Function	Category	Subcategory ID	Description	Support	Capability	Rationale
Identify	Asset Management	ID.AM-2	Software platforms and applications within the organization are inventoried	INFORM	Analytics	SPHEREboard discovers and records a complete inventory of assets within an organizations digital estate at a granular level to track and report on identity, account, and group activity (servers, DB, fileshares)
Identify	Asset Management	ID.AM-3	Organizational communication and data flows are mapped	INFORM	Analytics	SPHEREboard correlates identities with users, groups, and data and provides clear and detailed mapping of communication and data flows within an organization
Identify	Asset Management	ID.AM-5	Resources are prioritized based on their classification, criticality, and business value.	INFORM	Analytics	SPHEREboard provides clear insight tied to identities, accounts, groups, and data in order to identify and prioritize systems based on criticality, classification and value
Identify	Business Enviroment	ID.BE-4	Dependencies and critical functions for delivery of critical services are established.	INFORM	Reporting/ Remediation	SPHEREboard allows organizations to create personalized controls based on internal/external guidelines and best practices, identifies violations, and automates remediation of control violations to preserve critical business functions
Identify	Governance	ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.	INFORM	Reporting/ Remediation	SPHEREboard enables organizations to set granular details of roles and entitlement associated to applications. It highlights gaps and enables needed changes to be more easily identified.
Identify	Governance	ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	INFORM	Governance	SPHEREboard ensures organizations adhere to regulatory and contractual requirements for Identity Hygiene and access management, facilitating monitoring, control, and direct reporting to auditors.
Identify	Governance	ID.GV-4	Governance and risk management processes address cybersecurity risks	CONTRIBUTE	Governance	SPHEREboard's risk assessment reports individuals' access to assets, evaluating the potential harm in case of unauthorized information system access.
Identify	Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented	CONTRIBUTE	Reporting/ Remediation	SPHEREboard continually evaluates organizational security controls, providing documented insights into their effectiveness and efficiency.
Protect	Access Control	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	CONTRIBUTE	Reporting/ Remediation	SPHEREboard's core, Identity Hygiene, utilizes intelligent discovery to verify and manage access within accounts, groups, or devices, automatically remediating violations for sustained control of assets.
Protect	Access Control	PR.AC-3	Remote access is managed	CONTRIBUTE	Reporting/ Remediation	SPHEREboard limits system access to authorized transactions and functions by discovering, reporting, and remediating access privileges based on account type or a combination thereof.
Protect	Access Control	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	CONTRIBUTE	Reporting/ Remediation	SPHEREboard for Users and Groups ensures end-user access aligns with access control policies. Utilizing account access route capabilities, it reinforces the principle of least privilege, identifying and remedying excessive access. Advanced analytics also report on the alignment of organization-defined access controls with security standards.
Protect	Access Control	PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	CONTRIBUTE	Reporting/ Remediation	SPHEREboard workflows facilitate identity proofing for system access, correlating user identities, collecting, validating, verifying, and remediating identity evidence. The Asset Review Module supports IAM teams in conducting User Access Reviews as detective controls to promptly adjust user access based on changes in employment status.
Protect	Data Security	PR.DS-1	Data-at-rest is protected	CONTRIBUTE	Reporting	SPHEREboard for BigID protects critical data by discovering its location, accurately identifying ownership, and swiftly remediating access. It excels in locating and classifying PII, financial data, sensitive data, and other key information.
Protect	Data Security	PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	CONTRIBUTE	Reporting	SPHEREboard ensures consistent implementation of critical security controls for data protection. Modules like Activity Data Reporting, Cloud Data, and Unstructured Data enable organizations to implement controls for both standard and non-standard access to file systems, collaboration tools, and data storage devices.
Protect	Data Security	PR.DS-5	Protections against data leaks are implemented	CONTRIBUTE	Reporting	SPHEREboard contributes to data protection by discovering, reporting, and remediating non-standard, Open Access, and Excessive access to critical data, serving as a key responsibility for data-rich enterprises.
Protect	Data Security	PR.DS-7	The development and testing environment(s) are separate from the production environment.	CONTRIBUTE	Analytics	Effective management ensures users adhere to proper network boundaries, like those between development and production environments. SPHEREboard offers comprehensive insights into identities, accounts, and assets, empowering administrators to implement effective detective controls for environment restrictions.
Protect	Data Security	PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	CONTRIBUTE	Reporting/ Remediation	Provisioning and de-provisioning accounts are vital in human resource management. SPHEREboard offers necessary insights to facilitate the timely implementation of Identity Hygiene processes, regardless of the activity's location.
Protect	Maintenance	PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	CONTRIBUTE	Reporting/ Remediation	SPHEREboard provides essential oversight and control to determine who has access to assets, ensuring that only authorized users are permitted to perform maintenance activities.
Protect	Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	CONTRIBUTE	Reporting	SPHEREboard contributes all gathered and logged Identity Hygiene information into the organizations overall audit/log records.
Protect	Protective Technology	PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	CONTRIBUTE	Reporting/ Remediation	SPHEREboard for Users and Groups provides organizations with the ability to identify and limit what users can do with any given asset.
Detect	Anomalies and Events	DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors.	CONTRIBUTE	Analytics	SPHEREboard's Activity Data Module contributes to the overall event data that can be collected and analyzed.
Detect	Anomalies and Events	DE.AE-4	Impact of events is determined.	CONTRIBUTE	Analytics	SPHEREboard's account access routes capability can aid in determining the impact of certain kinds of incidents, particularly those involving a compromised user credential.
Respond	Response Planning	RS.AN-3	Forensics are performed.	CONTRIBUTE	Analytics	SPHEREboard's advanced analytics capabilities help identify root causes by utilizing the Account Detail Module to determine the impact perimeter of accounts, including databases, operating systems, applications, and administrative routes.
Respond	Response Planning	RS.MI-2	Incidents are mitigated	CONTRIBUTE	Reporting/ Remediation	At the heart of SPHEREboard's capabilities is intelligent discovery, asset ownership correlation, and control violation remediation. This empowers security administrators with essential information to initiate the Identity Hygiene process, adding an extra layer of control in managing compromised user accounts.