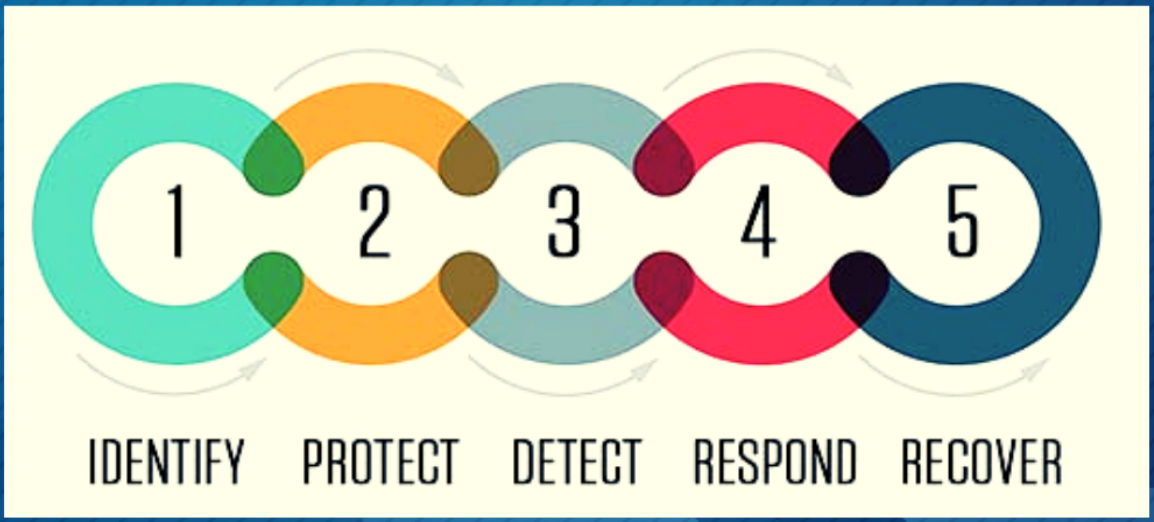
MINISTRY OF SECURITY

ULTIMATE NIST CSF CHECKLIST



Function	Category	Subcategory	Guidance	Artefacts to evidence
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.**	ID.AM-1: Physical devices and systems within the organization are inventoried	Document and implement a formal Asset Management Policy that establishes assets inventory and methods of inventory whether it is conducted manually or with help of automatic tools.	Asset Management Policy
			For each asset organization must document sufficient information to identify the asset, its physical (or logical) location, and information security classification.	Asset Inventory
			The organization will maintain a current inventory of all hardware (including operating systems) including type, publisher, version, location or workforce members-assignment, in-service date, and retirement/disposal date.	Comprehensive network diagram that includes allowed ports, protocols and services.
			Inventories should be reviewed to ensure that all firmware versions are current and supported by the publisher with security updates.	Asset Inventory with versions of firmware
		ID.AM-2: Software platforms and applications within the organization are inventoried	Define, document and implement procedures for handling unauthorized software. The software should be either approved or eliminated by the administrator.	Software Asset Management Policy
			The organization will maintain a current inventory of all software (including operating systems) including type, publisher, version, location or workforce members-assignment, in-service date, and retirement/disposal date.	Software Asset Inventory
			Inventories should be reviewed to ensure that all software versions are current and supported by the publisher with security updates.	Software Asset Inventory
		ID.AM-3: Organizational communication and data flows are mapped	Document all connections within the organization, and between departments. All connections must be documented, authorized, and reviewed. Connection information includes, for example, the interface characteristics, data characteristics, ports, protocols, addresses, description of the data, security requirements, and the nature of the connection.	Data Flow diagram
			Establish and document guidelines for electronic messaging usage which make users aware of what deems as acceptable and unacceptable use of its corporate messaging process.	End user policy & guidelines

			Create and implement Acceptable Use Policy, include these guidelines into the policy.	Acceptable Use Policy
			Diagram organizational communications flows, including cloud services.	Network and Logical diagram / Data Flow Diagrams
		ID.AM-4: External information systems are catalogued	Inventory cloud services and other external systems.	Cloud Asset Inventory
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Develop and implement information classification based on impact level classification. Information should be classified based on its value.	Information Classification Standard
			Classification guidelines should take into account impact from loss of integrity, availability and confidentiality of the information.	Information Classification Standard
			Implement formal procedures describing prioritization of organizational assets based on their importance to organizational systems	Asset Classification & Valuation Procedure
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Establish strict requirements that obligates each policy to contain cybersecurity roles. Roles have to be widely communicated to all relevant parties.	Information Security Roles & Responsibilities
			Third-party providers are required to notify the organization of any personnel transition (including transfers or terminations) involving personnel with physical or logical access to the production system components.	Security Awareness and Training Policy
	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.	ID.BE-1: The organization's role in the supply chain is identified and communicated	Ensure the supplier management policy is defined.	Supplier Security Management Policy
			Define information security requirements to apply to product or service acquisition in addition to the general requirements for supplier relationships	Supplier Security Management Procedure
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	Define, document and communicate critical infrastructure and key resources relevant to the company's production activity.	BC-DR Recovery Document
			Develop, document, and maintain a critical infrastructure and key resources protection plan.	BC-DR Recovery Document
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	Establish and communicate priorities for production activities, missions, objectives, with consideration for	Information security policy aligned with the organization's vision and mission.

			security. Make sure cybersecurity priorities align with business needs and priorities.	
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Write down procedures describing all alternate power support services. Establish regular ability and capacity testing of alternative support services.	BC-DR procedure
		ID.BE-5: Resilience requirements to support delivery of critical services are established	Conduct contingency planning for the continuance of essential production functions and services with little or no loss of operational continuity, and sustain that continuity until full system restoration.	BC-DR Plan
			Communicate that planning to all relevant parties, so that they are aware of their roles, responsibilities and procedures.	Email Communication Artifacts with R&R
	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.	ID.GV-1: Organizational information security policy is established	Establish an organizational information security policy	Information Security Policy
			Divide security rules into several policies like Access Control Policy, Classification Policy, Backup Policy, Acceptable Use Policy, etc. – this way such policies will be shorter (and therefore easier to read and understand), and easier to maintain. Policies must include, for example, the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	Information Security Policy
			Establish and communicate existing cybersecurity policies to all relevant parties.	Email Communication Artifacts with R&R
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	Describe and establish cybersecurity roles, responsibilities and procedures related to internal roles within the whole organization and external partners.	Roles & Responsibilities for internal & external stakeholders
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Identify and document all legal and regulatory requirements regarding cybersecurity.	Legal & regulatory requirements as captured in InfoSec policy
			Make sure that requirements related to legal and regulatory requirements affecting the production operations regarding cybersecurity are understood, managed and widely communicated between all relevant departments.	Artifacts of communication

		ID.GV-4: Governance and risk management processes address cybersecurity risks	Establish Risk Management Process; Create a Risk Management Framework document that would contain risk factors: threats, vulnerabilities, impacts, likelihoods, risk levels matrix. These factors are important for the organization to document prior to conducting risk assessment because the assessment relies upon well-defined attributes of threats, vulnerabilities, impact, and other risk factors to effectively determine risk.	Risk Management Process
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	Define and document Vulnerability Management process for assets defining roles & responsibilities.	Vulnerability Management Process
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	Consider the possibility of receiving cyber threat intelligence. Threat intelligence feeds take security data from vendors, analysts and other sources about threats and unusual activity happening all around the world. Malicious IP addresses, domains, file hashes and other data stream in constantly from external parties.	Artifacts of subscription to forums/newsletters etc
		ID.RA-3: Threats, both internal and external, are identified and documented	Conduct Vulnerability Scanning against internal environment(ESXi servers, users laptops: Windows OS, Mac OS, GNU/Linux) Conduct Penetration test and remediation testing of both infrastructure and web applications annually.	VA-PT reports
		ID.RA-4: Potential business impacts and likelihoods are identified	Develop potential business impacts and likelihood ranges within the risk assessment process.	Risk Assessment Methodology
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Define, document and implement a formal risk assessment process.	Risk Assessment Methodology
		ID.RA-6: Risk responses are identified and prioritized	Identify and prioritize risk responses within the risk assessment process.	Risk Assessment Methodology
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	Establish Risk Management Process; Create Risk Management Framework document that would contain risk factors: threats, vulnerabilities, impacts, likelihoods, risk levels matrix. These factors are important for the organization to document prior to conducting risk assessment because the assessment rely upon well-defined attributes of threats, vulnerabilities,	Risk Management Process

			impact, and other risk factors to effectively determine risk.	
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	Adjust Risk Assessment Framework so that it includes the criteria for accepting risk and identifying the acceptable level of (e.g. at what level can risk automatically be accepted and under what circumstances).	Risk Assessment Framework
			Approval should be obtained from top management for the decision to accept residual risks, and authorization obtained for the actual operation of the ISMS.	Management Approval/MoM
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	To maximize the benefit of risk assessments, the organization should establish policies, procedures, and implementing mechanisms to ensure that the information produced during such assessments is effectively communicated and shared across all risk management tiers.	Risk Assessment Framework
PROTECT (PR)	**Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.**	PR.AC-1: Identities and credentials are managed for authorized devices and users	Define, document and implement a process for asset owners to review access rights to their assets on a regular basis. Review and verify processes with all relevant parties.	Access Control Policy
		PR.AC-2: Physical access to assets is managed and protected	Define, document and implement procedures in Access Control Policy that would describe roles and responsibilities related to physical access.	Access Control Policy
		PR.AC-3: Remote access is managed	Define and establish remote working/teleworking policy	Teleworking policy
			Allow remote access only through approved and managed access points;	User Access Management Policy for Remote Access
			Monitor remote access to the production system.	User Access Management Policy for Remote Access
			Allow only authorized use of privileged functions from remote access.	User Access Management Policy for Remote Access
			Establish agreements and verify security for connections with external systems.	User Access Management Policy for Remote Access
		PR.AC-4: Access permissions are managed, incorporating the	Incorporate principle of least privilege, segregation of duties, role based access	User Access Management Policy

		principles of least privilege and separation of duties	Regularly review user access rights of all critical assets and other assets of the organization	User Access Management Policy
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	Incorporate network segmentation where applicable via VLAN, DMZ.	Network Security Policy & Network Diagram
	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.	PR.AT-1: All users are informed and trained	Define, document and implement Security Awareness and Training Policy that defines scope, procedures, topics, roles and responsibilities in terms of Security Awareness and Training Program.	Security awareness presentation
			Implement an information security workforce development and improvement programs which include, for example: defining the knowledge and skill levels needed to perform information security duties and tasks;	Security assessment results
			Use anecdotes from actual information security incidents in user awareness training as examples of what could happen, how to respond to such incidents and how to avoid them in the future.	Security awareness presentation
		PR.AT-2: Privileged users understand roles & responsibilities	Establish specific cybersecurity awareness and training procedures for privileged users (e.g. developers) describing acceptable and unacceptable activities at the workplace.	Roles & Responsibilities
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	Define cybersecurity roles and responsibilities within Security Awareness and Training Policy.	Roles & Responsibilities
		PR.AT-4: Senior executives understand roles & responsibilities	Define cybersecurity roles and responsibilities within Security Awareness and Training Policy.	Roles & Responsibilities
	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.	PR.DS-1: Data-at-rest is protected	Create and implement procedures which describe how to encrypt all data of the organization.	Data encryption process
		PR.DS-2: Data-in-transit is protected	Create and implement procedures which will describe how data should be transferred. For example which corporate messenger employees should use for communication or how to correct obfuscated data before transfer or how to choose a protected way for transferring data.	Data transfer procedure/Data protection policy

			Conduct trade-off analysis of data protection solutions with policies that enable user prompting, blocking, or automatic encryption for sensitive data in transit, such as when files are attached to an email message or moved to cloud storage, removable drives, or transferred elsewhere.	Data Protection Policy Encryption in Data in Transit
			Ensure your Information Classification Policy requires classifying all company data, no matter where it resides, in order to ensure that the appropriate data protection measures are applied while data remains at rest and triggered when data is accessed, used, or transferred.	Information Classification policy
			Implement SSL/TLS encryption for all HTTP transactions.	Network Security Policy Encryption in Data in Transit
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Document roles, responsibilities and procedures within Asset Disposal Process.	Asset disposal process
			Create procedures that describe the secure formatting of data from each media drive.	Asset disposal process Asset Destruction Certificates
		PR.DS-4: Adequate capacity to ensure availability is maintained	Create and implement procedures which will describe how to monitor and maintain the capacity and availability of both internal and external infrastructure.	Capacity Management Policy
			Conduct regular performance and load tests for both internal and external infrastructure.	Capacity Management Records
		PR.DS-5: Protections against data leaks are implemented	Conduct incorporating DLP solutions to implement protections against data leaks	Data Protection Policy DLP Implementation
			Create and document procedures defining correct equipment maintenance outside the organization's premises	Equipment Maintenance SOP
			Confidential information must be protected with Full Disk Encryption. You can include these procedures into Acceptable Usage Policy.	Acceptable Use Policy
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Define, document and implement procedures for handling unauthorized software. The software should be whether approved or eliminated by the administrator;	Secure Software Development Policy
		PR.DS-7: The development and testing environment(s) are separate from the production environment	Implement fully functional testing environments, so that test cases can be performed without fear of causing damage to the production environment.	Secure Software Development Policy Test Environment

	Information Protection Processes and Procedures (PR.IP): Security policies (that 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.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	Develop, document, and maintain a baseline configuration for the organization.	Baseline configuration document
			Configure the production to provide only essential capabilities;	Secure Software Development Policy
			Review and update the baseline configuration and disable unnecessary capabilities;	Secure Software Development Policy
			Focus on securing the highest privilege accounts and groups. You should do so because they can be leveraged by attackers to compromise and even destroy your Active Directory installation.	User Access Management Policy
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	Consider use of Secure Code Development practices where appropriate.	Secure code development guidelines
			Create and implement Software Development Life Cycle (SDLC) Policy that would describe the requirements for developing and/or implementing new software and systems.	SDLC policy
		PR.IP-3: Configuration change control processes are in place	Develop a change management policy along with detailed procedures describing: - Conduct security impact analysis in connection with change control reviews. - Conduct security impact analysis in a separate test environment before implementation into an operational environment for planned changes to the production. - Review and authorize proposed configuration-controlled changes prior to implementing them in the production environment.	Change Management policy
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	Create and implement Backup Policy which will describe backup procedures, retention periods, types of backups, scope, roles and responsibilities.	Backup policy
			Conduct periodic Backup restoration testing	Backup restoration testing reports
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	Define, implement, and enforce policy and regulations regarding emergency and safety systems, fire protection systems, and environment controls.	Physical Security Policy
			Implement secondary commercial power supply like UPS and/or diesel generators.	Physical Security Policy Secondary Source of Power

		PR.IP-6: Data is destroyed according to policy	Ensure that organization system data is destroyed according to policy.	Data destruction policy
			Implement regular testing of effectiveness of technical data destruction mechanisms, how they are measured and evaluated.	Data destruction procedures
		PR.IP-7: Protection processes are continuously improved	Implement The Follow-up Phase within your Incident Response policies that would represent the review of the Security Incident to look for “lessons learned” and to determine whether the process that was followed could have been improved in any way.	Incident Response Procedure
			Security Events and Security Incidents should be reviewed after identification resolution to determine where response could be improved.	Incident Response Procedure
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	Share information about security incidents and mitigation measures with designated sharing partners;	Incident Communication Plan
			Use automated mechanisms where feasible to assist in information collaboration.	Incident Communication Plan
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Plans must incorporate recovery objectives, restoration priorities, metrics, contingency roles, personnel assignments and contact information.	Incident Response Plan / Business Continuity Plan
			Conduct regular (quarterly) review of Incident Response and Disaster Recovery plans to keep them up-to-date.	IR/BCP/DR Test Calendar IR/BCP/DR Test Records
		PR.IP-10: Response and recovery plans are tested	Conduct regular testing of response and recovery plans, make records, evaluate effectiveness.	Test reports of the DR plans
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Define, document and implement Onboarding Policy.	HR policy/Onboarding policy
			Include personnel screening procedures within the policy.	BGV policy
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	Document and communicate procedures of maintenance and repairs to all relevant stakeholders. For example, to prevent data leakage check whether full disk encryption is enabled or hard drive is removed before sending the laptop to repair service.	Equipment Maintenance SOP
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Establish, implement and communicate formal procedures which would describe how the organization: - Approves and monitors nonlocal maintenance and diagnostic activities;	Remote Access Policy

			- Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; - Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; - Maintains records for nonlocal maintenance and diagnostic activities; - Terminates session and network connections when nonlocal maintenance is completed.	
			Unify procedures into Remote Maintenance Policy or include them into Acceptable Use Policy.	Acceptable Use Policy
	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.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Create and implement a policy which will describe how to contain information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or organizational components associated with the event.	Log Monitoring Policy
		PR.PT-2: Removable media is protected and its use restricted according to policy	Create and implement a policy which would describe how to protect and control portable storage devices containing critical data while in transit and in storage.	Removable media policy
			Scan all portable storage devices for malicious content before they are used within the organization.	Asset Management policy with Removable Media Security
			Consider restricting the use of portable storage devices within the departments where appropriate.	Asset Management policy with Removable Media Security
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	Ensure criteria used for granting access privileges is based on the principle of “least privilege” whereby authorized users will only be granted access to information system and network domains which are necessary for them to carry out the responsibilities of their company role or function.	Access Control Policy
			Relying on CI/CD best practices, developers are not expected to be experts at operations concerns. Assign one Application Operator who would have permissions to manage the continuous delivery process for apps. Deny collective decision-making in the process of a release.	Secure Software Development Policy

			Follow the least functionality principle. Document procedures within Access Control Policy.	User Access Control Policy
		PR.PT-4: Communications and control networks are protected	Continuously monitor the communications and control networks and ensure they are always updated with best practices and controls.	Log Monitoring Policy Network Monitoring Records
			Eliminate incoming or outgoing traffic if it doesn't align with business goals.	Log Monitoring Policy Network Monitoring Records
			Ensure that there are no publicly accessible cloud instances	Log Monitoring Policy
DETECT (DE)	**Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.**	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Implement automated mechanisms that help the organization maintain consistent baseline configurations for information systems include, for example: - hardware and software inventory tools, - configuration management tools, - network management tools.	IS Baseline Documents
		DE.AE-2: Detected events are analysed to understand attack targets and methods	Events should be collected and forwarded to log management solutions so that administrators can analyse suspicious events.	Log Monitoring Policy Log Monitoring Rules
			Events should be collected from internal Windows Servers, Domain Controllers, etc and also from external facing servers and applications and customer applications.	Log Monitoring Policy Log Monitoring Rules
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	Consider implementing correlation rules within your log management solutions to automate threat detection and log analysis. Consider acquiring a SIEM solution.	Log Monitoring Policy Log Monitoring Rules
			Ensure that event data is compiled and correlated across the organization system using various sources such as event reports, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.	Log Monitoring Policy Log Monitoring Rules
			Integrate analysis of events where feasible with the analysis of vulnerability scanning information; performance data; production systems monitoring, and facility monitoring to further enhance the ability to identify inappropriate or unusual activity.	Log Monitoring Policy Log Monitoring Rules
		DE.AE-4: Impact of events is determined	Test ability and effectiveness of Priority Matrix to measure the influence on the business on a regular basis.	Incident Priority Matrix

			Share effectiveness with relevant stakeholders.	Incident Reporting
		DE.AE-5: Incident alert thresholds are established	Establish the incident threshold matrix along with the expected time of resolution.	Incident Priority Matrix
			Monitor and optimize Expected time to resolution.	Incident Management Policy
	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.	DE.CM-1: The network is monitored to detect potential cybersecurity events	Implement correlation rules within the log management solutions to automate threat detection and log analysis. Consider acquiring a SIEM solution.	Log Monitoring Policy Log Monitoring Rules
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Define, document and implement procedures in Access Control Policy that would describe roles and responsibilities related to physical access.	Access Control Policy
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Implement correlation rules within the log management solutions to automate threat detection and log analysis. Consider acquiring a SIEM solution. SIEM solution involves installing forwarders on users workstation. Logs are forwarded from workstation to SIEM.	Log Monitoring Policy Log Monitoring Rules
		DE.CM-4: Malicious code is detected	Regularly update the anti-virus. Testing of antivirus endpoint protection must be conducted based on conventional criteria.	Endpoint Security Policy Antivirus Monitoring Records
		DE.CM-5: Unauthorized mobile code is detected	Create and implement a policy which will describe how to use Mobile Code Security.	Endpoint Security Policy
			Establish a process for secure code developing and secure data during all development processes in the organization.	Secure Software Development Policy
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	Create and implement procedures that would describe how to: - conduct ongoing security status monitoring of external service provider activity; - detect attacks and indicators of potential attacks from external service providers; - monitor compliance of external providers with personnel security policies and procedures, and contract security requirements.	Supplier Security Policy
		DE.CM-7: Monitoring for unauthorized personnel,	Implement correlation rules within the log management solutions to automate threat detection and log analysis. Consider acquiring a SIEM solution. SIEM solution	Log Monitoring Policy Log Monitoring Rules

		connections, devices, and software is performed	involves installing forwarders on users workstation. Logs are forwarded from workstation to SIEM.	
		DE.CM-8: Vulnerability scans are performed	Document and implement vulnerability management plan;	Vulnerability Management Plan
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	Roles and responsibilities shall be well documented for the SOC team and ensure there is proper escalation and delegation matrix.	Roles and Responsibilities of Incident management team
		DE.DP-2: Detection activities comply with all applicable requirements	Define, document, implement and communicate procedures describing configuring monitoring of services before deploying into production	Configuration SOP, Monitoring SOP
		DE.DP-3: Detection processes are tested	Implement formal procedures which would describe how the organization: - Creates a process for ensuring that organizational plans for conducting security testing, monitoring activities and training associated with organizational information systems; - Ensures that detection testing is executed in a timely manner - Reviews detection testing and monitoring plans for consistency with the organizational risk strategy.	Testing SOP
		DE.DP-4: Event detection information is communicated to appropriate parties	Ensure that event detection information is communicated to defined personnel.	Log Monitoring Policy
			Update list of events which must be detected on a regular basis. Event detection information includes for example, alerts on atypical account usage, unauthorized remote access, wireless connectivity, mobile device connection, altered configuration settings, contrasting system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, use of VoIP, and malware disclosure.	Log Monitoring Policy
		DE.DP-5: Detection processes are continuously improved	Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into detection process revisions.	Incident Management Policy with Lessons Learned

			Ensure the security plan for the production system provides for the review, testing, and continual improvement of the security detection processes;	Incident Management Policy with Lessons Learned
			Employ independent teams to assess the detection process;	Incident Management Policy with Lessons Learned
			Try to enrich your detection assessments including: - vulnerability scanning; - malicious user testing; - insider threat assessment; - performance/load testing;. - verification and validation testing.	Incident Management Policy with Lessons Learned
RESPOND (RS)	**Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.**	RS.RP-1: Response plan is executed during or after an event	Incident Response, Incident Management processes, plans, policies should include: - Roles and Responsibilities employees - Detection Phase - Analysis Phase - Containment Phase - Mitigation Phase - Eradication Phase - Recovery Phase - Post-Incident Activities Ensure above mentioned activities are executed during or after an incident;	IS Incident management Policy
			Create a detailed IT Incident Management Process highlighting roles & responsibilities of each personnel involved.	IT Incident management Policy
			Implement Incident Handling Checklists within your Incident Management processes, plans and policies, so that each team will take the appropriate sequence of actions depending on the type of incident.	Incident Handling Checklists
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include	RS.CO-1: Personnel know their roles and order of operations when a response is needed	Ensure personnel understand objectives, restoration priorities, task sequences and assignment responsibilities for event or incident response.	IT Security team composition document
			Communicate procedures relevant to event or incident response to all relevant parties.	Incident Communication procedures

	external support from law enforcement agencies.		Update Incident Management and IT Security Incident Response policies on a regular basis.	Revision history of Incident Management and IT Security Incident Response policies
		RS.CO-2: Events are reported consistent with established criteria	Create Security Incident Response Report Form to support the reporting action and to help the person reporting to remember all necessary actions in case of an information security event.	Security Incident Response Form
		RS.CO-3: Information is shared consistent with response plans	Share cybersecurity incident information with relevant stakeholders per the response plan drafted initially.	Security Incident Response Form
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	Coordinate cybersecurity incident response actions with all relevant stakeholders. Stakeholders for incident response include, for example, mission/business owners, manufacturing system owners, integrators, vendors, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices.	Security Incident Response Plan
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	Share cybersecurity event information voluntarily, as appropriate, with industry security groups to achieve broader cybersecurity awareness. Based on risk assessment, decide whether cooperation and information sharing with Cyber Police and other relevant regulatory bodies are needed.	Incident Communication procedures & Security Incident Response Plan
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated	Create and document formal procedures of events investigation, define roles and responsibilities, implement metrics, determine effectiveness.	IS Incident management Policy
			Consider implementation of security orchestration solutions to automate decision making.	Log Monitoring Policy
		RS.AN-2: The impact of the incident is understood	Conduct quantitative and qualitive risk analysis of impacted assets. Correlate detected event information and incident responses with risk assessment outcomes to achieve perspective on incident impact across the organization.	Security Incident Policy
		RS.AN-3: Forensics are performed	Conduct forensic analysis on collected cybersecurity event information to determine root cause. Consider outsourcing on-demand audit reviews, analysis, and reporting for investigations of cybersecurity incidents.	Security Incident Policy with Forensics
		RS.AN-4: Incidents are categorized consistent with response plans	Develop severity categories to assess cybersecurity incidents within each Incident Response plan, policy or process.	IS Incident management Plan with severity categories

	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-1: Incidents are contained	Describe and include Containment Phase that limits the root cause of the Security Incident to prevent further damage or exposure. Containment Phase might include following steps: - Short-term Containment; - System Back-Up; - Long-term containment.	Detailed Incident Management plan with all phases
		RS.MI-2: Incidents are mitigated	The organization must describe metrics which need to be collected to mitigate future incidents. The organization should decide what incident data to collect based on reporting requirements and on the expected return on investment from the data (e.g., identifying a new threat and mitigating the related vulnerabilities before they can be exploited.) Possible metrics for incident-related data include: - Number of Incidents Handled; - Time Per Incident; - Objective Assessment of Each Incident; - Subjective Assessment of Each Incident.	Incident Response Plan Incident Management Metrics
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	Create Vulnerability Management Policy procedures which will describe how to document and mitigate accepted risks and new vulnerabilities. For example, how to isolate a vulnerable environment if there doesn't exist a solution to fix vulnerability and how to handle acceptable risks.	Vulnerability Management Policy procedures
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; Write down lessons learned procedures into each incident response policy, procedure or process.	Incident Response Plan with Lessons Learned
		RS.IM-2: Response strategies are updated	Regularly update "Incident management" and "IT security incident response team composition" Updates may include, for example, responses to disruptions or failures, and predetermined procedures.	Incident Response Plan
RECOVER (RC)	**Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely**	RC.RP-1: Recovery plan is executed during or after an event	Document a detailed Disaster recovery plan that describes recovery procedures of internal infrastructure, cloud infrastructure, roles and responsibilities, escalation matrix, DRP timelines.	Disaster recovery plan

	restoration of systems or assets affected by cybersecurity events.		Make a checklist of all your critical assets which can include the applications, processes, servers etc.	DRP Checklist
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	Conduct the DR drill on a regular basis and capture all the drill activities step by step. Applicable lessons learned from previous incidents should be continuously incorporated and also shared with the users.	Disaster recovery plan
			Improving user awareness regarding incidents should reduce the frequency of incidents, particularly those involving malicious code and violations of acceptable use policies.	DR User awareness
		RC.IM-2: Recovery strategies are updated	The Disaster Recovery Plan should be reviewed for accuracy and completeness at least annually, as well as upon significant changes to any element of the DRP system, mission/business processes supported by the system, or resources used for recovery procedures. Elements of the plan subject to frequent changes, such as contact lists, should be reviewed and updated more frequently. Update schedules should be stated in the DRP.	Disaster recovery plan
	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.	RC.CO-1: Public relations are managed	Create a procedures which will include follows things: managing media interactions, coordinating and logging all requests for interviews, handling and 'triaging' phone calls and e-mail requests, matching media requests with appropriate and available internal experts who are ready to be interviewed, screening all of the information provided to the media, ensuring personnel are familiar with public relations and privacy policies.	External communication policy
		RC.CO-2: Reputation after an event is repaired	Implement and document crisis response strategies which will include actions to shape attributions of the crisis, change perceptions of the organization in crisis, and reduce the negative effect generated by the crisis.	Crisis response plan/Data breach response plan
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	Write down detailed descriptions of each procedure related to recovery communication(e.g. Notify SA, Notify data subjects, Input data in data breach register, etc.) to make sure each stakeholder is aware of his/her responsibilities.	Internal Communication Policy