is correlated from multiple sources.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, IT Security	CRI.DE.AE-03.01 CRI.DE.AE-03.02
DE.AE-04	Impact & Scope Determination	DE.AE-04: The estimated impact and scope of adverse events are understood.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, IT Security	CRI.DE.AE-04.01
DE.AE-06	Event Information Sharing	DE.AE-06: Information on adverse events is provided to authorized staff and tools.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, IT Security	CRI.DE.AE-06.01
DE.AE-07	Contextual Analysis	DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, IT Security	CRI.DE.AE-07.01 CRI.DE.AE-07.02
DE.AE-08	Incident Declaration	DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, IT Security	CRI.DE.AE-08.01
DE.CM-01	Network Monitoring	DE.CM-01: Networks and network services are monitored to find potentially adverse events.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, IT Security	CIS13.1
DE.CM-02	Physical Environment Monitoring	DE.CM-02: The physical environment is monitored to find potentially adverse events.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, Operations	CRI.DE.CM-02.01
DE.CM-03	Personnel Activity Monitoring	DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, Operations	CIS10.7
DE.CM-06	Service Provider Monitoring	DE.CM-06: External service provider activities and services are monitored to find potentially adverse events.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, Operations	CIS15.2 CIS15.6
DE.CM-09	Hardware, Software, & Data Monitoring	DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, IT Security	CIS10.1
GV.OC-01	Organizational Mission	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, Exec Mgmt	CRI.GV.OC-01.01
GV.OC-02	Stakeholder Risk Management Expectations	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, Exec Mgmt	CRI.GV.OC-02.01 CRI.GV.OC-02.02 CRI.GV.OC-02.03
GV.OC-03	Legal, Regulatory, & Contractual Requirements	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, Governance Dept	CRI.GV.OC-03.01 CRI.GV.OC-03.02
GV.OC-04	Stakeholder Service Expectations	GV.OC-04: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, Governance Dept	CRI.GV.OC-04.01 CRI.GV.OC-04.02 CRI.GV.OC-04.03 CRI.GV.OC-04.04
GV.OC-05	Organizational Service Dependencies	GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, Exec Mgmt	CRI.GV.OC-05.01 CRI.GV.OC-05.02 CRI.GV.OC-05.03 CRI.GV.OC-05.04
GV.OV-01	Risk Management Strategy Outcomes Review	GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	Compliance Dept, Governance Dept	CRI.GV.OV-01.01 CRI.GV.OV-01.02 CRI.GV.OV-01.03
GV.OV-02	Risk Management Strategy Review & Adjustment	GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	Compliance Dept, Governance Dept	CRI.GV.OV-02.01 CRI.GV.OV-02.02
GV.OV-03	Risk Management Performance Measurement	GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	Compliance Dept, Governance Dept	CRI.GV.OV-03.01 CRI.GV.OV-03.02
GV.PO-01	Establishment of Policies & Procedures	GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.	Yes	NIST CSF 2.0 Assessment		Compliance Dept, Governance Dept	CRI.GV.PO-01.01 CRI.GV.PO-01.02 CRI.GV.PO-01.03 CRI.GV.PO-01.04 CRI.GV.PO-01.05 CRI.GV.PO-01.06 CRI.GV.PO-01.07 CRI.GV.PO-01.08
GV.PO-02	Policy & Procedure Review & Update	GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	Governance Dept	CRI.GV.PO-02.01
GV.RM-01	Risk Management Objectives Agreement	GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders.	Yes	NIST CSF 2.0 Assessment		Governance Dept	CRI.GV.RM-01.01 CRI.GV.RM-01.02 CRI.GV.RM-01.03 CRI.GV.RM-01.04 CRI.GV.RM-01.05
GV.RM-02	Risk Appetite & Risk Tolerance Statements	GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained.	Yes	NIST CSF 2.0 Assessment		Governance Dept	CRI.GV.RM-02.01 CRI.GV.RM-02.02 CRI.GV.RM-02.03
GV.RM-03	Enterprise Risk Integration	GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.	Yes	NIST CSF 2.0 Assessment		Governance Dept	CRI.GV.RM-03.01 CRI.GV.RM-03.02 CRI.GV.RM-03.03 CRI.GV.RM-03.04
GV.RM-04	Risk Response Strategic Direction	GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated.	Yes	NIST CSF 2.0 Assessment		Governance Dept	CRI.GV.RM-04.01
GV.RM-05	Lines of Communication	GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	Governance Dept	CRI.GV.RM-05.01 CRI.GV.RM-05.02
GV.RM-06	Standardized Risk Management Method	GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated.	Yes	NIST CSF 2.0 Assessment		Governance Dept	CRI.GV.RM-06.01
GV.RM-07	Strategic Opportunities	GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	Governance Dept	CRI.GV.RM-07.01
GV.RR-01	Organizational Leadership Responsibility	GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving.	Yes	NIST CSF 2.0 Assessment		Governance Dept	CIS14.1
GV.RR-02	Risk Management Roles & Responsibilities	GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.	Yes	NIST CSF 2.0 Assessment		Governance Dept	CIS14.9
GV.RR-03	Resource Adequacy	GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.	Yes	NIST CSF 2.0 Assessment		Governance Dept	CRI.GV.RR-03.01 CRI.GV.RR-03.02 CRI.GV.RR-03.03
GV.RR-04	Human Resource Practices	GV.RR-04: Cybersecurity is included in human resources practices.	Yes	NIST CSF 2.0 Assessment		Governance Dept	CIS6.1 CIS6.2
GV.SC-01	Supply Chain Risk Management Program	GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	IT Security	CIS15.2
GV.SC-02	Third Party Roles & Responsibilities	GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS15.4
GV.SC-03	Supply Chain Risk Management Integration	GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	IT Security	CRI.GV.SC-03.01
GV.SC-04	Supplier Identification & Prioritization	GV.SC-04: Suppliers are known and prioritized by criticality.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	Governance Dept	CIS15.1 CIS15.3
GV.SC-05	Cybersecurity Risks & Supply Chain Contracts	GV.SC-05: 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.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS15.4
GV.SC-06	Supplier Due Diligence	GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS15.5
GV.SC-07	Supplier Risk Assessment and Risk Management	GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS15.6
GV.SC-08	Third Party Incident Management Integration	GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS15.4
GV.SC-09	Supply Chain Security Practice Integration	GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS15.6

Requirement ID	Requirement Name	Requirement Description	In Compliance	References	Issues	Assessed By	Related Controls
GV.SC-10	Third Party Post Relationship Risk Management	GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS15.7
ID.AM-01	Hardware Inventory	ID.AM-01: Inventories of hardware managed by the organization are maintained.	Yes	NIST CSF 2.0 Assessment		Governance Dept	CIS1.1
ID.AM-02	Software, Services, & Systems Inventory	ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.	Yes	NIST CSF 2.0 Assessment		IT Systems	CIS2.1
ID.AM-03	Network Communications & Data Flows	ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained.	Yes	NIST CSF 2.0 Assessment		Data Protection	CIS3.8
ID.AM-04	Supplier Services Inventory	ID.AM-04: Inventories of services provided by suppliers are maintained.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS15.1
ID.AM-05	Asset Protection Prioritization	ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission.	Yes	NIST CSF 2.0 Assessment		IT Systems	CIS3.7
ID.AM-07	Data & Metadata Inventory	ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained.	Yes	NIST CSF 2.0 Assessment		Data Protection	CIS3.2
ID.AM-08	Asset Life Cycle Management	ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles.	Yes	NIST CSF 2.0 Assessment		Data Protection, IT Security	CIS1.1 CIS3.5
ID.IM-01	Continuous Improvements Evaluation	ID.IM-01: Improvements are identified from evaluations.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	Governance Dept	CRI.ID.IM-01.01 CRI.ID.IM-01.02 CRI.ID.IM-01.03 CRI.ID.IM-01.04 CRI.ID.IM-01.05
ID.IM-02	Tests & Exercises	ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS17.7
ID.IM-03	Improvements from Lessons Learned	ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities.	Yes	NIST CSF 2.0 Assessment		Governance Dept	CRI.ID.IM-03.01 CRI.ID.IM-03.02
ID.IM-04	Plans Affecting Operations	ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.	Yes	NIST CSF 2.0 Assessment		Operations	CRI.ID.IM-04.01 CRI.ID.IM-04.02 CRI.ID.IM-04.03 CRI.ID.IM-04.04 CRI.ID.IM-04.05 CRI.ID.IM-04.06 CRI.ID.IM-04.07 CRI.ID.IM-04.08
ID.RA-01	Asset Vulnerability Identification	ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS7.1
ID.RA-02	Information Sharing Forums	ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources.	Yes	NIST CSF 2.0 Assessment		IT Security	CRI.ID.RA-02.01 CRI.ID.RA-02.02
ID.RA-03	Threat Identification	ID.RA-03: Internal and external threats to the organization are identified and recorded.	Yes	NIST CSF 2.0 Assessment		IT Security	CRI.ID.RA-03.01 CRI.ID.RA-03.02 CRI.ID.RA-03.03 CRI.ID.RA-03.04
ID.RA-04	Impact & Likelihood Analysis	ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.	Yes	NIST CSF 2.0 Assessment		IT Security	CRI.ID.RA-04.01
ID.RA-05	Risk Exposure Determination & Prioritization	ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization.	Yes	NIST CSF 2.0 Assessment		Exec Mgmt	CRI.ID.RA-05.01 CRI.ID.RA-05.02 CRI.ID.RA-05.03 CRI.ID.RA-05.04
ID.RA-06	Risk Response Determination	ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated.	Yes	NIST CSF 2.0 Assessment		IT Security	CRI.ID.RA-06.01 CRI.ID.RA-06.02 CRI.ID.RA-06.03 CRI.ID.RA-06.04 CRI.ID.RA-06.05 CRI.ID.RA-06.06
ID.RA-07	Change & Exception Management	ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked.	Yes	NIST CSF 2.0 Assessment		IT Security	CRI.ID.RA-07.01 CRI.ID.RA-07.02 CRI.ID.RA-07.03 CRI.ID.RA-07.04 CRI.ID.RA-07.05
ID.RA-08	Vulnerability Disclosure Response	ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	IT Security	CIS7.2
ID.RA-09	Pre-acquisition Integrity Assessment	ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	IT Security	CRI.EX.DD-04.01 CRI.EX.DD-04.02
ID.RA-10	Supplier Pre-Acquisition Assessments	ID.RA-10: Critical suppliers are assessed prior to acquisition.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	Governance Dept	CRI.EX.DD-03.01 CRI.EX.DD-03.02 CRI.EX.DD-03.03
PR.AA-01	Identity & Credential Management	PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS5.1 CIS6.7
PR.AA-02	Identity Binding to Credentials	PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	IT Security	CRI.PR.AA-02.01
PR.AA-03	Authentication	PR.AA-03: Users, services, and hardware are authenticated.	Yes	NIST CSF 2.0 Assessment		IT Security	CRI.PR.AA-03.01 CRI.PR.AA-03.02 CRI.PR.AA-03.03
PR.AA-04	Identity Assertions	PR.AA-04: Identity assertions are protected, conveyed, and verified.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	IT Security	CRI.PR.AA-04.01
PR.AA-05	Access Authorizations	PR.AA-05: 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.	Yes	NIST CSF 2.0 Assessment		Data Protection	CIS3.3 CIS6.8
PR.AA-06	Physical Access	PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk.	Yes	NIST CSF 2.0 Assessment		Operations	CRI.PR.AA-06.01 CRI.PR.AA-06.02
PR.AT-01	User Awareness & Training	PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS14.1
PR.AT-02	Specialized Role Awareness & Training	PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS14.9
PR.DS-01	Protection of Data at Rest	PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected.	Yes	NIST CSF 2.0 Assessment		Data Protection	CIS3.11
PR.DS-02	Protection of Data in Transit	PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected.	Yes	NIST CSF 2.0 Assessment		Data Protection	CIS3.10
PR.DS-10	Protection of Data in Use	PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected.	Yes	NIST CSF 2.0 Assessment		Data Protection	CRI.PR.DS-10.01
PR.DS-11	Data Backup	PR.DS-11: Backups of data are created, protected, maintained, and tested.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	Data Protection	CIS11.2 CIS11.3 CIS11.5
PR.IR-01	Logical Access Protections	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS3.12 CIS12.2
PR.IR-02	Environmental Threat Protections	PR.IR-02: The organization's technology assets are protected from environmental threats.	Yes	NIST CSF 2.0 Assessment		Operations	CRI.PR.IR-02.01
PR.IR-03	Resilience Measures	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	Operations	CRI.PR.IR-03.01
PR.IR-04	Capacity Management	PR.IR-04: Adequate resource capacity to ensure availability is maintained.	Yes	NIST CSF 2.0 Assessment		Operations	CRI.PR.IR-04.01 CRI.PR.IR-04.02
PR.PS-01	Configuration Management	PR.PS-01: Configuration management practices are established and applied.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS4.1 CIS4.2
PR.PS-02	Software Maintenance & Replacement	PR.PS-02: Software is maintained, replaced, and removed commensurate with risk.	Yes	NIST CSF 2.0 Assessment		IT Systems	CIS2.2 CIS2.3
PR.PS-03	Hardware Maintenance	PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk.	Yes	NIST CSF 2.0 Assessment		IT Systems	CIS1.2
PR.PS-04	Log Record Generation	PR.PS-04: Log records are generated and made available for continuous monitoring.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS8.2
PR.PS-05	Unauthorized Software Installation & Execution	PR.PS-05: Installation and execution of unauthorized software are prevented.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS2.5

Requirement ID	Requirement Name	Requirement Description	In Compliance	References	Issues	Assessed By	Related Controls
PR.PS-06	Secure Systems Development Practices	PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	IT Security	CIS16.1
RC.CO-03	Recovery Activity Communication	RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders.	Yes	NIST CSF 2.0 Assessment		Governance Dept	CRI.RC.CO-03.01 CRI.RC.CO-03.02
RC.CO-04	Public Information Sharing	RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS17.2 CIS17.6
RC.RP-01	Recovery Plan Execution	RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process.	Yes	NIST CSF 2.0 Assessment		Operations	CRI.RC.RP-01.01
RC.RP-02	Recovery Action Performance	RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed.	Yes	NIST CSF 2.0 Assessment		Operations	CRI.RC.RP-02.01 CRI.RC.RP-02.02
RC.RP-03	Backup & Restoration Asset Integrity	RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration.	Yes	NIST CSF 2.0 Assessment		Operations	CIS11.5
RC.RP-04	Post-Incident Operational Norms	RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms.	Yes	NIST CSF 2.0 Assessment		Exec Mgmt, Governance Dept	CRI.RC.RP-04.01
RC.RP-05	Asset Integrity Restoration	RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	IT Security	CRI.RC.RP-05.01 CRI.RC.RP-05.02
RC.RP-06	End-of-Incident Determination	RC.RP-06: The end of incident recovery is declared based on criteria, and incident-related documentation is completed.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	IT Security	CRI.RC.RP-06.01
RS.AN-03	Incident Analysis & Root Cause Determination	RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident.	Yes	NIST CSF 2.0 Assessment		IT Security	CIS17.8
RS.AN-06	Investigation Documentation	RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved.	Yes	NIST CSF 2.0 Assessment		IT Security	CRI.RS.AN-06.01
RS.AN-07	Incident Data Collection & Preservation	RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	IT Security	CRI.RS.AN-07.01
RS.AN-08	Incident Magnitude Determination	RS.AN-08: An incident's magnitude is estimated and validated.	Yes	NIST CSF 2.0 Assessment		IT Security	CRI.RS.AN-08.01
RS.CO-02	Stakeholder Incident Notification	RS.CO-02: Internal and external stakeholders are notified of incidents.	Yes	NIST CSF 2.0 Assessment		Exec Mgmt, Governance Dept	CIS17.2
RS.CO-03	Stakeholder Incident Information Sharing	RS.CO-03: Information is shared with designated internal and external stakeholders.	Yes	NIST CSF 2.0 Assessment		Exec Mgmt, Governance Dept	CIS17.2
RS.MA-01	Response Plan Execution	RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared.	Yes	NIST CSF 2.0 Assessment		Exec Mgmt, Governance Dept	CIS17.4
RS.MA-02	Incident Triage & Validation	RS.MA-02: Incident reports are triaged and validated.	Yes	NIST CSF 2.0 Assessment		IT Security	CRI.RS.MA-02.01
RS.MA-03	Incident Categorization & Prioritization	RS.MA-03: Incidents are categorized and prioritized.	Yes	NIST CSF 2.0 Assessment		IT Security	CRI.RS.MA-03.01
RS.MA-04	Incident Escalation	RS.MA-04: Incidents are escalated or elevated as needed.	Yes	NIST CSF 2.0 Assessment		IT Security	CRI.RS.MA-04.01
RS.MA-05	Recovery Initiation	RS.MA-05: The criteria for initiating incident recovery are applied.	No	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Requirement not addressed.	Exec Mgmt, Governance Dept	CIS17.9
RS.MI-01	Incident Containment	RS.MI-01: Incidents are contained.	Yes	NIST CSF 2.0 Assessment		IT Security	CRI.RS.MI-01.01
RS.MI-02	Incident Eradication	RS.MI-02: Incidents are eradicated.	Yes	NIST CSF 2.0 Assessment		IT Security	CRI.RS.MI-02.01

NIST CSF 2.0 - Assessor Checklist

Control ID	Control Name	Control Description	Implementation Status	References	Issues	Assessed By	NIST CSF 2.0
CIS1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	Fully Implemented	NIST CSF 2.0 Assessment		IT Systems	ID.AM-01 ID.AM-08
CIS1.2	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	Fully Implemented	NIST CSF 2.0 Assessment		IT Systems	PR.PS-03
CIS2.1	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	Fully Implemented	NIST CSF 2.0 Assessment		IT Systems	ID.AM-02
CIS2.2	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	Fully Implemented	NIST CSF 2.0 Assessment		IT Systems	PR.PS-02
CIS2.3	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	Fully Implemented	NIST CSF 2.0 Assessment		IT Systems	PR.PS-02
CIS2.5	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	PR.PS-05
CIS3.2	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	Fully Implemented	NIST CSF 2.0 Assessment		Data Protection	ID.AM-07
CIS3.3	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Fully Implemented	NIST CSF 2.0 Assessment		Data Protection	PR.AA-05
CIS3.5	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Data Protection	ID.AM-08
CIS3.7	Establish and Maintain a Data Classification Scheme	Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as Sensitive, Confidential, and Public, and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.	Fully Implemented	NIST CSF 2.0 Assessment		Data Protection	ID.AM-05
CIS3.8	Document Data Flows	Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Fully Implemented	NIST CSF 2.0 Assessment		Data Protection	ID.AM-03
CIS3.10	Encrypt Sensitive Data in Transit	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).	Fully Implemented	NIST CSF 2.0 Assessment		Data Protection	PR.DS-02
CIS3.11	Encrypt Sensitive Data at Rest	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.	Fully Implemented	NIST CSF 2.0 Assessment		Data Protection	PR.DS-01
CIS3.12	Segment Data Processing and Storage Based on Sensitivity	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	PR.IR-01
CIS4.1	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	PR.PS-01
CIS4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	PR.PS-01
CIS5.1	Establish and Maintain an Inventory of Accounts	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	Fully Implemented	NIST CSF 2.0 Assessment		IT Systems	PR.AA-01
CIS6.1	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	GV.RR-04
CIS6.2	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	GV.RR-04
CIS6.7	Centralize Access Control	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	PR.AA-01
CIS6.8	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	PR.AA-05
CIS7.1	Establish and Maintain a Vulnerability Management Process	Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-01
CIS7.2	Establish and Maintain a Remediation Process	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	IT Security	ID.RA-08
CIS8.2	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	PR.PS-04
CIS8.11	Conduct Audit Log Reviews	Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	DE.AE-02
CIS10.1	Deploy and Maintain Anti-Malware Software	Deploy and maintain anti-malware software on all enterprise assets.	Fully Implemented	NIST CSF 2.0 Assessment		IT Systems	DE.CM-09
CIS10.7	Use Behavior-Based Anti-Malware Software	Use behavior-based anti-malware software.	Fully Implemented	NIST CSF 2.0 Assessment		IT Systems	DE.CM-03
CIS11.2	Perform Automated Backups	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	IT Systems	PR.DS-11
CIS11.3	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	PR.DS-11
CIS11.5	Test Data Recovery	Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.	Fully Implemented	NIST CSF 2.0 Assessment		IT Systems	PR.DS-11 RC.RP-03
CIS12.2	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	PR.IR-01
CIS13.1	Centralize Security Event Alerting	Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	DE.CM-01
CIS14.1	Establish and Maintain a Security Awareness Program	Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	GV.RR-01 PR.AT-01
CIS14.9	Conduct Role-Specific Security Awareness and Skills Training	Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	GV.RR-02 PR.AT-02
CIS15.1	Establish and Maintain an Inventory of Service Providers	Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.SC-04 ID.AM-04
CIS15.2	Establish and Maintain a Service Provider Management Policy	Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	DE.CM-06 GV.SC-01

Control ID	Control Name	Control Description	Implementation Status	References	Issues	Assessed By	NIST CSF 2.0
CIS15.3	Classify Service Providers	Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	GV.SC-04
CIS15.4	Ensure Service Provider Contracts Include Security Requirements	Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	GV.SC-02 GV.SC-05 GV.SC-08
CIS15.5	Assess Service Providers	Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	GV.SC-06
CIS15.6	Monitor Service Providers	Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	DE.CM-06 GV.SC-07 GV.SC-09
CIS15.7	Securely Decommission Service Providers	Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	GV.SC-10
CIS16.1	Establish and Maintain a Secure Application Development Process	Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	IT Security	PR.PS-06
CIS17.2	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	RC.CO-04 RS.CO-02 RS.CO-03
CIS17.4	Establish and Maintain an Incident Response Process	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	RS.MA-01
CIS17.6	Define Mechanisms for Communicating During Incident Response	Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	RC.CO-04
CIS17.7	Conduct Routine Incident Response Exercises	Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.IM-02
CIS17.8	Conduct Post-Incident Reviews	Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	RS.AN-03
CIS17.9	Establish and Maintain Security Incident Thresholds	Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	IT Security	RS.MA-05
CRI.DE.AE-03.01	Event Information Correlation.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-03.01: The organization implements systematic and real-time logging, collection, monitoring, detection, and alerting measures across multiple layers of the organization's infrastructure, including physical perimeters, network, operating systems, applications, data, and external (cloud and outsourced) environments, sufficient to protect the organization's information assets.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	DE.AE-03
CRI.DE.AE-03.02	Event Information Correlation.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-03.02: The organization performs real-time central analysis, aggregation, and correlation of anomalous activities, network and system alerts, and relevant event and cyber threat intelligence, including both internal and external (cloud and outsourced) environments, to better detect and prevent multifaceted cyber attacks.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	DE.AE-03
CRI.DE.AE-04.01	Impact & Scope Determination	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-04.01: The organization has a documented process to analyze and triage incidents to assess root cause, technical impact, mitigation priority, and business impact on the organization, as well as across the financial sector and other third party stakeholders.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	DE.AE-04
CRI.DE.AE-06.01	Event Information Sharing	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-06.01: The organization has established processes and protocols to communicate, alert, and regularly report potential cyber attacks and incident information, including its corresponding analysis and cyber threat intelligence, to authorized internal and external stakeholders.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	DE.AE-06
CRI.DE.AE-07.01	Contextual Analysis.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-07.01: The organization implements measures for monitoring external sources (e.g., social media, the dark web, etc.) to integrate with other intelligence information to better detect and evaluate potential threats and compromises.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	DE.AE-07
CRI.DE.AE-07.02	Contextual Analysis.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-07.02: Relevant event data is packaged for subsequent review and triage and events are categorized for efficient handling, assignment, and escalation.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	DE.AE-07
CRI.DE.AE-08.01	Incident Declaration	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-08.01: Defined criteria and severity levels are in place to facilitate the declaration, escalation, organization, and alignment of response activities to response plans within the organization and across relevant third parties.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	DE.AE-08
CRI.DE.CM-02.01	Physical Environment Monitoring	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.CM-02.01: The organization's controls include monitoring and detection of anomalous activities and potential intrusion events across the organization's physical environment and infrastructure, including the detection of environmental threats (fire, water, service outages, etc.) and unauthorized physical access to high-risk system components and locations.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	DE.CM-02
CRI.EX.DD-03.01	Technology & Cybersecurity Risk Assessment.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - EX.DD-03.01: The organization reviews, evaluates, and risk assesses a prospective critical third party's cybersecurity program, including its ability to identify, assess, monitor, and mitigate its cyber risks; the completeness of its policies and procedures; the strength of its technical and administrative controls; and the coverage of its internal and independent control testing programs.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	ID.RA-10
CRI.EX.DD-03.02	Technology & Cybersecurity Risk Assessment.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - EX.DD-03.02: The organization reviews, evaluates, and risk assesses a prospective critical third party's business continuity program, to include business impact analyses, risk assessments, continuity plans, disaster recovery plans, technology resilience architecture, and response and recovery plans, test plans, and test results.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	ID.RA-10
CRI.EX.DD-03.03	Technology & Cybersecurity Risk Assessment.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - EX.DD-03.03: The organization reviews, evaluates, and risk assesses a prospective critical third party's incident response program, to include monitoring and alerting capabilities, incident reporting procedures and protocols, and capabilities for event analysis, problem resolution, and forensic investigation.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	ID.RA-10
CRI.EX.DD-04.01	Product & Service Due Diligence.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - EX.DD-04.01: The organization defines and implements procedures for assessing the compatibility, security, integrity, and authenticity of externally-developed or externally-sourced applications, software, software components, and firmware before deployment and upon any major change.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	IT Security	ID.RA-09
CRI.EX.DD-04.02	Product & Service Due Diligence.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - EX.DD-04.02: The organization reviews and evaluates any technologies or information systems proposed to support a third party's services or activities, to include compatibility with the organization's technology and cybersecurity architectures, interactions and interfaces with existing systems, security controls, operational management and support requirements, and suitability to the task.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	IT Security	ID.RA-09
CRI.GV.OC-01.01	Organizational Mission	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OC-01.01: Technology and cybersecurity strategies, architectures, and programs are formally governed to align with and support the organization's mission, objectives, priorities, tactical initiatives, and risk profile.	Fully Implemented	NIST CSF 2.0 Assessment		Exec Mgmt	GV.OC-01
CRI.GV.OC-02.01	Stakeholder Risk Management Expectations.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OC-02.01: The organization's obligation to its customers, employees, and stakeholders to maintain safety and soundness, while balancing size and complexity, is reflected in the organization's risk management strategy and framework, its risk appetite and risk tolerance statements, and in a risk-aware culture.	Fully Implemented	NIST CSF 2.0 Assessment		Exec Mgmt	GV.OC-02

Control ID	Control Name	Control Description	Implementation Status	References	Issues	Assessed By	NIST CSF 2.0
CRI.GV.OC-02.02	Stakeholder Risk Management Expectations.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OC-02.02: Technology and cybersecurity risk management strategies identify and communicate the organization's role within the financial services sector as a component of critical infrastructure.	Fully Implemented	NIST CSF 2.0 Assessment		Exec Mgmt	GV.OC-02
CRI.GV.OC-02.03	Stakeholder Risk Management Expectations.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OC-02.03: Technology and cybersecurity risk management strategies identify and communicate the organization's role as it relates to other critical infrastructure sectors outside of the financial services sector and the interdependency risks.	Fully Implemented	NIST CSF 2.0 Assessment		Exec Mgmt	GV.OC-02
CRI.GV.OC-03.01	Legal, Regulatory, & Contractual Requirements.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OC-03.01: The organization's technology and cybersecurity strategy, framework, and policies align and are consistent with the organization's legal, statutory, contractual, and regulatory obligations and ensure that compliance responsibilities are unambiguously assigned.	Fully Implemented	NIST CSF 2.0 Assessment		Compliance, Legal	GV.OC-03
CRI.GV.OC-03.02	Legal, Regulatory, & Contractual Requirements.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OC-03.02: The organization implements and maintains a documented policy or policies that address customer data privacy that is approved by a designated officer or the organization's appropriate governing body (e.g., the Board or one of its committees).	Fully Implemented	NIST CSF 2.0 Assessment		Compliance, Legal	GV.OC-03
CRI.GV.OC-04.01	Stakeholder Service Expectations.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OC-04.01: The organization maintains an inventory of key internal assets, business functions, and external dependencies that includes mappings to other assets, business functions, and information flows.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.OC-04
CRI.GV.OC-04.02	Stakeholder Service Expectations.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OC-04.02: The organization documents the business processes that are critical for the delivery of services and the functioning of the organization, and the impacts to the business if those processes are degraded or not functioning.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.OC-04
CRI.GV.OC-04.03	Stakeholder Service Expectations.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OC-04.03: Resilience requirements to support the delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, and normal operations).	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.OC-04
CRI.GV.OC-04.04	Stakeholder Service Expectations.04	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OC-04.04: The organization prioritizes the resilience design, planning, testing, and monitoring of systems and other key internal and external dependencies according to their criticality to the supported business functions, enterprise mission, and to the financial services sector.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.OC-04
CRI.GV.OC-05.01	Organizational Service Dependencies.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OC-05.01: The organization identifies, assesses, and documents the key dependencies, interdependencies, and potential points of failure to support the delivery of critical services (e.g., systems, business processes, workforce, third parties, facilities, etc.)	Fully Implemented	NIST CSF 2.0 Assessment		Exec Mgmt	GV.OC-05
CRI.GV.OC-05.02	Organizational Service Dependencies.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OC-05.02: The organization has prioritized its external dependencies according to their criticality to the supported enterprise mission, business functions, and to the financial services sector.	Fully Implemented	NIST CSF 2.0 Assessment		Exec Mgmt	GV.OC-05
CRI.GV.OC-05.03	Organizational Service Dependencies.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OC-05.03: The organization defines objectives (e.g., Recovery Time Objective, Maximum Tolerable Downtime, Impact Tolerance) for the resumption of critical operations in alignment with business imperatives, stakeholder obligations, and critical infrastructure dependencies.	Fully Implemented	NIST CSF 2.0 Assessment		Exec Mgmt	GV.OC-05
CRI.GV.OC-05.04	Organizational Service Dependencies.04	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OC-05.04: Recovery point objectives to support data integrity are consistent with the organization's recovery time objectives, information flow dependencies between systems, and business obligations.	Fully Implemented	NIST CSF 2.0 Assessment		Exec Mgmt	GV.OC-05
CRI.GV.OV-01.01	Risk Management Strategy Outcomes Review.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OV-01.01: The governing authority (e.g., the Board or one of its committees) regularly reviews and evaluates the organization's ability to manage its technology, cybersecurity, third-party, and resilience risks.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	GV.OV-01
CRI.GV.OV-01.02	Risk Management Strategy Outcomes Review.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OV-01.02: The designated Cybersecurity Officer (e.g., CISO) periodically reports to the appropriate governing authority (e.g., the Board or one of its committees) or equivalent governing body on the status of cybersecurity within the organization.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	GV.OV-01
CRI.GV.OV-01.03	Risk Management Strategy Outcomes Review.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OV-01.03: The designated Technology Officer (e.g., CIO or CTO) regularly reports to the governing authority (e.g., the Board or one of its committees) on the status of technology use and risks within the organization.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	GV.OV-01
CRI.GV.OV-02.01	Risk Management Strategy Review & Adjustment.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OV-02.01: The organization regularly assesses its inherent technology and cybersecurity risks and ensures that changes to the business and threat environment lead to updates to the organization's strategies, programs, risk appetite and risk tolerance.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	GV.OV-02
CRI.GV.OV-02.02	Risk Management Strategy Review & Adjustment.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OV-02.02: The organization determines and articulates how it intends to maintain an acceptable level of residual technology and cybersecurity risk as set by the governing authority (e.g., the Board or one of its committees).	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	GV.OV-02
CRI.GV.OV-03.01	Risk Management Performance Measurement.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OV-03.01: The organization develops, implements, and reports to management and the governing body (e.g., the Board or one of its committees) key technology and cybersecurity risk and performance indicators and metrics to measure, monitor, and report actionable indicators.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	GV.OV-03
CRI.GV.OV-03.02	Risk Management Performance Measurement.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.OV-03.02: Resilience program performance is measured and regularly reported to senior executives and the governing authority (e.g., the Board or one of its committees).	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	GV.OV-03
CRI.GV.PO-01.01	Establishment of Policies & Procedures.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.PO-01.01: Technology and cybersecurity policies are documented, maintained and approved by the governing authority (e.g., the Board or one of its committees) or a designated executive.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.PO-01
CRI.GV.PO-01.02	Establishment of Policies & Procedures.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.PO-01.02: The accountable governing body, and applicable cybersecurity program and policies, for any given organizational unit, affiliate, or merged entity are clearly established, applied, and communicated.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.PO-01
CRI.GV.PO-01.03	Establishment of Policies & Procedures.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.PO-01.03: The organization's incentive programs are consistent with cyber risk management objectives, and technology and cybersecurity policies integrate with an employee accountability policy to ensure that all personnel are held accountable for complying with policies.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.PO-01
CRI.GV.PO-01.04	Establishment of Policies & Procedures.04	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.PO-01.04: All personnel (employees and third party) consent to policies addressing acceptable technology use, social media use, personal device use (e.g., BYOD), confidentiality, and/or other security-related policies and agreements as warranted by their position.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.PO-01
CRI.GV.PO-01.05	Establishment of Policies & Procedures.05	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.PO-01.05: Technology and cybersecurity processes, procedures, and controls are established in alignment with cybersecurity policy.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.PO-01
CRI.GV.PO-01.06	Establishment of Policies & Procedures.06	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.PO-01.06: Physical and environmental security policies are implemented and managed.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.PO-01
CRI.GV.PO-01.07	Establishment of Policies & Procedures.07	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.PO-01.07: The organization maintains documented business continuity and resilience program policies and procedures approved by the governing authority (e.g., the Board or one of its committees).	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.PO-01
CRI.GV.PO-01.08	Establishment of Policies & Procedures.08	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.PO-01.08: The organization maintains documented third-party risk management program policies and procedures approved by the governing authority (e.g., the Board or one of its committees).	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.PO-01
CRI.GV.PO-02.01	Policy & Procedure Review & Update	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.PO-02.01: The cybersecurity policy is regularly reviewed, revised, and communicated under the leadership of a designated Cybersecurity Officer (e.g., CISO) to address changes in the risk profile and risk appetite, the evolving threat environment, and new technologies, products, services, and interdependencies.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	GV.PO-02
CRI.GV.RM-01.01	Risk Management Objectives Agreement.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-01.01: Technology and cybersecurity risk management strategies and frameworks are approved by the governing authority (e.g., the Board or one of its committees) and incorporated into the overall business strategy and enterprise risk management framework.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.RM-01
CRI.GV.RM-01.02	Risk Management Objectives Agreement.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-01.02: Technology and cybersecurity risk management strategies and frameworks are informed by applicable international, national, and financial services industry standards and guidelines.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.RM-01
CRI.GV.RM-01.03	Risk Management Objectives Agreement.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-01.03: The organization has established, and maintains, technology and cybersecurity programs designed to protect the confidentiality, integrity and availability of its information and operational systems, commensurate with the organization's risk appetite and business needs.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.RM-01
CRI.GV.RM-01.04	Risk Management Objectives Agreement.04	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-01.04: Technology and cybersecurity risk management programs incorporate risk identification, measurement, monitoring, and reporting.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.RM-01

Control ID	Control Name	Control Description	Implementation Status	References	Issues	Assessed By	NIST CSF 2.0
CRI.GV.RM-01.05	Risk Management Objectives Agreement.05	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-01.05: The organization's technology, cybersecurity, resilience, and third-party risk management programs, policies, resources, and priorities are aligned and mutually supporting.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.RM-01
CRI.GV.RM-02.01	Risk Appetite & Risk Tolerance Statements.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-02.01: The governing authority (e.g., the Board or one of its committees) endorses and regularly reviews technology and cybersecurity risk appetite and is regularly informed about the status of, and material changes to, the organization's inherent risk profile.	Fully Implemented	NIST CSF 2.0 Assessment		Exec Mgmt, Governance	GV.RM-02
CRI.GV.RM-02.02	Risk Appetite & Risk Tolerance Statements.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-02.02: The organization has established statements of technology and cybersecurity risk tolerance consistent with its risk appetite, and has integrated them into technology, cybersecurity, operational, and enterprise risk management practices.	Fully Implemented	NIST CSF 2.0 Assessment		Exec Mgmt, Governance	GV.RM-02
CRI.GV.RM-02.03	Risk Appetite & Risk Tolerance Statements.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-02.03: Determination of the organization's risk appetite and tolerance includes consideration of the organization's stakeholder obligations, role in critical infrastructure, and sector-specific risk analysis.	Fully Implemented	NIST CSF 2.0 Assessment		Exec Mgmt, Governance	GV.RM-02
CRI.GV.RM-03.01	Enterprise Risk Integration.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-03.01: Technology and cybersecurity risk management frameworks and programs are integrated into the enterprise risk management framework.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.RM-03
CRI.GV.RM-03.02	Enterprise Risk Integration.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-03.02: The organization's business continuity and resilience strategy and program align with and support the overall enterprise risk management framework.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.RM-03
CRI.GV.RM-03.03	Enterprise Risk Integration.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-03.03: Technology and cybersecurity risk management and risk assessment processes are consistent with the organization's enterprise risk management policies, procedures, and methodologies and include criteria for the evaluation and categorization of enterprise-specific risks and threats.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.RM-03
CRI.GV.RM-03.04	Enterprise Risk Integration.04	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-03.04: Technology and cybersecurity risk management considerations are integrated into daily operations, cultural norms, management discussions, and management decision-making, and are tailored to address enterprise-specific risks (both internal and external).	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.RM-03
CRI.GV.RM-04.01	Risk Response Strategic Direction	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-04.01: The governing authority (e.g., the Board or one of its committees) and senior management provide guidance, direction, and credible challenge in the design and implementation of risk management strategies, assessment of identified risks against risk appetite and risk tolerance, and in the selection of risk treatment approaches.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.RM-04
CRI.GV.RM-05.01	Lines of Communication.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-05.01: The organization has a process for monitoring its technology, cybersecurity, and third-party risks, including escalating those risks that exceed risk appetite to management and identifying risks with the potential to impact multiple operating units.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	GV.RM-05
CRI.GV.RM-05.02	Lines of Communication.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-05.02: The organization establishes minimum requirements for its third-parties that include how the organizations will communicate and coordinate in times of emergency, including: 1) Joint maintenance of contingency plans; 2) Responsibilities for responding to incidents, including forensic investigations; 3) Planning and testing strategies that address severe events in order to identify single points of failure that would cause wide-scale disruption; and 4) Incorporating the potential impact of an incident into their BCM process and ensure resilience capabilities are in place.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	GV.RM-05
CRI.GV.RM-06.01	Standardized Risk Management Method	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-06.01: Technology and cybersecurity risk management and risk assessment processes and methodologies are documented and regularly reviewed and updated to address changes in the risk profile and risk appetite, the evolving threat environment, and new technologies, products, services, and interdependencies.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.RM-06
CRI.GV.RM-07.01	Strategic Opportunities	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RM-07.01: The organization has mechanisms in place to ensure that strategies, initiatives, opportunities, and emerging technologies (e.g., artificial intelligence, quantum computing, etc.) are evaluated both in terms of risks and uncertainties that are potentially detrimental to the organization, as well as potentially advantageous to the organization (i.e., positive risks).	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	GV.RM-07
CRI.GV.RR-03.01	Resource Adequacy.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RR-03.01: The organization's budgeting and resourcing processes identify, prioritize, and address resource needs to manage identified technology and cybersecurity risks (e.g., skill shortages, headcount, new tools, incident-related expenses, and unsupported systems).	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.RR-03
CRI.GV.RR-03.02	Resource Adequacy.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RR-03.02: The organization regularly assesses its skill and resource level requirements against its current personnel complement to determine gaps in resource need.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.RR-03
CRI.GV.RR-03.03	Resource Adequacy.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.RR-03.03: The organization provides adequate resources, appropriate authority, and access to the governing authority for the designated Cybersecurity Officer (e.g., CISO).	Fully Implemented	NIST CSF 2.0 Assessment		Governance	GV.RR-03
CRI.GV.SC-03.01	Supply Chain Risk Management Integration	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - GV.SC-03.01: The organization's third-party risk management strategy and program aligns with and supports its enterprise, technology, cybersecurity, and resilience risk management frameworks and programs.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Compliance, Governance	GV.SC-03
CRI.ID.IM-01.01	Continuous Improvements Evaluation.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.IM-01.01: Technology, cybersecurity, and resilience controls are regularly assessed and/or tested for design and operating effectiveness.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	ID.IM-01
CRI.ID.IM-01.02	Continuous Improvements Evaluation.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.IM-01.02: The organization implements a regular process to collect, store, report, benchmark, and assess trends in actionable performance indicators and risk metrics (e.g., threat KRIs, security incident metrics, vulnerability metrics, and operational measures).	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	ID.IM-01
CRI.ID.IM-01.03	Continuous Improvements Evaluation.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.IM-01.03: The organization establishes specific objectives, performance criteria, benchmarks, and tolerance limits to identify areas that have improved or are in need of improvement over time.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	ID.IM-01
CRI.ID.IM-01.04	Continuous Improvements Evaluation.04	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.IM-01.04: Technology and cybersecurity programs include elements designed to assess, manage, and continually improve the quality of program delivery in addressing stakeholder requirements and risk reduction.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	ID.IM-01
CRI.ID.IM-01.05	Continuous Improvements Evaluation.05	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.IM-01.05: The organization's third-party risk management program is regularly assessed, reported on, and improved.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Governance	ID.IM-01
CRI.ID.IM-03.01	Improvements from Lessons Learned.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.IM-03.01: A formal process is in place to improve protection controls and processes by integrating recommendations, findings, and lessons learned from exercises, testing. audits, assessments, and incidents.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	ID.IM-03
CRI.ID.IM-03.02	Improvements from Lessons Learned.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.IM-03.02: The organization establishes a systematic and comprehensive program to regularly evaluate and improve its monitoring and detection processes and controls as the threat environment changes, tools and techniques evolve, and lessons are learned.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	ID.IM-03
CRI.ID.IM-04.01	Plans Affecting Operations.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.IM-04.01: The organization's business continuity, disaster recovery, crisis management, and response plans are in place and managed, aligned with each other, and incorporate considerations of cyber incidents.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	ID.IM-04
CRI.ID.IM-04.02	Plans Affecting Operations.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.IM-04.02: The organization's incident response and business continuity plans contain clearly defined roles, responsibilities, and levels of decision-making authority, and include all needed areas of participation and expertise across the organization and key third-parties.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	ID.IM-04
CRI.ID.IM-04.03	Plans Affecting Operations.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.IM-04.03: Recovery plans include service resumption steps for all operating environments, including traditional, alternate recovery, and highly available (e.g., cloud) infrastructures.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	ID.IM-04
CRI.ID.IM-04.04	Plans Affecting Operations.04	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.IM-04.04: The organization has plans to identify, in a timely manner, the status of all transactions and member positions at the time of a disruption, supported by corresponding recovery point objectives.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	ID.IM-04
CRI.ID.IM-04.05	Plans Affecting Operations.05	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.IM-04.05: Recovery plans include restoration of resilience following a long term loss of capability (e.g., at an alternate site or a third-party), detailing when the plan should be activated and implementation steps.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	ID.IM-04
CRI.ID.IM-04.06	Plans Affecting Operations.06	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.IM-04.06: The organization has established and implemented plans to identify and mitigate the cyber risks it poses through interconnectedness to sector partners and external stakeholders.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	ID.IM-04
CRI.ID.IM-04.07	Plans Affecting Operations.07	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.IM-04.07: The organization pre-identifies, pre-qualifies, and retains third party incident management support and forensic service firms, as required, that can be called upon to quickly assist with incident response, investigation, and recovery.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	ID.IM-04

Control ID	Control Name	Control Description	Implementation Status	References	Issues	Assessed By	NIST CSF 2.0
CRI.ID.IM-04.08	Plans Affecting Operations.08	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.IM-04.08: The organization regularly reviews response strategy, incident management plans, recovery plans, and associated tests and exercises and updates them, as necessary, based on: (1) Lessons learned from incidents that have occurred (both internal and external to the organization); (2) Current cyber threat intelligence (both internal and external sources); (3) Recent and wide-scale cyber attack scenarios; (4) Operationally and technically plausible future cyber attacks; (5) Organizational or technical environment changes; and, (6) New technological developments.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	ID.IM-04
CRI.ID.RA-02.01	Information Sharing Forums.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-02.01: The organization participates actively (in alignment with its business operations, inherent risk, and complexity) in information-sharing groups and collectives (e.g., cross-industry, cross-government and cross-border groups) to gather, distribute and analyze information about cyber practices, cyber threats, and early warning indicators relating to cyber threats.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-02
CRI.ID.RA-02.02	Information Sharing Forums.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-02.02: The organization shares authorized information on its cyber resilience framework and the effectiveness of protection technologies bilaterally with trusted external stakeholders to promote the understanding of each party's approach to securing systems.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-02
CRI.ID.RA-03.01	Threat Identification.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-03.01: The organization, on an ongoing basis, identifies, analyzes, correlates, characterizes, and reports threats that are internal and external to the firm.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-03
CRI.ID.RA-03.02	Threat Identification.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-03.02: The organization solicits and considers threat intelligence received from the organization's stakeholders, service and utility providers, and other industry and security organizations.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-03
CRI.ID.RA-03.03	Threat Identification.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-03.03: The organization includes in its threat analysis those cyber threats which could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred in the past.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-03
CRI.ID.RA-03.04	Threat Identification.04	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-03.04: The organization regularly reviews and updates its threat analysis methodology, threat information sources, and supporting tools.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-03
CRI.ID.RA-04.01	Impact & Likelihood Analysis	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-04.01: The organization's risk assessment approach includes the analysis and characterization of the likelihood and potential business impact of identified risks being realized.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-04
CRI.ID.RA-05.01	Risk Exposure Determination & Prioritization.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-05.01: Threats, vulnerabilities, likelihoods, and impacts are used to determine overall technology, cybersecurity, and resilience risk to the organization.	Fully Implemented	NIST CSF 2.0 Assessment		Exec Mgmt	ID.RA-05
CRI.ID.RA-05.02	Risk Exposure Determination & Prioritization.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-05.02: The organization has established threat modeling capabilities to identify how and why critical assets might be compromised by a threat actor, what level of protection is needed for those critical assets, and what the impact would be if that protection failed.	Fully Implemented	NIST CSF 2.0 Assessment		Exec Mgmt	ID.RA-05
CRI.ID.RA-05.03	Risk Exposure Determination & Prioritization.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-05.03: The organization's business units assess, on an ongoing basis, the technology, cybersecurity, and resilience risks associated with the activities of the business unit.	Fully Implemented	NIST CSF 2.0 Assessment		Exec Mgmt	ID.RA-05
CRI.ID.RA-05.04	Risk Exposure Determination & Prioritization.04	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-05.04: The organization uses scenario planning, table-top-exercises, or similar event analysis techniques to identify vulnerabilities and determine potential impacts to critical infrastructure, technology, and business processes.	Fully Implemented	NIST CSF 2.0 Assessment		Exec Mgmt	ID.RA-05
CRI.ID.RA-06.01	Risk Response Determination.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-06.01: Technology and cybersecurity risk management programs and risk assessment processes produce actionable recommendations that the organization uses to select, design, prioritize, implement, maintain, evaluate, and modify cybersecurity and technology controls.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-06
CRI.ID.RA-06.02	Risk Response Determination.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-06.02: The implementation of responses to address identified risks (i.e., risk avoidance, risk mitigation, risk acceptance, or risk transfer (e.g., cyber insurance)) are formulated, assessed, documented, and prioritized based on criticality to the business.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-06
CRI.ID.RA-06.03	Risk Response Determination.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-06.03: Technology and cybersecurity programs identify and implement controls to manage applicable risks within the risk appetite set by the governing authority (e.g., the Board or one of its committees).	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-06
CRI.ID.RA-06.04	Risk Response Determination.04	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-06.04: The organization assesses the threats, impacts, and risks that could adversely affect the organization's ability to provide services on an ongoing basis, and develops its resilience requirements and plans to address those risks.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-06
CRI.ID.RA-06.05	Risk Response Determination.05	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-06.05: The organization defines and implements standards and procedures to prioritize and remediate issues identified in vulnerability scanning or penetration testing, including emergency or zero-day threats and vulnerabilities.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-06
CRI.ID.RA-06.06	Risk Response Determination.06	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-06.06: The organization follows documented procedures, consistent with established risk response processes, for mitigating or accepting the risk of vulnerabilities or weaknesses identified in exercises and testing or when responding to incidents.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-06
CRI.ID.RA-07.01	Change & Exception Management.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-07.01: The organization defines and implements change management standards and procedures, to include emergency change procedures, that explicitly address risk identified both prior to and during a change, any new risk created post-change, as well as the reviewing and approving authorities (e.g., change advisory boards).	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-07
CRI.ID.RA-07.02	Change & Exception Management.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-07.02: Risk-based criteria are used to categorize each system change, to include emergency changes, to determine the necessary change process standards to apply for change planning, rollback planning, pre-change testing, change access control, post-change verification, and change review and approval.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-07
CRI.ID.RA-07.03	Change & Exception Management.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-07.03: Technology projects and system change processes ensure that requisite changes in security posture, data classification and flows, architecture, support documentation, business processes, and business resilience plans are addressed.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-07
CRI.ID.RA-07.04	Change & Exception Management.04	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-07.04: Policy exceptions, risk mitigation plans, and risk acceptances resulting from assessments and evaluations, such as testing, exercises, audits, etc., are formally managed, approved, escalated to defined levels of management, and tracked to closure.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-07
CRI.ID.RA-07.05	Change & Exception Management.05	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - ID.RA-07.05: The organization establishes and maintains an exception management process for identified vulnerabilities that cannot be mitigated within target timeframes.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	ID.RA-07
CRI.PR.AA-02.01	Identity Binding to Credentials	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - PR.AA-02.01: The organization authenticates identity, validates the authorization level of a user before granting access to its systems, limits the use of an account to a single individual, and attributes activities to the user in logs and transactions.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	IT Security	PR.AA-02
CRI.PR.AA-03.01	Authentication.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - PR.AA-03.01: Based on the risk level of a user access or a specific transaction, the organization defines and implements authentication requirements, which may include multi-factor or out-of-band authentication, and may adopt other real-time risk prevention or mitigation tactics.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	PR.AA-03
CRI.PR.AA-03.02	Authentication.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - PR.AA-03.02: Decisions to authorize user access to devices and other assets are made with consideration of: (1) Business need for the access; (2) The type of data being accessed (e.g., customer PII, public data); (3) The risk of the transaction (e.g., internal-to-internal, external-to-internal); (4) The organization's level of trust for the accessing agent (e.g., external application, internal user); and (5) The potential for harm.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	PR.AA-03
CRI.PR.AA-03.03	Authentication.03	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - PR.AA-03.03: The organization reduces fraudulent activity and protects reputational integrity through email verification mechanisms (e.g., DMARC, DKIM), call-back verification, secure file exchange facilities, out-of-band communications, customer outreach and education, and other tactics designed to thwart imposters and fraudsters.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	PR.AA-03
CRI.PR.AA-04.01	Identity Assertions	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - PR.AA-04.01: Access credential and authorization mechanisms for internal systems and across security perimeters (e.g., leveraging directory services, directory synchronization, single sign-on, federated access, credential mapping, etc.) are designed to maintain security, integrity, and authenticity.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	IT Security	PR.AA-04
CRI.PR.AA-06.01	Physical Access.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - PR.AA-06.01: The organization manages, protects, and logs physical access to sensitive areas, devices, consoles, equipment, and network cabling and infrastructure.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	PR.AA-06
CRI.PR.AA-06.02	Physical Access.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - PR.AA-06.02: The organization manages and protects physical and visual access to sensitive information assets and physical records (e.g., session lockout, clean desk policies, printer/facsimile output trays, file cabinet/room security, document labelling, etc.)	Fully Implemented	NIST CSF 2.0 Assessment		Operations	PR.AA-06
CRI.PR.DS-10.01	Protection of Data in Use	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - PR.DS-10.01: Data-in-use is protected commensurate with the criticality and sensitivity of the information and in alignment with the data classification and protection policy (e.g., through the use of encryption, authentication, access control, masking, tokenization, visual shielding, memory integrity monitoring, etc.)	Fully Implemented	NIST CSF 2.0 Assessment		Data Protection	PR.DS-10

Control ID	Control Name	Control Description	Implementation Status	References	Issues	Assessed By	NIST CSF 2.0
CRI.PR.IR-02.01	Environmental Threat Protections	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - PR.IR-02.01: The organization designs, documents, implements, tests, and maintains environmental and physical controls to meet defined business resilience requirements (e.g., environmental monitoring, dual power and communication sources, regionally separated backup processing facilities, etc.)	Fully Implemented	NIST CSF 2.0 Assessment		Operations	PR.IR-02
CRI.PR.IR-03.01	Resilience Measures	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - PR.IR-03.01: The organization implements mechanisms (e.g., failsafe, load balancing, hot swaps, redundant equipment, alternate services, backup facilities, etc.) to achieve resilience requirements in normal and adverse situations.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	Operations	PR.IR-03
CRI.PR.IR-04.01	Capacity Management.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - PR.IR-04.01: Baseline measures of network and system utilization and transaction activity are captured to support capacity planning and anomalous activity detection.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	PR.IR-04
CRI.PR.IR-04.02	Capacity Management.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - PR.IR-04.02: Technology availability and capacity is planned, monitored, managed, and optimized to meet business resilience objectives and reasonably anticipated infrastructure demands.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	PR.IR-04
CRI.RC.CO-03.01	Recovery Activity Communication.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RC.CO-03.01: The organization timely involves and communicates the recovery activities, procedures, cyber risk management issues to the governing body (e.g., the Board or one of its committees), senior management, incident management support teams, and relevant internal stakeholders.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	RC.CO-03
CRI.RC.CO-03.02	Recovery Activity Communication.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RC.CO-03.02: The organization promptly communicates the status of recovery activities to regulatory authorities and relevant external stakeholders, as required or appropriate.	Fully Implemented	NIST CSF 2.0 Assessment		Governance	RC.CO-03
CRI.RC.RP-01.01	Recovery Plan Execution	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RC.RP-01.01: The organization executes its recovery plans, including incident recovery, disaster recovery, and business continuity plans, during or after an incident to resume operations.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	RC.RP-01
CRI.RC.RP-02.01	Recovery Action Performance.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RC.RP-02.01: The organization's response plans are used as informed guidance to develop and manage task plans, response actions, priorities, and assignments for responding to incidents, but are adapted as necessary to address incident-specific characteristics.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	RC.RP-02
CRI.RC.RP-02.02	Recovery Action Performance.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RC.RP-02.02: Recovery plans are executed by first resuming critical services and core business functions, while minimizing any potential concurrent and widespread interruptions to interconnected entities and critical infrastructure, such as energy and telecommunications.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	RC.RP-02
CRI.RC.RP-04.01	Post-Incident Operational Norms	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RC.RP-04.01: Restoration steps include the verification of data integrity, transaction positions, system functionality, and the operation of security controls by appropriate organizational stakeholders and system owners.	Fully Implemented	NIST CSF 2.0 Assessment		Operations	RC.RP-04
CRI.RC.RP-05.01	Asset Integrity Restoration.01	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RC.RP-05.01: The organization maintains documented procedures for sanitizing, testing, authorizing, and returning systems to service following an incident or investigation.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	IT Security	RC.RP-05
CRI.RC.RP-05.02	Asset Integrity Restoration.02	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RC.RP-05.02: Business, technology, cybersecurity, and relevant third-party stakeholders confirm that systems, data, and services have been returned to functional and secure states and that a stable operational status has been achieved.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	IT Security	RC.RP-05
CRI.RC.RP-06.01	End-of-Incident Determination	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RC.RP-06.01: Incident management activities are closed under defined conditions and documentation to support subsequent post-mortem review, process improvement, and any follow-on activities is collected and verified.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	IT Security	RC.RP-06
CRI.RS.AN-06.01	Investigation Documentation	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RS.AN-06.01: The organization establishes a risk-based approach and procedures for quarantining systems, conducting investigations, and collecting and preserving evidence per best practices and forensic standards.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	RS.AN-06
CRI.RS.AN-07.01	Incident Data Collection & Preservation	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RS.AN-07.01: Incident-related forensic data is captured, secured, and preserved in a manner supporting integrity, provenance, and evidentiary value.	Not Implemented	NIST CSF 2.0 Assessment, NIST CSF 2.0 Plan of Action and Milestones	Control not implemented.	IT Security	RS.AN-07
CRI.RS.AN-08.01	Incident Magnitude Determination	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RS.AN-08.01: Available incident information is assessed to determine the extent of impact to the organization and its stakeholders, the potential near- and long-term financial implications, and whether or not the incident constitutes a material event.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	RS.AN-08
CRI.RS.MA-02.01	Incident Triage & Validation	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RS.MA-02.01: Tools and processes are in place to ensure timely detection, inspection, assessment, and analysis of security event data for reliable activation of incident response processes.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	RS.MA-02
CRI.RS.MA-03.01	Incident Categorization & Prioritization	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RS.MA-03.01: The organization categorizes and prioritizes cybersecurity incident response consistent with response plans and criticality of systems and services to the enterprise.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	RS.MA-03
CRI.RS.MA-04.01	Incident Escalation	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RS.MA-04.01: Response activities are centrally coordinated, response progress and milestones are tracked and documented, and new incident information is assimilated into ongoing tasks, assignments, and escalations.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	RS.MA-04
CRI.RS.MI-01.01	Incident Containment	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RS.MI-01.01: The organization has established processes to implement vulnerability mitigation plans, involve third-party partners and outside expertise as needed, and contain incidents in a timely manner.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	RS.MI-01
CRI.RS.MI-02.01	Incident Eradication	NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - RS.MI-02.01: Targeted investigations and actions are taken to ensure that all vulnerabilities, system components, devices, or remnants used or leveraged in an attack (e.g., malware, compromised accounts, open ports, etc.) are removed or otherwise returned to a secure and reliable state, or that plans to address the vulnerabilities are documented.	Fully Implemented	NIST CSF 2.0 Assessment		IT Security	RS.MI-02