Xton Access Manager for ISO 27001 Compliance

Contents

About ISO 27001

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization.

ISO 27001 (formally known as ISO/IEC 27001:2013) is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes. According to its documentation, ISO 27001 was developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system."

While ISO 27001 standard applies to various kind of organizations with sensitive data the following industries are typically implementing this standard the most.

In IT industry software development companies, cloud companies, and IT support companies are typically implementing ISO 27001 to assure their clients by proving a certificate that they are able to safeguard their clients' information in the best possible way or to comply with contractual security requirements from their main clients. In financial industry, banks, insurance companies, brokerage houses, and other financial institutions typically implement ISO 27001 when they want to comply with numerous laws and regulations. Telecommunication companies, including Internet providers, are trying to transparently protect the huge amount of data they handle, so naturally they look toward ISO 27001 as a framework that helps them do that. Government agencies looks for ISO 27001 to protect confidentiality, integrity and availability of the data they handle which is a cornerstone of the standard.

Several industries derive their own standards from ISO 27001 to tailor the standard requirements to their specific needs. Health organizations attempt to protect the data of their patients, pharmaceutical companies want to protect their R&D data, food processing companies protect their special recipes, manufacturing companies want to protect their knowledge on how certain parts are produced.

About Xton Access Manager

Xton Access Manager (XTAM) is an agentless, cross-platform privileged access management solution with unlimited licensing model built from the ground up with an enterprise feature set. Simple to implement, without your typical enterprise cost and effort.

A privileged account refers to non-individual, often shared, user accounts frequently used by machines for or by administrators to perform maintenance activities. Examples of such accounts include:

- Accounts used by machines to communicate between each other;
- Shared accounts shared by groups of people (external billing, corporate representatives);

- Accounts for Database Administrators, database schema, application pool owners, global administrators;
- Local computer accounts (root, administrator, tomcat, jenkins, jira);
- Built-in IoT accounts (sensors, printers, routers, coffee machines, cameras, beacons).

XTAM provides out-of-the-box features to discover, manage, access and monitor privileged accounts:

- A secure AES-256 encrypted Identity Vault to maintain total administrative control over all your passwords, certificates, key, files, secrets and privileged accounts.
- Privileged session recording to ensure all sessions are retained and can be used for diagnosis or forensic investigations.
- Integrated job and policy engine to automate password resets, privileged account discovery and repetitive tasks.
- Full system event and user audit trails that can trigger notifications and in-application alerts.

Recommended XTAM Workflow

XTAM supports multiple use cases and might be uses as a part of several security and productivity enhancement workflows. To help organizations to comply with ISO 27001 requirements we recommend the following workflow.

Step	Description
Discover	Discover privileged accounts in the network using XTAM discovery facilities.
Import	Import privileged accounts to XTAM vault from XTAM discovery process or from other sources using XTAM import facilities. Enter undiscovered privileges accounts into XTAM vault.
Manage	Define password rotation policy for imported or entered privileged accounts describing when and how the passwords should be rotated for groups of accounts or individual accounts. Grant and revoke access to privileged account records or groups of records in the XTAM vault for organization users and groups. Use Microsoft Active Directory, LDAP based user directory or local XTAM user directory as a directory of organization users and groups.
Rotate	Let XTAM engine to change password for managed accounts. Alternatively, change privileged accounts passwords manually and update the XTAM vault. After this step all privileged account activities will be performed using XTAM instance because nobody would know the password to access them.

Unlock	Authorize XTAM users to unlock passwords or certificates in XTAM vault when needed.
Access	Authorize XTAM users to connect to managed privileged accounts without disclosing credentials when needed using XTAM session manager.
Execute	Authorize XTAM users to execute privileged commands and scripts on managed information systems without disclosing credentials when needed using the XTAM job engine.
Monitor	Use XTAM notification facilities, audit log, history, job execution history and session history reports to monitor system activity. Stream system logs to your organization's SIEM system for global analysis.

Mapping XTAM Functions to the Standard Requirements

The following pages contain tables that summarize how XTAM functionality maps to the standard requirements to ensure compliance with the ISO 27001 framework. Note that only relevant product mappings are included here. Other requirements in this standard as well as ensuring compliance with areas of the organization security practices not covered by the XTAM recommended workflow, should be addressed separately.

Addressing § A.6 Organization of information security

Number	Control	Description
A.6.1.2	Segregation of duties	XTAM granular account-level permissions scheme enables fine control over segregation of privileged account duties among several users when accessing shared privileged accounts. XTAM's extensive notifications, logging mechanism and session recordings allows independent review of the individual user activity in the system.

Addressing § A.8 Asset management

Number	Control	Description
A.8.1.1	Inventory of assets	XTAM provides a discovery option to detect privileged accounts that should be used as a part of the inventory process.

Addressing § A.9 Access Control

Number	Control	Description
A.9.1.1	Access control policy	XTAM provides account-level permission controlled access of named user accounts or processes to shared privileged accounts. XTAM controls access to information systems based

		on the authorization of individual user or a process permissioned to access an information system even in case the system itself uses shared privileged accounts.
A.9.1.2	Access to networks and network services	XTAM provides account-level permission controlled access of named user accounts or processes to shared privileged accounts. XTAM controls access to information systems based on the authorization of an individual user or a process permissioned to access an information system even in case the system itself uses shared privileged accounts.
A.9.2.2	User access provisioning	XTAM allows individual user access provisioning for shared privileged accounts.
A.9.2.3	Management of privileged access rights	XTAM is specifically designed to control access to privileged resources, execution of privileged commands and to manage privileged rights for named or shared accounts.
A.9.2.5	Review of user access rights	XTAM allows review of individual user access rights for shared privileged accounts.
A.9.2.6	Removal or adjustment of access rights	XTAM enables management of individual user access to shared privileged resources with the option of policy based password rotation to prevent access to the privileged resource after expiration.
A.9.4.1	Information Access Restriction	XTAM enables individual user access control to shared privileged accounts.
A.9.4.2	Secure log-on procedures	XTAM enables a SSL protected HTTPS log-on procedure and traffic to provide access to managed privileged accounts.
A.9.4.3	Password management system	XTAM vault is an interactive WEB based enterprise password management system for managed privileged accounts with the option to automatically generate random complex passwords and reset passwords in its managed systems.
A.9.4.4	Use of privileged utility programs	XTAM controls access to managed shared privileged accounts based on the XTAM permissions defined for named users with the option to collect audit logs, send notifications and record privileged sessions. XTAM also allows permission controlled execution of selected privileged commands and scripts by a user with limited permissions.

Addressing § A.10 Cryptography

Number	Control	Description
A.10.1.2	Key management	XTAM vault enables permission controlled storage for security keys and certificates with an audit log and notifications when these assets are accessed.

Addressing § A.12 Operations security

Number	Control	Description
A.12.1.2	Change management	XTAM auditing and session recording capabilities as well as access control provide a basis for change management procedures for privileged accounts.
A.12.4.3	Administrator and operator logs	XTAM provides logging and session recording for shared privileged accounts mapped to the named users performing the operation.
A.12.5.1	Installation of software on operational systems	XTAM enables permission controlled access to privileged accounts capable to install new software on operational systems with audit logging and session recording capabilities.
A.12.6.2	Restrictions on software installation	XTAM enables permission controlled access to privileged accounts capable to install new software with audit logging and session recording capabilities

Addressing § A.15 Supplier Relationships

Number	Control	Description
A.15.2.1	Monitoring and review of supplier services	XTAM provides outsource suppliers permission controlled access to privileged accounts on sensitive information systems through the XTAM instance with the options to restrict access, commands and scripts execution while generating audit logs and session recordings.
A.15.2.2	Managing changes to supplier services	XTAM manages and monitors changes in information systems access available to suppliers.

Addressing § A.16 Information security incident management

Number	Control	Description
A.16.1.7	Collection of evidence	XTAM handles access and traffic to privileged accounts producing and preserving audit logs and session recordings involving sensitive information system activities.

Addressing § A.18 Compliance

Number	Control	Description
A.18.2.2	Compliance with security policies and standards	XTAM out-of-the-box functionality allows compliance with several critical information system access and discovery controls of multiple government, regional and industry regulations.

Conclusion

By partnering with Xton Technologies, organizations can address their compliance and security requirements as defined in ISO 27001 standard, leaving fewer gaps and improving efficiency over their privileged access management practices.

About Us

Philadelphia, PA based Xton Technologies makes it easy and affordable to have high security for your privileged access. Our enterprise grade XT Access Manager (XTAM) is purpose built to protect against malicious or accidental access from both within and beyond your firewall. The XTAM platform works across the corporate network, third party cloud infrastructure and is accessible using any modern browser on the desktop or mobile.

Xton Access Manager software is brought to you by industry veterans focusing on enterprise software development helping IT administrators in cyber security and content management areas since 2004. With more than 3000 customers around the globe and an experience in organic growth of a business from a small startup to an acquisition the team aligns its goals with the success of its clients.

The team goal is to disrupt the market with simple to install, to evaluate, to buy, to implement and to maintain software at the reasonable price point. The software that removes complexity barriers for the majority of businesses, large and small, to protects their IT infrastructure. Let's make the world better connected and more secure – together.

