strongdm

SOLUTION GUIDE

How strongDM Helps with ISO 27001 Compliance

ISO 27001 is a framework developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It outlines requirements to help organizations keep their information assets and those of their customers secure.

Below are the specific requirements where strongDM can help you achieve ISO 27001 certification.

	Requirement	Control	strongDM Feature
A.6	**Organization of information security**		
A.6.1 Internal organization		**To establish a management framework to initiate and control the implementation and operation of information security within the organization.**	
A.6.1.2 Segregation of duties		Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Segregation of duties can be enforced through granular role-based, attribute-based, or just-in-time access control policies - all of which are least privilege by default and do not allow for escalation of privileges.
A.6.2 Mobile devices and teleworking		**To ensure the security of teleworking and use of mobile devices.**	
A.6.2.2 Teleworking		A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	With strongDM, users are authenticated and authorized to access critical infrastructure. Credentials and keys are stored within strongDM or a secret store and unavailable to the end user.
A.8	**Asset management**		
A.8.1 Responsibility for assets		**To identify organizational assets and define appropriate protection responsibilities.**	
A.8.1.3 Acceptable use of assets		Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	The strongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes; access can be permanent or temporary. Comprehensive auditing of permissions is available for all access types.

Requirement	Control	strongDM Feature
A.8.2 Information classification	**To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.**	
A.8.2.3 Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	strongDM enforces least privilege by default. Role-based access control, attribute-based access control, and temporary access controls enable the right level of access. Comprehensive auditing of permissions shows who and what resources users have access to.
A.9 Access control		
A.9.1 Business requirements of access control	**To limit access to information and information processing facilities.**	
A.9.1.1 Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	strongDM uses a combination of user identities, network segmentation (making only gateways public), and roles/groups to generate and enforce access control rules.
A.9.1.2 Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	In the strongDM architecture, resources do not connect with each other. Users can only connect to what they are given access to and are unable to elevate their privileges to move horizontally through an organization's infrastructure.
A.9.2 User access management	**To ensure authorized user access and to prevent unauthorized access to systems and services.**	
A.9.2.1 User registration and de-registration	A formal user registration and deregistration process shall be implemented to enable assignment of access rights.	strongDM can federate with your identity provider or you can use strongDM's native authentication, which allows administrators to set minimum password requirements. Every user in strongDM is unique with an individual ID, and any shared accounts (i.e., service accounts, API keys, admin tokens) can have expirations or be automatically expired when the user that created the account(s) has been suspended or deleted.
A.9.2.2 User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Grant and revoke permanent or just-in-time access to resources through the strongDM admin UI, CLI, SDKs or through your identity provider.
A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	strongDM supports Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) policies. Additionally, strongDM enables you to grant temporary or just-in-time access with least privilege by default.

Requirement	Control	strongDM Feature
A.9.2.4 Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	strongDM stores credentials in a hardened AWS vault. We also support customer-owned-and-maintained secret stores that can be configured for access.
A.9.2.5 Review of user access rights	Asset owners shall review users' access rights at regular intervals.	strongDM provides comprehensive audit logs for all access to configured data sources.
A.9.2.6 Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Revoke permanent or just-in-time access to resources through the strongDM admin UI, CLI, SDKs or through your identity provider.
A.9.3 User responsibilities	**To make users accountable for safeguarding their authentication information.**	
A.9.3.1 Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	Credentials are never provided to the end user. The gateway authenticates to the final resource in the last hop using stored credentials, which are stored securely with strongDM or with an existing secret store (HashiCorp Vault, AWS Secrets Manager, GCP Secret Manager).
A.9.4 System and application access control	**To prevent unauthorized access to systems and applications.**	
A.9.4.1 Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	The strongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.
A.9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	strongDM allows you to authenticate and/or provision users & groups through your identity provider. You can also authenticate through strongDM with MFA.
A.9.4.3 Password management system	Password management systems shall be interactive and shall ensure quality passwords.	strongDM centralizes the storage of passwords either with strongDM or by using a customer-managed secret store. Passwords are never disclosed to end users or needed to grant access to systems.

Requirement	Control	strongDM Feature
A.9.4.4 Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	strongDM enables customers to grant automated access to systems via service accounts and benefit from the same robust access and audit controls they use for regular users. Permission levels in strongDM restrict the types of access that tokens and service accounts can have in order to prevent privilege escalation from these systems.
A.10 Cryptography		
A.10.1 Cryptographic controls	**To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.**	
A.10.1.1 Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Because strongDM uses strong cryptographic controls for the encryption and storage of authentication secrets, we can help support a customer's policy on cryptographic controls. strongDM also supports the storage of credentials and keys in secret stores, which reduce the need to transmit any secrets outside of an organization's system or network.
A.10.1.2 Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	All secrets and credentials are obfuscated with encryption keys stored in a hardened vault. The end user does not have or need access to the cryptographic keys to access resources.
A.11 Physical and environmental security		
A.11.2 Equipment	**To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.**	
A.11.2.6 Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Access to critical infrastructure occurs only through strongDM, which authenticates the users through your identity provider or through strongDM with MFA.
A.12 Operations security		
A.12.1 Change management	**To ensure correct and secure operations of information processing facilities.**	
A.12.1.1 Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	strongDM can be a part of a standard documented operating procedure for accessing infrastructure.

Requirement	Control	strongDM Feature
A.12.1.2 Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Grant temporary access, with least privilege by default, for managing access to critical infrastructure. Integrate testing, approving, and implementing changes for emergency situations (e.g., grant temporary access within applications like Slack and Microsoft Teams).
A.12.1.4 Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	In the strongDM architecture, resources do not connect with each other. Users can only connect to what they are given access to and are unable to elevate their privileges to move horizontally through an organization's infrastructure.
A.12.4 Logging and monitoring	**To record events and generate evidence.**	
A.12.4.1 Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	strongDM provides comprehensive audit logs for all access to configured data sources, which can assist in evaluations and investigations of security incidents.
A.12.4.2 Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	strongDM tunnels all connections between local clients and strongDM's proxy server through a single TLS 1.2-secured TCP connection and enhances traditional TLS handshakes with its own secrets between each node. There are 3 levels of encryption that can be enabled: default encryption, public key and local logging, and non-shared key encryption.
A.12.4.3 Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	strongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.
A.12.7 Information systems audit considerations	**To minimize the impact of audit activities on operational systems.**	
A.12.7.1 Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.	strongDM can support comprehensive auditing of systems and access in a way that doesn't affect the target systems at all, since all activity and audit logs are processed on the strongDM platform and not on individual systems.
A.13 Communications security		
A.13.1 Network security management	**To ensure the protection of information in networks and its supporting information processing facilities.**	

Requirement	Control	strongDM Feature
A.13.1.1 Network controls	Networks must be managed and controlled in order to protect information within systems and applications.	strongDM uses network segmentation and only makes gateways public to generate and enforce access control rules.
A.13.1.2 Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	In the strongDM architecture, resources do not connect with each other. Users can only connect to what they are given access to and are unable to elevate their privileges to move horizontally through an organization's infrastructure.
A.13.1.3 Segregation in networks	Groups of information services, users and information systems should be segregated on networks.	By reducing the need for resources to connect to each other, strongDM can help customers implement network segmentation. Resource tagging can help customers implement environment segmentation and RBAC.
A.14 System acquisition, development and maintenance		
A.14.1 Security requirements of information systems	**To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.**	
A.14.1.2 Securing application services on public networks	The information involved in application services passing over public networks need to be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	The use of encrypted connections at all layers of the strongDM platform ensures that any communications between users and resources are encrypted over public networks.
A.14.2 Security in development and support processes	**To ensure that information security is designed and implemented within the development lifecycle of information systems.**	
A.14.2.1 Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	User access privileges are derived from their assigned roles with the exception of temporary access and no role assigned. The strongDM AccessBot can also be used to grant temporary access within applications like Slack and Microsoft Teams.
A.14.2.6 Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	User access privileges are derived from their assigned roles or attributes with a comprehensive audit trail to detect the who, what, where, and when of every interaction with backend infrastructure.
A.14.2.7 Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	strongDM manages and audits all activities, whether employees, contractors, or other third-parties, regarding access to backend infrastructure.

Requirement	Control	strongDM Feature
A.16 Information security incident management		
A.16.1 Management of information security incidents and improvements	**To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.**	
A.16.1.4 Assessment of and decision on information security events	Information security events must be assessed and it shall be decided if they should be classified as information security incidents.	By providing detailed audit logs, strongDM can support a customer's assessment of an information security event.
A.16.1.7 Collection of evidence	The organization shall define and apply controls for the identification, collection, acquisition and preservation of information, which can serve as evidence.	strongDM provides comprehensive audit logs for all access to configured data sources, which can assist in evaluations and investigations of security incidents.
A.17 Redundancies		
A.17.2 Redundancies	**To ensure availability of information processing facilities.**	
A.17.2.1 Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	strongDM is architected and deployed as a highly available service whereby redundancy is built-in and uptime and disaster recovery times are predictable.
A.18 Compliance		
A.18.1 Compliance with legal and contractual requirements	**To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.**	
A.18.1.4 Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	The strongDM implementation fully leverages Authenticated Encryption with Associated Data (AEAD) via the KMS Encryption Context. All credential decryption events are written to a tamper-hardened audit log that is owned by a separate AWS account. Your gateway is the only thing that can decrypt credentials on an end user's behalf.
A.18.2 Information security reviews	**To ensure information security is implemented and operated in accordance with the organizational policies and procedures.**	
A.18.2.3 Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	By logging all of the queries that are run on target systems and optionally exporting strongDM logs to a SIEM, customers can detect potential areas of noncompliance.