Function	Category		Subcategory	Implemented?	Responsible	Metric	Value Assesed	Audit Comments
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.	1	**ID.AM-1**: Physical devices and systems within the organization are inventoried					
		2	**ID.AM-2:** Software platforms and applications within the organization are inventoried					
		3	**ID.AM-3:** Organizational communication and data flows are mapped					
		4	**ID.AM-4:** External information systems are catalogued					
		5	**ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value					
		6	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established					
	Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	7	**ID.BE-1:** The organization’s role in the supply chain is identified and communicated					
		8	**ID.BE-2:** The organization’s place in critical infrastructure and its industry sector is identified and communicated					
		9	**ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated					
		10	**ID.BE-4**: Dependencies and critical functions for delivery of critical services are established					
		11	**ID.BE-5**: Resilience requirements to support delivery of critical services are established					

	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	12	**ID.GV-1:** Organizational information security policy is established					
		13	**ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners					
		14	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed					
		15	**ID.GV-4**: Governance and risk management processes address cybersecurity risks					
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	16	**ID.RA-1:** Asset vulnerabilities are identified and documented					
		17	**ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources					
		18	**ID.RA-3:** Threats, both internal and external, are identified and documented					
		19	**ID.RA-4:** Potential business impacts and likelihoods are identified					
		20	**ID.RA-5**: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk					
		21	**ID.RA-6:** Risk responses are identified and prioritized					
	Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	22	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders					
		23	**ID.RM-2:** Organizational risk tolerance is determined and clearly expressed					
		24	**ID.RM-3**: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis					
		25	**PR.AC-1:** Identities and credentials are managed for authorized devices and users					

	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	26	**PR.AC-2:** Physical access to assets is managed and protected					
		27	**PR.AC-3:** Remote access is managed					
		28	**PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties					
		29	**PR.AC-5:** Network integrity is protected, incorporating network segregation where appropriate					
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	30	**PR.AT-1:** All users are informed and trained					
		31	**PR.AT-2:** Privileged users understand roles & responsibilities					
		32	**PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities					
		33	**PR.AT-4:** Senior executives understand roles & responsibilities					
		34	**PR.AT-5:** Physical and information security personnel understand roles & responsibilities					
		35	**PR.DS-1:** Data-at-rest is protected					

PROTECT (PR)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	36	**PR.DS-2:** Data-in-transit is protected					
		37	**PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition					
		38	**PR.DS-4:** Adequate capacity to ensure availability is maintained					
		39	**PR.DS-5:** Protections against data leaks are implemented					
		40	**PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity					
		41	**PR.DS-7:** The development and testing environment(s) are separate from the production environment					
	Information Protection Processes and Procedures (PR.IP): Security policies (that	42	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained					
		43	**PR.IP-2:** A System Development Life Cycle to manage systems is implemented					
		44	**PR.IP-3:** Configuration change control processes are in place					
		45	**PR.IP-4:** Backups of information are conducted, maintained, and tested periodically					
		46	**PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met					

	address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	47	**PR.IP-6:** Data is destroyed according to policy					
		48	**PR.IP-7:** Protection processes are continuously improved					
		49	**PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties					
		50	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed					
		51	**PR.IP-10:** Response and recovery plans are tested					
		52	**PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)					
		53	**PR.IP-12:** A vulnerability management plan is developed and implemented					
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	54	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools					
		55	**PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access					
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	56	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy					
		57	**PR.PT-2:** Removable media is protected and its use restricted according to policy					
		58	**PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least					

			functionality					
		59	**PR.PT-4:** Communications and control networks are protected					
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	60	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed					
		61	**DE.AE-2:** Detected events are analyzed to understand attack targets and methods					
		62	**DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors					
		63	**DE.AE-4:** Impact of events is determined					
		64	**DE.AE-5:** Incident alert thresholds are established					
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	65	**DE.CM-1:** The network is monitored to detect potential cybersecurity events					
		66	**DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events					
		67	**DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events					
		68	**DE.CM-4:** Malicious code is detected					
		69	**DE.CM-5:** Unauthorized mobile code is detected					
		70	**DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events					
		71	**DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed					
		72	**DE.CM-8:** Vulnerability scans are performed					

	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	73	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability					
		74	**DE.DP-2:** Detection activities comply with all applicable requirements					
		75	**DE.DP-3:** Detection processes are tested					
		76	**DE.DP-4:** Event detection information is communicated to appropriate parties					
		77	**DE.DP-5:** Detection processes are continuously improved					
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	78	**RS.RP-1:** Response plan is executed during or after an event					
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	79	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed					
		82	**RS.CO-2:** Events are reported consistent with established criteria					
		83	**RS.CO-3:** Information is shared consistent with response plans					
		84	**RS.CO-4:** Coordination with stakeholders occurs consistent with response plans					
		85	**RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness					
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	86	**RS.AN-1:** Notifications from detection systems are investigated					
		87	**RS.AN-2:** The impact of the incident is understood					
		88	**RS.AN-3:** Forensics are performed					

		88	**RS.AN-3:** Forensics are performed					
		89	**RS.AN-4:** Incidents are categorized consistent with response plans					
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	90	**RS.MI-1:** Incidents are contained					
		91	**RS.MI-2:** Incidents are mitigated					
		92	**RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks					
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	93	**RS.IM-1:** Response plans incorporate lessons learned					
		94	**RS.IM-2:** Response strategies are updated					
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	95	**RC.RP-1:** Recovery plan is executed during or after an event					
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	96	**RC.IM-1:** Recovery plans incorporate lessons learned					
		97	**RC.IM-2:** Recovery strategies are updated					
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	98	**RC.CO-1:** Public relations are managed					
		99	**RC.CO-2:** Reputation after an event is repaired					
		100	**RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams					