Publication	Category	Subcategory ID	Description	Support	Capability	Rationale
ISO 27001 – Annex A Controls	Annex A.9 - Access Control	Annex A.9.2- User access management	User access management (UAM) is the process of authorizing users to access specific system resources and defining the extent of that access. The purpose of the UAM controls is to ensure that only authorized users have access to the resources they need and only have the level of access they need.	CONTRIBUTE	Reporting/ Remediation	SPHEREboard's Ownership Engine enables organizations to: -Determine who should have access to information assets -Validate user roles and responsibilities SPHEREboard's Intelligent Discovery engine provides insight into: - Managing user accounts - Monitoring and auditing user access Leveraging it's Account Remediation Engine, SPHEREboard provides automation that can revoke access to information assets such as Active directory groups, account disabling, accounts vaulting.
ISO 27001 – Annex A Controls	Annex A.9 - Access Control	Annex A.9.2.1- User access provisioning	User access provisioning refers to the creation and management of user accounts, and the assignment of permissions and roles that determine what a user is able to do within the system.	CONTRIBUTE	Reporting/ Remediation	SPHEREboard provides a comprehensive functionality for identification and authentications by utilizing it's Assets Review Module capabilities. This functionality permits organizations validate and certify permissions and roles, review user access, and validate that access have been removed in a timely manner (60 days after termination)
ISO 27001 – Annex A Controls	Annex A.9 - Access Control	Annex A.9.2.3- Management of Privileged Access Rights	Ensure that all privileged access rights (PAR) in scope are managed in a defined and controlled manner. This includes identifying, defining, approving, documenting, and periodically reviewing all PARs.	CONTRIBUTE	Reporting/ Remediation	SPHEREboard's Account Discovery and Reporting Engine provide organizations with the level of access and sprawl permissions for individual user accounts to helps IAM organizations control account inventory following least privileged best practices. SPHEREboard's Asset Review Module enhances assets, accounts and identity attestation or certification.
ISO 27001 – Annex A Controls	Annex A.9 - Access Control	Annex A.9.2.5 Review of user access rights	This control aims to ensure that only authorized individuals have access to information and systems and that their access is appropriate for their needs. This helps to protect information from unauthorized access, use, disclosure, or loss.	CONTRIBUTE	Reporting/ Remediation	SPHEREboard's Asset Review capability permits organization's to review access rights and provides visibility into what type of access is required by each user and the need for any changes to access rights based on changes in the user's role or needs. By conducting a regular review of user access rights, organizations can protect information systems from unauthorized access.
ISO 27001 – Annex A Controls	Annex A.9 - Access Control		After the end of an employee's or contractor's assignment, their access rights to information and information processing facilities shall be removed or adjusted in a timely and controlled manner.	CONTRIBUTE	Analytics	Leveraging SPHEREboard, these are some of the measures that can be taken to controls the assignment, and removal of access rights: - Utilizing the Intelligent Discovery Engine you can create an inventory of authorized personnel and their access to all organizational assets. - Periodically review access rights for employees and contractors within the organizations. - Remove access rights when an employee or contractor leaves the organization (Leavers). SPHEREboard's Virtual Workers enable Information Security teams to perform this capability automatically.
ISO 27001 – Annex A Controls	Annex A.9 - Access Control	Annex A.9.4: System and application access control	This control is that it helps to prevent unauthorized access to systems and applications. in turn, helps to protect sensitive information and assets from being compromised	CONTRIBUTE	Analytics	SPHEREboard for Users and Groups assessment capabilities provide organizations with the ability to identify and limit what users can do with any given asset.
ISO 27001 – Annex A Controls	Annex A.9 - Access Control	A.9.4.3 Password management system	Password management system (iso 27001) defines three types of passwords: Administrator: used to access the system administrator functions. user: used to access the system user functions; and operator: used to access the system operator functions. The system also defines a fourth type of password, the shared password, which is used to share access to the system among multiple users.	CONTRIBUTE	Reporting/ Remediation	SPHEREboard's core capability, the Account Discovery Engine, and account vaulting in partnership with CyberArk enables your organization to reduce risk exposure by implementing privileged account onboarding into a password management system. As an end result, security teams can store, manage, and protect the following: -Administrator: used to access the system administrator functions - Share Accounts passwords -User: used to access the system user functions; and Operator for system operator functions
ISO 27001 – Annex A Controls	Annex A.8 - Asset Management	A.8.1.2 - Ownership of assets	This control is applicable to all organizations regardless of size or industry. In order to effectively implement this control, organizations should take the following steps: -Define the roles and responsibilities for asset ownership -Develop a process for tracking and approving changes to asset ownership -Ensure that all assets are accounted for and that unauthorized access is prevented	CONTRIBUTE	Analytics	SPHEREboard's Ownership Engine capabilities provide your organization with an automated, repetitive process to ensure that all organization assets (like Accounts, Groups, and Servers) as well as any associated data is only accessed by the correct individuals.
ISO 27001 – Annex A Controls	Annex A.8 - Asset Management	A.8.1.4 - Assets Return	This control is applicable to all organizations regardless of size or industry. In order to effectively implement this control, organizations should take the following steps: -Define the roles and responsibilities for asset ownership -Develop a process for tracking and approving changes to asset ownership -Ensure that all assets are accounted for and that unauthorized access is prevented	CONTRIBUTE	Analytics	SPHEREboard ownership capability provides organization with a repetitive process to ensure that all organization assets (Groups, accounts, servers…) as well as any associated data is access by the correct individuals.
ISO 27001 – Annex A Controls	Annex A.8 - Asset Management	Annex A.8.2.1- Information Classification	Classification of Information (iso 27001) is the process of identifying and classifying information assets. It is a fundamental security control that helps organizations protect their information from unauthorized disclosure. Classification of information is a three-step process: - Identify the information assets that need to be protected. - Classify the information assets based on their sensitivity. - Label the information assets with the appropriate security classification.	CONTRIBUTE	Reporting/ Remediation	SPHEREboard for BigID protects your critical data by discovering where it resides (at rest), accurately identifying ownership, and quickly remediating access. SPHEREboard for Big ID provides unrivaled expertise in locating and classifying Personally Identifiable Information (PII), financial data, sensitive data, and other key data.