CYBER FUNDAMENTALS

FRAMEWORK NIS2

RC.RP

RC.RP-1.1: A recovery process for disasters and information/cybersecurity incidents shall be developed and executed as appropriate.

RC.RP-1.2: The essential organization's functions and services shall be continued with little or no loss of operational continuity and continuity shall be sustained until full system restoration.

RC.IM

RC.IM-1.1: The organization shall incorporate lessons learned from incident recovery activities into updated or new system recovery procedures and, after testing, frame this with appropriate training.

RC.CO

RC.CO-1.1: The organization shall centralize and coordinate how information is disseminated and manage how the organization is presented to the public.

RC.CO-1.2: A Public Relations Officer shall be assigned.

RC.CO-2.1: The organization shall implement a crisis response strategy to protect the organization from the negative consequences of a crisis and help restore its reputation.

RC.CO-3.1: The organization shall communicate recovery activities to predefined stakeholders, executive and management teams.

RS.IM

RS.IM-1.1: The organization shall conduct post-incident evaluations to analyse lessons learned from incident response and recovery, and consequently improve processes / procedures / technologies to enhance its cyber resilience.

RS.IM-1.2: Lessons learned from incident handling shall be translated into updated or new incident handling procedures that shall be tested, approved and trained.

RS.IM-2.1:The organization shall update the response and recovery plans to address changes in its context.

RS.MI

RS.MI-1.1: The organization shall implement an incident handling capability for information/cybersecurity incidents on its business critical systems that includes preparation, detection and analysis, containment, eradication, recovery and documented risk acceptance.

RS.NA

RS.AN-1.1: The organization shall investigate information/cybersecurity-related notifications generated from detection systems.

RS.AN-1.2: The organization shall implement automated mechanisms to assist in the investigation and analysis of information/cybersecurity-related notifications.

RS.AN-2.1:Thorough investigation and result analysis shall be the base for understanding the full implication of the information/cybersecurity incident.

RS.AN-2.2: The organization shall implement automated mechanisms to support incident impact analysis.

RS.AN-3.1: The organization shall provide on-demand audit review, analysis, and reporting for after-the-fact investigations of information/cybersecurity incidents.

RS.AN-3.2: The organization shall conduct forensic analysis on collected information/ cybersecurity event information to determine root cause.

RS.AN-4.1: Information/cybersecurity incidents shall be categorized according to the level of severity and impact consistent with the evaluation criteria included the incident response plan.

RS.AN-5.1: The organization shall implement vulnerability management processes and procedures that include processing, analyzing and remedying vulnerabilities from internal and external sources.

RS.AN-5.2: The organization shall implement automated mechanisms to disseminate and track remediation efforts for vulnerability information, captured from internal and external sources, to key stakeholders.

RS.CO

RS.CO-1.1: The organization shall ensure that personnel understand their roles, objectives, restoration priorities, task sequences (order of operations) and assignment responsibilities for event response.

RS.CO-2.1: The organization shall implement reporting on information/cybersecurity incidents on its critical systems in an organization-defined time frame to organization-defined personnel or roles.

RS.CO-2.2: Events shall be reported consistent with established criteria.

RS.CO-3.1: Information/cybersecurity incident information shall be communicated and shared with the organization's employees in a format that they can understand.

RS.CO-3.2: The organization shall share information/cybersecurity incident information with relevant stakeholders as foreseen in the incident response plan.

RS.CO-4.1: The organization shall coordinate information/cybersecurity incident response actions with all predefined stakeholders.

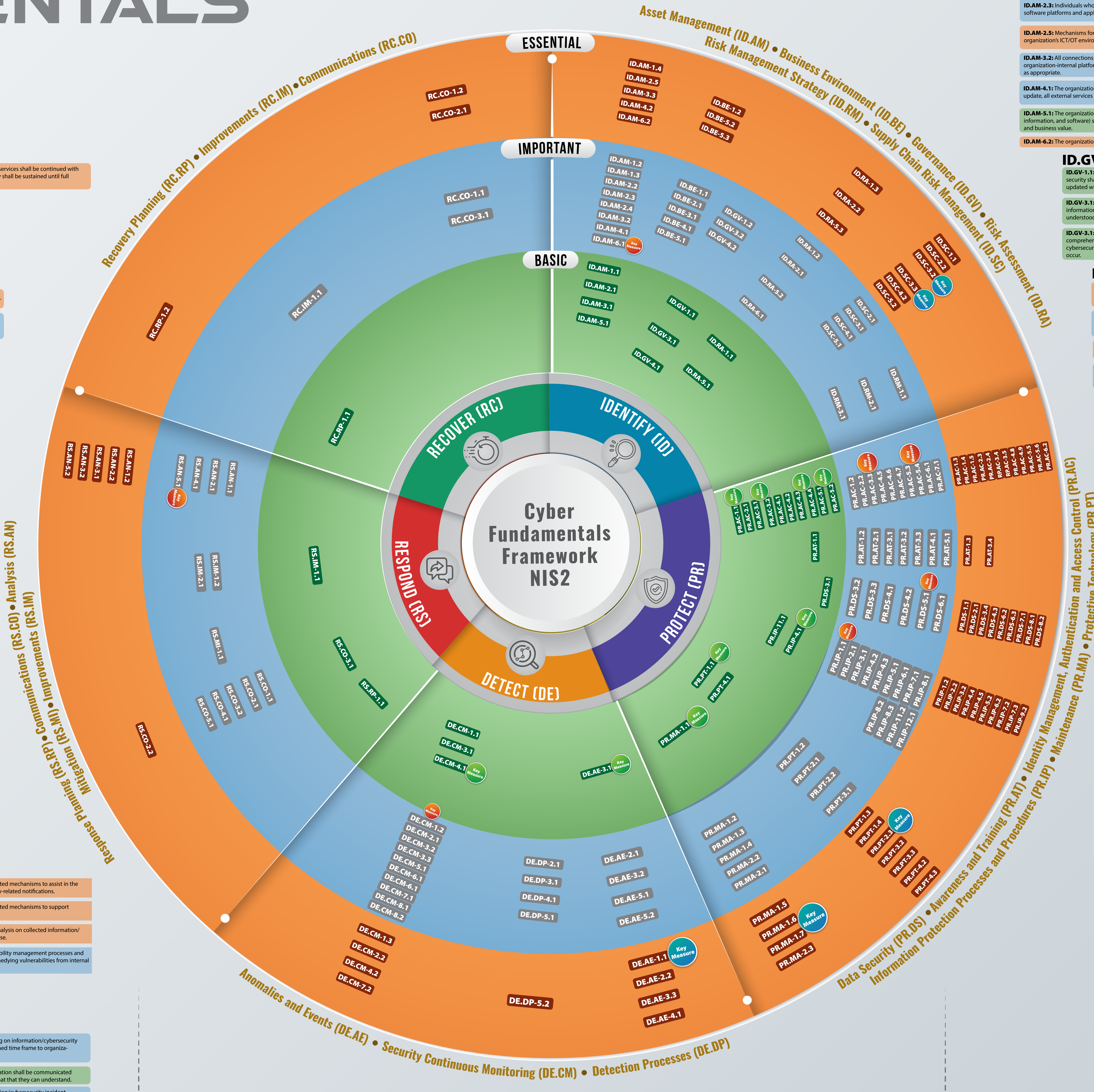
RS.CO-5.1: The organization shall share information/cybersecurity event information voluntarily, as appropriate, with external stakeholders, industry security groups,… to achieve broader information/cybersecurity situational awareness.

RS.RP

RS.RP-1.1: An incident response process, including roles, responsibilities, and authorities, shall be executed during or after an information/cybersecurity event on the organization's critical systems.

Framework Sourced and Owned by CCB
https://ccb.belgium.be
The CyberFundamentals Framework is a set of concrete measures to protect data, significantly reduce the risk of the most common cyber-attacks, and increase an organisation's cyber resilience.

Copyrighted Document by
Jean-François Avart
https://www.linkedin.com/in/avart/
Expert in Cybersecurity Governance, Pragmatism & Risk Management | NIS2 Challenge | Senior Lead Implementer ISO 27001, 27005, 27032



ESSENTIAL
IMPORTANT
BASIC
Cyber Fundamentals Framework NIS2
RECOVER (RC)
IDENTIFY (ID)
PROTECT (PR)
DETECT (DE)
RESPOND (RS)
Key Measure
Asset Management (ID.AM) • Business Environment (ID.BE) • Governance (ID.GV) • Risk Assessment (ID.RA)
Risk Management Strategy (ID.RM) • Supply Chain Risk Management (ID.SC)
Identity Management, Authentication and Access Control (PR.AC) • Awareness and Training (PR.AT) • Data Security (PR.DS)
Information Protection Processes and Procedures (PR.IP) • Maintenance (PR.MA) • Protective Technology (PR.PT)
Anomalies and Events (DE.AE) • Security Continuous Monitoring (DE.CM) • Detection Processes (DE.DP)
Response Planning (RS.RP) • Communications (RS.CO) • Analysis (RS.AN)
Mitigation (RS.MI) • Improvements (RS.IM)
Recovery Planning (RC.RP) • Improvements (RC.IM) • Communications (RC.CO)

DE.CM

DE.CM-1.1: Firewalls shall be installed and operated on the network boundaries and completed with firewall protection on the endpoints.

DE.CM-1.2: The organization shall monitor and identify unauthorized use of its business critical systems through the detection of unauthorized local connections, network connections and remote connections.

DE.CM-1.3: The organization shall conduct ongoing security status monitoring of its network to detect defined information/cybersecurity events and indicators of potential information/cybersecurity events.

DE.CM-2.1: The physical environment of the facility shall be monitored for potential information/cybersecurity events.

DE.CM-2.2: The physical access to organization's critical systems and devices shall be, on top of the physical access monitoring to the facility, increased through physical intrusion alarms, surveillance equipment, independent surveillance teams.

DE.CM-3.1: End point and network protection tools to monitor end-user behavior for dangerous activity shall be implemented.

DE.CM-3.2: End point and network protection tools that monitor end-user behavior for dangerous activity shall be managed.

DE.CM-3.3: Software usage and installation restrictions shall be enforced.

DE.CM-4.1: Anti-virus, -spyware, and other -malware programs shall be installed and updated.

DE.CM-4.2: The organisation shall set up a system to detect false positives while detecting and eradicating malicious code.

DE.CM-5.1: The organization shall define acceptable and unacceptable mobile code and mobile code technologies; and authorize, monitor, and control the use of mobile code within the system.

DE.CM-6.1: All external connections by vendors supporting IT/OT applications or infrastructure shall be secured and actively monitored to ensure that only permissible actions occur during the connection.

DE.CM-6.2: External service providers' conformance with personnel security policies and procedures and contract security requirements shall be monitored relative to their cybersecurity risks.

DE.CM-7.1: The organization's business critical systems shall be monitored for unauthorized personnel access, connections, devices, access points, and software.

DE.CM-7.2: Unauthorized configuration changes to organization's systems shall be monitored and addressed with the appropriate mitigation actions.

DE.CM-8.1: The organization shall monitor and scan for vulnerabilities in its critical systems and hosted applications ensuring that system functions are not adversely impacted by the scanning process.

DE.CM-8.2: The vulnerability scanning process shall include analysis, remediation, and information sharing.

DE.DP

DE.DP-2.1: The organization shall conduct detection activities in accordance with applicable federal and regional laws, industry regulations and standards, policies, and other applicable requirements.

DE.DP-3.1: The organization shall validate that event detection processes are operating as intended.

DE.DP-4.1: The organization shall communicate event detection information to predefined parties.

DE.DP-5.1: Improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned, shall be incorporated into detection process revisions.

DE.DP-5.2: The organization shall conduct specialized assessments including in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing, and verification and validation testing on the organization's critical systems.

DE.AE

DE.AE-1.1: The organization shall ensure that a baseline of network operations and expected data flows for its critical systems is developed, documented and maintained to track events.

DE.AE-2.1: The organization shall review and analyze detected events to understand attack targets and methods.

DE.AE-2.2: The organization shall implement automated mechanisms where feasible to review and analyze detected events.

DE.AE-3.1: The activity logging functionality of protection / detection hardware or software (e.g. firewalls, anti-virus) shall be enabled, backed-up and reviewed.

DE.AE-3.2: The organization shall ensure that event data is compiled and correlated across its critical systems using various sources such as event reports, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

DE.AE-3.3: The organization shall integrate analysis of events where feasible with the analysis of vulnerability scanning information; performance data; its critical system's monitoring, and facility monitoring to further enhance the ability to identify inappropriate or unusual activity.

DE.AE-4.1: Negative impacts to organization's operations, assets, and individuals resulting from detected events shall be determined and correlated with risk assessment outcomes.

DE.AE-5.2: The organization shall define incident alert thresholds.

DE.AE-5.1: The organization shall implement automated mechanisms and system generated alerts to support event detection and to assist in the identification of security alert thresholds.

ID.AM

ID.AM-1.1: An inventory of assets associated with information and information processing facilities within the organization shall be documented, reviewed, and updated when changes occur.

ID.AM-1.2: The inventory of assets associated with information and information processing facilities shall reflect changes in the organization's context and include all information necessary for effective accountability.

ID.AM-1.3: When unauthorized hardware is detected, it shall be quarantined for possible exception handling, removed, or replaced, and the inventory shall be updated accordingly.

ID.AM-1.4: Mechanisms for detecting the presence of unauthorized hardware and firmware components within the organization's network shall be identified.

ID.AM-2.1: An inventory that reflects what software platforms and applications are being used in the organization shall be documented, reviewed, and updated when changes occur.

ID.AM-2.2: The inventory of software platforms and applications associated with information and information processing shall reflect changes in the organization's context and include all information necessary for effective accountability.

ID.AM-2.3: Individuals who are responsible and who are accountable for administering software platforms and applications within the organization shall be identified.

ID.AM-2.4: When unauthorized software is detected, it shall be quarantined for possible exception handling, removed, or replaced, and the inventory shall be updated accordingly.

ID.AM-2.5: Mechanisms for detecting the presence of unauthorized software within the organization's ICT/OT environment shall be identified.

ID.AM-3.1: Information that the organization stores and uses shall be identified.

ID.AM-3.2: All connections within the organization's ICT/OT environment, and to other organization-internal platforms shall be mapped, documented, approved, and updated as appropriate.

ID.AM-3.3: The information flows/data flows within the organization's ICT/OT environment, as well as to other organization-internal systems shall be mapped, documented, authorized, and updated when changes occur.

ID.AM-4.1: The organization shall map, document, authorize and when changes occur, update, all external services and the connections made with them.

ID.AM-4.2: The flow of information to/from external systems shall be mapped, documented, authorized, and update when changes occur.

ID.AM-5.1: The organization's resources (hardware, devices, data, time, personnel, information, and software) shall be prioritized based on their classification, criticality, and business value.

ID.AM-6.1: Information security and cybersecurity roles, responsibilities and authorities within the organization shall be documented, reviewed, authorized, and updated and alignment with organization-internal roles and external partners.

ID.AM-6.2: The organization shall appoint an information security officer.

ID.BE

ID.BE-1.1: The organization's role in the supply chain shall be identified, documented, and communicated.

ID.BE-1.2: The organization shall protect its ICT/OT environment from supply chain threats by applying security safeguards as part of a documented comprehensive security strategy.

ID.BE-2.1: The organization's place in critical infrastructure and its industry sector shall be identified and communicated.

ID.BE-3.1: Priorities for organizational mission, objectives, and activities are established and communicated.

ID.BE-4.1: Dependencies and mission-critical functions for the delivery of critical services shall be identified, documented, and prioritized according to their criticality as part of the risk assessment process.

ID.BE-5.1: To support cyber resilience and secure the delivery of critical services, the necessary requirements are identified, documented and their implementation tested and approved.

ID.BE-5.2: Information processing & supporting facilities shall implement redundancy to meet availability requirements, as defined by the organization and/or regulatory frameworks.

ID.BE-5.3: Recovery time and recovery point objectives for the resumption of essential ICT/OT system processes shall be defined.

ID.GV

ID.GV-1.1: Policies and procedures for information security and cyber security shall be created, documented, reviewed, approved, and updated when changes occur.

ID.GV-1.2: An organization-wide information security and cybersecurity policy shall be established, documented, updated when changes occur, disseminated, and approved by senior management.

ID.GV-3.1: Legal and regulatory requirements regarding information/cybersecurity, including privacy obligations, shall be understood and implemented.

ID.GV-3.2: Legal and regulatory requirements regarding information/-cybersecurity, including privacy obligations,
shall be managed.

ID.GV-3.1: As part of the company's overall risk management, a comprehensive strategy to manage information security and cybersecurity risks shall be developed and updated when changes occur.

ID.GV-4.2: Information security and cybersecurity risks shall be documented, formally approved, and updated when changes occur.

ID.RA

ID.RA-1.1: Threats and vulnerabilities shall be identified.

ID.RA-1.2: A process shall be established to monitor, identify, and document vulnerabilities of the organisation's business critical systems in a continuous manner.

ID.RA-1.3: To ensure that organization's operations are not adversely impacted by the testing process, performance/-load testing and penetration testing on the organization's systems shall be conducted with care.

ID.RA-2.1: A threat and vulnerability awareness program that includes a cross-organization information-sharing capability shall be implemented.

ID.RA-2.2: It shall be identified where automated mechanisms can be implemented to make security alert and advisory information available to relevant organization stakeholders.

ID.RA-5.1: The organization shall conduct risk assessments in which risk is determined by threats, vulnerabilities and impact on business processes and assets.

ID.RA-5.2: The organization shall conduct and document risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence.

ID.RA-5.3: Risk assessment results shall be disseminated to relevant stakeholders.

ID.RA-6.1: A comprehensive strategy shall be developed and implemented to manage risks to the organization's critical systems, that includes the identification and prioritization of risk responses.

ID.SC

ID.SC-1.1: The organization shall document, review, approve, update when changes occur, and implement a cyber supply chain risk management process that supports the identification, assessment, and mitigation of the risks associated with the distributed and interconnected nature of ICT/OT product and service supply chains.

ID.SC-2.1: The organization shall conduct cyber supply chain risk assessments at least annually or when a change to the organization's critical systems, operational environment, or supply chain occurs; These assessments shall be documented, and the results disseminated to relevant stakeholders including those responsible for ICT/OT systems.

ID.SC-2.2: A documented list of all the organization's suppliers, vendors and partners who may be involved in a major incident shall be established, kept up-to-date and made available online and offline.

ID.SC-3.1: Based on the results of the cyber supply chain risk assessment, a contractual framework for suppliers and external partners shall be established to address sharing of sensitive information and distributed and interconnected ICT/OT products and services.

ID.SC-3.2: Contractual information security and cybersecurity' requirements for suppliers and third-party partners shall be implemented to ensure a verifiable flaw remediation process, and to ensure the correction of flaws identified during 'information security and cybersecurity' testing and evaluation.

ID.SC-3.3: The organization shall establish contractual requirements permitting the organization to review the 'information security and cybersecurity' programs implemented by suppliers and third-party partners.

ID.SC-4.1: The organization shall review assessments of suppliers' and third-party partner's compliance with contractual obligations by routinely reviewing audits, test results, and other evaluations.

ID.SC-4.2: The organization shall review assessments of suppliers' and third-party partner's compliance with contractual obligations by routinely reviewing third-party independent audits, test results, and other evaluations.

ID.SC-5.1: The organization shall identify and document key personnel from suppliers and third-party partners to include them as stakeholders in response and recovery planning activities.

ID.SC-5.2: The organization shall identify and document key personnel from suppliers and third-party partners to include them as stakeholders in testing and execution of the response and recovery plans.

ID.RM

ID.RM-1.1: A cyber risk management process that identifies key internal and external stakeholders and facilitates addressing risk-related issues and information shall be created, documented, reviewed, approved, and updated when changes occur.

ID.RM-2.1: The organization shall clearly determine it's risk appetite.

ID.RM-3.1: The organization's role in critical infrastructure and its sector shall determine the organization's risk appetite.

PR.AC

PR.AC-1.1: Identities and credentials for authorized devices and users shall be managed.

PR.AC-1.2: Identities and credentials for authorized devices and users shall be managed, where feasible through automated mechanisms.

PR.AC-1.3: System credentials shall be deactivated after a specified period of inactivity unless it would compromise the safe operation of (critical) processes.

PR.AC-1.4: For transactions within the organization's critical systems, the organization shall implement:
• multi-factor end-user authentication (MFA or "strong authentication").
• certificate-based authentication for system-to-system communications

PR.AC-1.5: The organization's critical systems shall be monitored for atypical use of system credentials. Credentials associated with significant risk shall be disabled.

PR.AC-2.1: Physical access to the facility, servers and network components shall be managed.

PR.AC-2.2: The management of physical access shall include measures related to access in emergency situations.

PR.AC-2.3: Physical access to critical zones shall be controlled in addition to the physical access to the facility.

PR.AC-2.4: Assets related to critical zones shall be physically protected.

PR.AC-3.1 The organisation's wireless access points shall be secured.

PR.AC-3.2: The organization's networks when accessed remotely shall be secured, including through multi-factor authentication (MFA).

PR.AC-3.3: Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization's critical systems environment shall be identified, documented and implemented.

R.AC-3.4: Remote access to the organization's critical systems shall be monitored and cryptographic mechanisms shall be implemented where determined necessary.

R.AC-3.5: The security for connections with external systems shall be verified and framed by documented agreements.

PR.AC-4.1: Access permissions for users to the organization's systems shall be defined and managed.

PR.AC-4.2: It shall be identified who should have access to the organization's business's critical information and technology and the means to get access.

PR.AC-4.3: Employee access to data and information shall be limited to the systems and specific information they need to do their jobs (the principle of Least Privilege).

PR.AC-4.4: Nobody shall have administrator privileges for daily tasks.

PR.AC-4.5: Where feasible, automated mechanisms shall be implemented to support the management of user accounts on the organisation's critical systems, including disabling, monitoring, reporting and deleting user accounts.

PR.AC-4.6: Separation of duties (SoD) shall be ensured in the management of access rights.

PR.AC-4.7: Priviliged users shall be managed and monitored.

PR.AC-4.8: Account usage restrictions for specific time periods and locations shall be taken into account in the organization's security access policy and applied accordingly.

PR.AC-4.9: Priviliged users shall be managed, monitored and audited.

PR.AC-5.1: Firewalls shall be installed and activated on all the organization's networks.

PR.AC-5.2: Where appropriate, network integrity of the organization's critical systems shall be protected by incorporating network segmentation and segregation.

PR.AC-5.3: Where appropriate, network integrity of the organization's critical systems shall be protected by
(1) Identifying, documenting, and controlling connections between system components.
(2) Limiting external connections to the organization's critical systems.

PR.AC-5.4: The organization shall monitor and control connections and communications at the external boundary and at key internal boundaries within the organization's critical systems by implementing boundary protection devices where appropriate.

PR.AC-5.5: The organization shall implement, where feasible, authenticated proxy servers for defined communications traffic between the organization's critical systems and external networks.

PR.AC-6.1: The organization shall implement documented procedures for verifying the identity of individuals before issuing credentials that provide access to organization's systems.

PR.AC-6.2: The organization shall ensure the use of unique credentials bound to each verified user, device, and process interacting with the organization's critical systems; make sure that they are authenticated, and that the unique identifiers are captured when performing system interactions.

PR.AC-7.1: The organization shall perform a documented risk assessment on organization's critical system transactions and authenticate users, devices, and other assets (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

PR.AT

PR.AT-1.1: Employees shall be trained as appropriate.

PR.AT-1.2: The organization shall incorporate insider threat recognition and reporting into security awareness training.

PR.AT-1.3: The organization shall implement an evaluation method to measure the effectiveness of the awareness trainings.

PR.AT-2.1: Privileged users shall be qualified before privileges are granted, and these users shall be able to demonstrate the understanding of their roles, responsibilities, and authorities.

PR.AT-3.1: The organization shall establish and enforce security requirements for business-critical third-party providers and users.

PR.AT-3.2: Third-party providers shall be required to notify any personnel transfers, termination, or transition involving personnel with physical or logical access to organization's business critical system's components.

PR.AT-3.3:The organization shall monitor business critical service providers and users for security compliance.

PR.AT-3.4: The organization shall audit business-critical external service providers for security compliance.

PR.AT-4.1: Senior executives shall demonstrate the understanding of their roles, responsibilities, and authorities.

PR.AT-5.1: The organization shall ensure that personnel responsible for the physical protection and security of the organization's critical systems and facilities are qualified through training before privileges are granted, and that they understand their responsibilities.

PR.DC

PR.DS-1.1: The organization shall protect its critical system information determined to be critical/ sensitive while at rest.

PR.DS-2.1: The organization shall protect its critical system information determined to be critical when in transit.

PR.DS-3.1: Assets and media shall be disposed of safely.

PR.DS-3.2: The organization shall enforce accountability for all its business-critical assets throughout the system lifecycle, including removal, transfers, and disposition.

PR.DS-3.3: The organization shall ensure that the necessary measures are taken to deal with loss, misuse, damage, or theft of assets.

PR.DS-3.4: The organization shall ensure that disposal actions are approved, tracked, documented, and verified.

PR.DS-4.1: Capacity planning shall ensure adequate resources for organization's critical system information processing, networking, telecommunications, and data storage.

PR.DS-4.2: Audit data from the organization's critical systems shall be moved to an alternative system.

PR.DS-4.3: The organization's critical systems shall be protected against denial-of-service attacks or at least the effect of such attacks will be limited.

PR.DS-5.1: The organization shall take appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorized access and activities, including data leakage, is detected.

PR.DS-6.1: The organization shall implement software, firmware, and information integrity checks to detect unauthorized changes to its critical system components during storage, transport, start-up and when determined necessary.

PR.DS-6.2: The organization shall implement automated tools where feasible to provide notification upon discovering discrepancies during integrity verification.

PR.DS-6.3: The organization shall implement automatic response capability with pre-defined security safeguards when integrity violations are discovered.

PR.DS-7.1: The development and test environment(s) shall be isolated from the production environment.

PR.DS-8.1: The organization shall implement hardware integrity checks to detect unauthorized tampering to its critical system's hardware.

PR.DS-8.2: The organization shall incorporate the detection of unauthorized tampering to its critical system's hardware into the organization incident response capability.

PR.IP

PR.IP-1.1: The organization shall develop, document, and maintain a baseline configuration for the its business critical systems.

PR.IP-1.2: The organization shall configure its business-critical systems to provide only essential capabilities; Therefore the baseline configuration shall be reviewed, and unnecessary capabilities disabled.

PR.IP-2.1: The system and application development life cycle shall include security considerations.

PR.IP-2.2: The development process for critical systems and system components shall cover the full design cycle and shall provide a description of the functional properties of security controls, and design and implementation information for security-relevant system interfaces.

PR.IP-3.1: Changes shall be tested and validated before being implemented into operational systems.

PR.IP-3.2: For planned changes to the organization's critical systems, a security impact analysis shall be performed in a separate test environment before implementation in an operational environment.

PR.IP-4.1: Backups for organization's business critical data shall be conducted and stored on a system different from the device on which the original data resides.

PR.IP-4.2: The reliability and integrity of backups shall be verified and tested on regular basis.

PR.IP-4.3: A separate alternate storage site for system backups shall be operated and the same security safeguards as the primary storage location shall be employed.

PR.IP-4.4: Backup verification shall be coordinated with the functions in the organization that are responsible for related plans.

PR.IP-4.5: Critical system backup shall be separated from critical information backup.

PR.IP-5.1: The organization shall define, implement, and enforce policy and procedures regarding emergency and safety systems, fire protection systems, and environment controls for its critical systems.

PR.IP-6.1: The organization shall ensure that its critical system's data is destroyed according to policy.

PR.IP-6.2: Sanitation processes shall be documented and tested.

PR.IP-7.1: The organization shall incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into protection process updates (continuous improvement).

PR.IP-7.2: The organization shall implement independent teams to assess the protection process(es).

PR.IP-7.3: The organization shall ensure that the security plan for its critical systems facilitates the review, testing, and continual improvement of the security protection processes.

PR.IP-8.1: The organization shall collaborate and share information about its critical system's related security incidents and mitigation measures with designated partners.

PR.IP-8.2: Communication of effectiveness of protection technologies shall be shared with appropriate parties.

PR.IP-8.3: The organization shall implement, where feasible, automated mechanisms to assist in information collaboration.

PR.IP-9.1: Incident response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) shall be established, maintained, approved, and tested to determine the effectiveness of the plans, and the readiness to execute the plans.

PR.IP-9.2: The organization shall coordinate the development and the testing of incident response plans and recovery plans with stakeholders responsible for related plans.

PR.IP-11.1: Personnel having access to the organization's most critical information or technology shall be verified.

PR.IP-11.2: Develop and maintain a human resource information/cyber security process that is applicable when recruiting, during employment and at termination of employment.

PR.IP-12.1: The organization shall establish and maintain a documented process that allows continuous review of vulnerabilities and strategies to mitigate them.

PR.MA

PR.MA-1.1: Patches and security updates for Operating Systems and critical system components shall be installed.

PR.MA-1.2: The organization shall plan, perform and document preventive maintenance and repairs on its critical system components according to approved processes and tools.

PR.MA-1.3: The organization shall enforce approval requirements, control, and monitoring of maintenance tools for use on the its critical systems.

PR.MA-1.4: The organization shall verify security controls following hardware maintenance or repairs, and take action as appropriate.

PR.MA-1.5: The organization shall prevent the unauthorized removal of maintenance equipment containing organization's critical system information.

PR.MA-1.6: Maintenance tools and portable storage devices shall be inspected when brought into the facility and shall be protected by anti-malware solutions so that they are scanned for malicious code before they are used on organization's systems.

PR.MA-1.7: The organization shall verify security controls following hardware and software maintenance or repairs/patching and take action as appropriate.

PR.MA-2.1: Remote maintenance shall only occur after prior approval, monitoring to avoid unauthorised access, and approval of the outcome of the maintenance activities as described in approved processes or procedures.

PR.MA-2.2: The organization shall make sure that strong authenticators, record keeping, and session termination for remote maintenance is implemented.

PR.MA-2.3: The organization shall require that diagnostic services pertaining to remote maintenance be performed from a system that implements a security capability comparable to the capability implemented on the equivalent organization's critical system.

PR.PT

PR.PT-1.1: Logs shall be maintained, documented, and reviewed.

PR.PT-1.2: The organization shall ensure that the log records include an authoritative time source or internal clock time stamp that are compared and synchronized to an authoritative time source.

PR.PT-1.3: The organization shall ensure that audit processing failures on the organization's systems generate alerts and trigger defined responses.

PR.PT-1.4: The organization shall enable authorized individuals to extend audit capabilities when required by events.

PR.PT-2.1: The usage restriction of portable storage devices shall be ensured through an appropriate documented policy and supporting safeguards.

PR.PT-2.2: The organisation should technically prohibit the connection of removable media unless strictly necessary; in other instances, the execution of autoruns from such media should be disabled.

PR.PT-2.3: Portable storage devices containing system data shall be controlled and protected while in transit and in storage.

PR.PT-3.1: The organization shall configure the business critical systems to provide only essential capabilities.

PR.PT-3.2: The organization shall disable defined functions, ports, protocols, and services within its critical systems that it deems unnecessary.

PR.PT-3.3: The organization shall implement technical safeguards to enforce a deny-all, permit-by-exception policy to only allow the execution of authorized software programs.

PR.PT-4.1: Web and e-mail filters shall be installed and used.

PR.PT-4.2: The organization shall control the information flows/data flows within its critical systems and between interconnected systems.

PR.PT-4.3: The organization shall manage the interface for external communication services by establishing a traffic flow policy, protecting the confidentiality and integrity of the information being transmitted; This includes the review and documenting of each exception to the traffic flow policy.