

# **NIST Categories SSOT SUPPORT**

## **ID.AM - Asset Management**

**CyFun Framework [SSOT CORE]:** ID.AM-1.1 , ID.AM-1.2 , ID.AM-1.3 , ID.AM-1.4 , ID.AM-2.1 , ID.AM-2.2 , ID.AM-2.3 , ID.AM-2.4 , ID.AM-2.5 , ID.AM-3.1 , ID.AM-3.2 , ID.AM-3.3 , ID.AM-4.1 , ID.AM-4.2 , ID.AM-5.1 , ID.AM-6.1 , ID.AM-6.2

**CyFun Framework Goals [SSOT SUPPORT]:** The data, personnel, devices, systems, and facilities that enable the organization to achieve business objectives are identified and managed in accordance with their relative importance to organizational objectives and the organization's risk strategy.

## **ID.BE - Business Environment**

**CyFun Framework [SSOT CORE]:** ID.BE-1.1 , ID.BE-1.2 , ID.BE-2.1 , ID.BE-3.1 , ID.BE-4.1 , ID.BE-5.1 , ID.BE-5.2

**CyFun Framework Goals [SSOT SUPPORT]:** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles and responsibilities, and to support risk management decisions.

## **ID.GV - Governance**

**CyFun Framework [SSOT CORE]:** ID.BE-5.3 , ID.GV-1.1 , ID.GV-1.2 , ID.GV-3.1 , ID.GV-3.2 , ID.GV-4.1 , ID.GV-4.2

**CyFun Framework Goals [SSOT SUPPORT]:** 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.RA - Risk Assessment**

**CyFun Framework [SSOT CORE]:** ID.RA-1.1 , ID.RA-1.2 , ID.RA-1.3 , ID.RA-2.1 , ID.RA-2.2 , ID.RA-5.1 , ID.RA-5.2 , ID.RA-5.3 , ID.RA-6.1

**CyFun Framework Goals [SSOT SUPPORT]:** The organization understands the cybersecurity risk to organizational operations, organizational assets, and individuals (including mission, functions, image, or reputation).

## **ID.RM - Risk Management**

**CyFun Framework [SSOT CORE]:** ID.RM-1.1 , ID.RM-2.1 , ID.RM-3.1

**CyFun Framework Goals [SSOT SUPPORT]:** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

## **ID.SC - Supply Chain Risk Management**

**CyFun Framework [SSOT CORE]:** ID.SC-1.1 , ID.SC-2.1 , ID.SC-2.2 , ID.SC-3.1 , ID.SC-3.2 , ID.SC-3.3 , ID.SC-4.1 , ID.SC-4.2 , ID.SC-5.1 , ID.SC-5.2

**CyFun Framework Goals [SSOT SUPPORT]:** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has the ability to inform its understanding of its dependencies and associated supply chains.

## **PR.AC - Identity Management and Access Control**

**CyFun Framework [SSOT CORE]:** PR.AC-1.1 , PR.AC-1.2 , PR.AC-1.3 , PR.AC-1.4 , PR.AC-1.5 , PR.AC-2-1 , PR.AC-2-2 , PR.AC-2-3 , PR.AC-2-4 , PR.AC-3.1 , PR.AC-3.2 , PR.AC-3.3 , PR.AC-3.4 , PR.AC-3.5 , PR.AC-4.1 , PR.AC-4.2 , PR.AC-4.3 , PR.AC-4.4 , PR.AC-4.5 , PR.AC-4.6 , PR.AC-4.7 , PR.AC-4.8 , PR.AC-5.1 , PR.AC-5.2 , PR.AC-5.3 , PR.AC-5.4 , PR.AC-5.5 , PR.AC-5.6 , PR.AC-6.1 , PR.AC-6.2 , PR.AC-7.1

**CyFun Framework Goals [SSOT SUPPORT]:** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

## **PR.AT - Awareness & Training**

**CyFun Framework [SSOT CORE]:** PR.AT-1.1 , PR.AT-1.2 , PR.AT-1.3 , PR.AT-2.1 , PR.AT-3-1 , PR.AT-3-2 , PR.AT-3-3 , PR.AT-3-4 , PR.AT-4.1 , PR.AT-5.1

**CyFun Framework Goals [SSOT SUPPORT]:** The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

## **PR.DS - Data Security**

**CyFun Framework [SSOT CORE]:** PR.DS-1.1 , PR.DS-2.1 , PR.DS-3.1 , PR.DS-3.2 , PR.DS-3.3 , PR.DS-3.4 , PR.DS-4.1 , PR.DS-4.2 , PR.DS-4.3 , PR.DS-5.1 , PR.DS-6.1 , PR.DS-6.2 , PR.DS-6.3 , PR.DS-7.1 , PR.DS-8.1 , PR.DS-8.2

**CyFun Framework Goals [SSOT SUPPORT]:** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

## **PR.IP - Information Protection Processes & Procedures**

**CyFun Framework [SSOT CORE]:** PR.IP-1.1 , PR.IP-1.2 , PR.IP-2.1 , PR.IP-2.2 , PR.IP-3.1 , PR.IP-3.2 , PR.IP-4.1 , PR.IP-4.2 , PR.IP-4.3 , PR.IP-4.4 , PR.IP-4.5 , PR.IP-5.1 , PR.IP-5.2 , PR.IP-6.1 , PR.IP-6.2 , PR.IP-7.1 , PR.IP-7.2 , PR.IP-7.3 , PR.IP-8.1 , PR.IP-8.2 , PR.IP-8.3 , PR.IP-9.1 , PR.IP-9.2 , PR.IP-11.1 , PR.IP-11.2 , PR.IP-12.1

**CyFun Framework Goals [SSOT SUPPORT]:** 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.MA - Maintenance**

**CyFun Framework [SSOT CORE]:** PR.MA-1.1 , PR.MA-1.2 , PR.MA-1.3 , PR.MA-1.4 , PR.MA-1.5 , PR.MA-1.6 , PR.MA-2.1 , PR.MA-2.2 , PR.MA-2.3

**CyFun Framework Goals [SSOT SUPPORT]:** Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

## **PR.PT - Protective Technology**

**CyFun Framework [SSOT CORE]:** PR.PT-1.1 , PR.PT-1.2 , PR.PT-1.3 , PR.PT-1.4 , PR.PT-2.1 , PR.PT-2.2 , PR.PT-2.3 , PR.PT-3.1 , PR.PT-3.2 , PR.PT-3.3 , PR.PT-4.1 , PR.PT-4.2 , PR.PT-4.3

**CyFun Framework Goals [SSOT SUPPORT]:** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

## **DE.AE - Anomalies & Events**

**CyFun Framework [SSOT CORE]:** DE.AE-1.1 , DE.AE-2.1 , DE.AE-2.2 , DE.AE-3.1 , DE.AE-3.2 , DE.AE-3.3 , DE.AE-4.1 , DE.AE-5.1 , DE.AE-5.2

**CyFun Framework Goals [SSOT SUPPORT]:** Anomalous activity is detected and the potential impact of events is understood.

## **DE.CM - Security Continuous Monitoring**

**CyFun Framework [SSOT CORE]:** DE.CM-1.1 , DE.CM-1.2 , DE.CM-1.3 , DE.CM-1.4 , DE.CM-2.1 , DE.CM-3.1 , DE.CM-3.2 , DE.CM-3.3 , DE.CM-4.1 , DE.CM-4.2 , DE.CM-5.1 , DE.CM-6.1 , DE.CM-6.2 , DE.CM-7.1 , DE.CM-7.2 , DE.CM-8.1 , DE.CM-8.2

**CyFun Framework Goals [SSOT SUPPORT]:** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

## **DE.DP - Detection Processes**

**CyFun Framework [SSOT CORE]:** DE.DP-2.1 , DE.DP-3.1 , DE.DP-4.1 , DE.DP-5.1 , DE.DP-5.2

**CyFun Framework Goals [SSOT SUPPORT]:** Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

## **RS.RP - Response Planning**

**CyFun Framework [SSOT CORE]:** RS.RP-1.1 , RC.RP-1.2

**CyFun Framework Goals [SSOT SUPPORT]:** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

## **RS.CO - Communications**

**CyFun Framework [SSOT CORE]:** RS.CO-1.1 , RS.CO-2.1 , RS.CO-2.2 , RS.CO-3.1 , RS.CO-3.2 , RS.CO-4.1 , RS.CO-5.1

**CyFun Framework Goals [SSOT SUPPORT]:** Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

## **RS.AN - Analysis**

**CyFun Framework [SSOT CORE]:** RS.AN-1.1 , RS.AN-1.2 , RS.AN-2.1 , RS.AN-2.2 , RS.AN-3.1 , RS.AN-3.2 , RS.AN-4.1 , RS.AN-5.1 , RS.AN-5.2

**CyFun Framework Goals [SSOT SUPPORT]:** Analysis is performed to ensure effective response and support recovery activities.

## **RS.MI - Mitigation**

**CyFun Framework [SSOT CORE]:** RS.MI-1.1 , RS.MI-2.1 , RS.MI-3.1

**CyFun Framework Goals [SSOT SUPPORT]:** Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

## **RS.IM - Improvements**

**CyFun Framework [SSOT CORE]:** RS.IM-1.1 , RS.IM-1.2 , RS.IM-2.1

**CyFun Framework Goals [SSOT SUPPORT]:** Organizational response activities are improved by incorporating lessons learned from current and previous detection and response activities.

## **RC.RP - Recovery Planning**

**CyFun Framework [SSOT CORE]:** RC.RP-1.1

**CyFun Framework Goals [SSOT SUPPORT]:** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

## **RC.IM - Improvements**

**CyFun Framework [SSOT CORE]:** RC.IM - 1.1

**CyFun Framework Goals [SSOT SUPPORT]:** Recovery planning and processes are improved by incorporating lessons learned into future activities.

## **RC.CO - Communications**

**CyFun Framework [SSOT CORE]:** RC.CO-1.1 , RC.CO-1.2 , RC.CO-2.1 , RC.CO-3.1

**CyFun Framework Goals [SSOT SUPPORT]:** Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).