MAPPING TO ISO 27001 CONTROLS

Thycotic helps organizations easily meet ISO 27001 requirements

OVERVIEW

The International Organization for Standardization (ISO) has put forth the ISO 27001 standard to help organizations implement an Information Security Management System which "preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed."

ISO 27001 is divided into 10 main sections:

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement.

> "Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable with an organization that claims conformity to this International Standard"

This standard serves as a broad and flexible framework that can apply to organizations of all industry types and sizes. In order for an organization to claim they are in compliance with ISO 27001, they must meet all requirements in sections 4 through 10 above.

Many of these sections highlight policies, planning, and procedures at the organization level - which are outside of the scope this document. This document maps out how Thycotic can help organizations meet certain security controls outlined in Annex SL. The controls annex applies to the following two sections:

> The organization shall define and apply an information security risk treatment process to:
>
> Section 6.1.3 (b) - determine all controls that are necessary to implement the information security risk treatment options chosen;
>
> Section 6.1.3 (c) - compare the controls determined in 6.1.3 (b) above with those in Annex A and verify that no necessary controls have been omitted;
>
> Section 6.1.3 (d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and (c) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;

The rest of this document outlines the controls that Thycotic can help organizations implement from the Annex. Each section highlights whether Thycotic can help your organization meet the control, or if the control is not applicable to our solution set. We have also included a checklist table at the end of this document to review control compatability at a glance.

ISO 27001 CONTROL

A.5 INFORMATION SECURITY POLICIES

A.5.1 Management direction of information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

A.5.1.1 Policies for Information Security - A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.

- Thycotic has a password policy template that can help organizations meet policy creation requirements for Information Security, as a portion of the overall information security policy.

A.5.1.2 Review of the policies for information security - The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

A.6 ORGANZATION OF INFORMATION SECURITY

A.6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

A.6.1.1 Information Security Roles and Responsibilities - All information security responsibilities shall be defined and allocated.

- Thycotic solutions rely on a Role Based Access Control (RBAC) that can help organzations define and allocate responsibilities set forth in the information security policy.

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.

- Thycotic solutions rely on a Role Based Access Control (RBAC) that can help organzations segregate access to assets based on a user's role in the organzation defined in the policy and solution. Approval workflows can be created to give limited access to users as needed.

A.6.1.3 Contact with Authorities - Appropriate contacts with relevant authorities shall be maintained

A.6.1.4 Contact with special interest groups - Appropriate contacts with special interest groups or other specialist

security forums and professional associations shall be maintained.
A.6.1.5 Information security in project management - Information security shall be addressed in project management, regardless of the type of the project.

- Access to any system that is required during projects can be controlled using Thycotic solutions.

A.6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

A.6.2.1 Mobile device policy - A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.

A.6.2.2 Telworking - A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

- Thycotic solutions, specifically Secret Server and Privilege Manager for Windows, can help organizations implement security measures to protect access to systems by remote users. In addition, our solutions can be extended to manage remote locations with Distributed Engines.

A.7 HUMAN RESOURCE SECURITY

A.7.1 Prior to Employment

Objective: To ensure that employees and contractors understand their responsibilities and are suit- able for the roles for which they are considered.

A.7.1.1 Screening - Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the per- ceived risks.

A.7.1.2 Terms and conditions of employment - The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.

A.7.2 During employment

Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

A.7.2.1 Management responsibilities - Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

- If Thycotic's solutions are implemented as a requirement for access to protected systems, then all employees and contractors will be automatically in compliance with information security controls applicable to the sections that Thycotic solutions help organizations meet.

A.7.2.2 Information security awareness, education and training- All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

- Thycotic has a number of free and paid training material to help organizations strengthen their information security awareness, education and training programs. Thycotic offers a self paced, Privileged Password Security Certification Training course, for free that also provides 1 CPE credit upon completion.

A.7.2.3 Disciplinary process - There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

A.7.3 Termination and change of employment

Objective: To protect the organization's interests as part of the process of changing or terminating employment.

A.7.3.1 Termination or change of employment responsibilities - Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.

- Terminated employees can be a great vulnerability to an organization's information security, as such, our solutions have extensive reporting and auditing trails that can provide insight into every protected system that employee had access to. In addition, if privileged accounts are protected with Secret Server, all passwords that the employee had access to can be changed with a single administrative action from the User Audit report.

A.8 ASSET MANAGEMENT

A.8.1 Responsibility for assets

Objective: To identify organizational assets and define appropriate protection responsibilities.

A.8.1.1 Inventory of assets - Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

- Thycotic solutions, specifically Secret Server and Privilege Manager for Windows, can help organization discover, monitor, and inventory privileged accounts and Windows/Unix endpoints.

A.8.1.2 Ownership of assets - Assets maintained in the inventory shall be owned.

- Assets discovered through Thycotic solutions can be automatically brought into the respective solution for continued management and ownership of the asset.

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.

- Thycotic solutions can be implemented to enforce policies for information security set forth by the organization for acceptable use of protected and controlled assets.

A.8.1.4 Return of assets - All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

A.8.2 Information classification

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

- Thycotic solutions do not directly manage data or information; we can however, help you ensure that access to systems with protected data is controlled.

A.8.2.1 Classification of information - Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification**.**

A.8.2.2 Labeling of information - An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by 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.

A.8.3 Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

A.8.3.1 Management of removable media - Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

A.8.3.2 Disposal of media - Media shall be disposed of securely when no longer required, using formal procedures.

A.8.3.3 Physical media transfer - Media containing information shall be protected against unauthor- ized access, misuse or corruption during transportation.

A.9 ACCESS CONTROL

A.9.1 Business requirements of access control

Objective: 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.

Thycotic solutions can help organizations implement strict access controls with Secret Server. Secret Server, leveraging the RBAC system and Session Proxies, can help organization strictly control access to any number of protected systems. Additional controls are available such as Session Recording and Request Access workflows.

A.9.1.2 Access of 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.

Thycotic solutions can help organizations implement strict access controls with Secret Server. Secret Server, leveraging the RBAC system and Session Proxies, can help organization strictly control access to any number of protected systems. Additional controls are available such as Session Recording and Request Access workflows.

A.9.2 User access management

Objective: 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 de-registration process shall be implemented to enable assignment of access rights.

Thycotic is not involved in Identity Provisioning (features common with IAM solutions) but we integrate with a number of Identity Provisioning systems, such as Sailpoint.

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.

User access can be provisioned directly in Secret Server or Privilege Manager for Windows. Additionally, access rights can be removed with a single administrative action.

A.9.2.3 Management of privileged access right - The allocation and use of privileged access rights shall be restricted and controlled.

Secret Server is a Privileged Account Management (PAM) solution, built to help organizations discover, protect, and manage privileged accounts and access. Access to privileged accounts is tightly monitored and audited, and additional controls can be added to ensure stronger protections of the most sensitive of privileged accounts.

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.

Thycotic solutions can integrate with a number of authentication systems, specifically any system that supports SAML 2.0.

A.9.2.5 Review of user access rights - Asset owners shall review users' access rights at regular intervals.

Administrators and Auditors can review access rights of all users in the Thycotic solutions. Additionally, our solution can integrate with Identity Management platforms, such as Sailpoint, in order to provide a single view of an identity and their access.

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.

User access can be directly controled within the solution, and all access to both our solutions, as well as protected accounts and endpoints, can be revoked with a single administrative action.

A.9.3 User responsibilities

Objective: To prevent unauthorized access to systems and applications.

A.9.3.1 User responsibilities - To make users accountable for safeguarding their authentication information.

Thycotic solutions integrate with a number of 2 Factor Authentication systems to help users stay accountable for safeguarding their authentication information into the system.

A.9.4 System and application access control

Objective: 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.

Any system protected and controlled through Thycotic solutions can help organizations restrict access to these systems.

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.

Session proxy can be leveraged with Secret Server to ensure that all access to systems are passed through the solution.

A.9.4.3 Password management system - Password management systems shall be interactive and shall ensure quality passwords.

Thycotic Solutions, both Secret Server and Password Reset Servers, can help organizations enforce strict password policy requirements on systems as well as in Active Directory.

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.

- Privilege Manager for Windows/Unix, can help organizations implement strict application controls to ensure that powerful programs are closely controled depending on who is running the utility and what system they are attempting to run the application on.

A.9.4.5 Access control to program source code - Access to program source code shall be restricted.

- If the source code is stored on a system, access to that system can be closely protected using Thycotic solutions to ensure that only the right people have the required access.

A.10 CRYPTOGRAPHY

A.10.1 Cryptographic controls

Objective: 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.

- All sensitive data stored in Thycotic solutions are encrypted at rest and in transit.

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.

- Secret Server can be used to store cryptographic keys only. Thycotic solutions are not leveraged for encrypting of large sources of data, but invidivual keys can be stored for safe keeping or backups.

A.11 PHYSICAL AND ENVIRONMENTAL SECURITY

A.11.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

A.11.1.1 Physical security perimeter - Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

A.11.1.2 Physical entry controls - Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

A.11.1.3 Securing offices, rooms and facilities - Physical security for offices, rooms and facilities shall be designed

and applied.

A.11.1.4 Protecting against external and environmental threats - Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

A.11.1.5 Working in secure areas - Procedures for working in secure areas shall be designed and applied.

A.11.1.6 Delivery and loading areas - Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

A.11.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

A.11.2.1 Equipment siting and protection - Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

A.11.2.2 Supporting utilities - Equipment shall be protected from power failures and other dis- ruptions caused by failures in supporting utilities.

A.11.2.3 Cabling security - Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

A.11.2.4 Equipment maintenance - Equipment shall be correctly maintained to ensure its continued availability and integrity.

A.11.2.5 Removal of assets - Equipment, information or software shall not be taken off-site without prior authorization.

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.

A.11.2.7 Secure disposal or re-use of equipment - All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

A.11.2.8 Unattended user equipment - Users shall ensure that unattended equipment has appropriate protection.

A.11.2.9 Clear desk and clear screen policy - A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

A.12 OPERATIONS SECURITY

A.12.1 Operational procedures and responsibilities

Objective: 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.

A.12.1.2 Change management - Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

A.12.1.3 Capacity management - The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

A.12.1.4 Seperation 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.

A.12.2 Protection from malware

Objective: To ensure that information and information processing facilities are protected against malware.

A.12.2.1 Controls against malware - Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

- In addition to anti-malware software, we encourage the use of our Privilege Manager for Windows solution to leverage Application Whitelisting/Blacklisting/Graylisting to prohibit unknown malware threats from running on an endpoint.

A.12.3 Backup

Objective: To protect against loss of data.

A.12.3.1 Information backup - Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

- A number of Disaster Recovery options are available, to ensure Thycotic solutions meet your information backups requirements.

A.12.4 Logging and monitoring

Objective: 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.

- Thycotic solutions have extensive reporting and auditing capabilities, including event logging and subscriptions.

A.12.4.2 Protection of log information - Logging facilities and log information shall be protected against tampering and unauthorized access.

- Logs in Secret Server can be protected with both RBAC as well as Dual Control requirements.

A.12.4.3 Administrator and operator logs - System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

- All administrative actions are logged and available for reporting and audits.

A.12.4.4 Clock synchronization - The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.

- Secret Server points to the IIS server clock for synchronization with other systems.

A.12.5 Control of operational software

Objective: To ensure the integrity of operational systems.

A.12.5.1 Installation of software on operational systems - Procedures shall be implemented to control the installation of software on operational systems..

- Privilege Manager for Windows can help organizations implement application whitelist, blacklist, and graylists for granular control on what applications are allowed to be installed or updated on protected systems. Thus protecting against malicious applications while keeping employees productive

A.12.6 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

A.12.6.1 Management of systems audit controls - Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

- Secret Server can integrate with a number of vulnerability management systems, such as Tenable, and provide privileged credentials for a deeper vulnerability scan of target systems.

A.12.6.2 Restrictions on software installation - Rules governing the installation of software by users shall be established and implemented.

- Privilege Manager for Windows can help organizations implement application whitelist, blacklist, and graylists

for granular control on what applications are allowed to be installed or updated on protected systems.

A.12.7 Information systems audit considerations

Objective: 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.

- Thycotic solutions have extensive reporting and audit histories to help organizations meet their audit requirements.

A.13 COMMUNICATIONS SECURITY

A.13.1 Network Security Management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

A.13.1.1 Network controls - Networks shall be managed and controlled to protect information in systems and applications.

- Privileged accounts that provide adminsitrative access on network devices can be managed and controled through Secret Server.

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.

- Privileged accounts that provide adminsitrative access on network devices can be managed and controled through Secret Server.

A.13.1.3 Segregation in networks - Groups of information services, users and information systems shall be segregated on networks.

A.13.2 Information Transfer

Objective: To maintain the security of information transferred within an organization and with any external entity.

A.13.2.1 Information transfer policies and procedures - Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

A.13.2.2 Agreements on information transfer - Agreements shall address the secure transfer of business information between the organization and external parties.

A.13.2.3 Electronic messaging - Information involved in electronic messaging shall be appropriately protected.

A.13.2.4 Confidentiality or non-disclosure agreements - Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of informa- tion shall be identified, regularly reviewed and documented.

A.14 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

A.14.1 Security requirements of information systems

Objective: 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.14.1.1 Information security requirements analysis and specification - The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

Thycotic solutions can be used to help discover new privileged accounts as they are added to protected systems, or as new systems are added to the network, thus keeping an updated audit of privileged systems and preventing back door accounts.

A.14.1.2 Securing application services on public networks - Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

A.14.1.3 Protecting application services transactions - Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauhorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

A.14.2 Security in development and support processes

Objective: 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 estabished and applied to developments within the organization.

A.14.2.2 System changes control procedures - Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

A.14.2.3 Technical review of applications after operating platform changes - When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

A.14.2.4 Restrictions on changes to software packages - Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

A.14.2.5 Secure system engineering principles - Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

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.

- Thycotic solutions can be used to protect development environments in the same manner that production/live environments are protected.

A.14.2.7 Outsourced development - The organization shall supervise and monitor the activity of outsourced system development.

- Secret Server can provide monitoring and control capabilities for outsourced system developers that require access to systems on the organization's network.

A.14.2.8 System security testing - Testing of security functionality shall be carried out during development.

A.14.2.9 System acceptance testing - Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

A.14.3 Test data

Objective: To ensure the protection of data used for testing

A.14.3.1 Protection of test data - Test data shall be selected carefully, protected and controlled.

A.15 SUPPLIER RELATIONSHIPS

A.15.1 Information security policy for supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

A.15.1.1 Information security policy for supplier relationships - Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

A.15.1.2 Addressing security within supplier agreements - All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

A.15.1.3 Information and communications technology supply chain - Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

A.15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

A.15.2.1 Monitoring and review of supplier services - Organizations shall regularly monitor, review and audit supplier service delivery.

A.15.2.2 Managing changes to supplier services - Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

A.16 INFORMATION SECURITY INCIDENT MANAGEMENT

A.16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A.16.1.1 Responsibilities and procedures - Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

A.16.1.2 Reporting information security events - Information security events shall be reported through appropriate management channels as quickly as possible.

- Security events related to privileged accounts & access, as well as application control on endpoints, can be routed directly to the appropriate channels based on configuration settings in Thycotic solutions.

A.16.1.3 Reporting information security weaknesses - Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

A.16.1.4 Assessment of and decision on information security events - Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

- For privileged accounts, Thycotic's Privileged Behavior Analytics, can help alert, prioritize, and analyze information security events related to privileged accounts and access.

A.16.1.5 Response to information security incidents - Information security incidents shall be responded to in accordance with the documented procedures.

A.16.1.6 Learning from information security incidents - Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

A.16.1.7 Collection of evidence - The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

- Thycotic solutions maintain an extensive audit history to help organizations collect and preserve security event related information as evidence.

A.17 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

A.17.1 Information security continuity

Objective: Information security continuity shall be embedded in the organization's business continuity management systems.

A.17.1.1 Planning information security continuity - The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

A.17.1.2 Implementing information security continuity - The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

A.17.1.3 Verify, review and evaluate information security continuitiy - The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

A.17.2 Redundancies

Objective: 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.

- Thycotic solutions can be deployed in high availability and geo-redunandant setups to help implement the availability of protected information systems.

A.18 COMPLIANCE

A.18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to infor- mation security and of any security requirements.

A.18.1.1 Identification of applicable legislation and contractual requirements - All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.

A.18.1.2 Intellectual propery rights - Appropriate procedures shall be implemented to ensure compli- ance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary soft- ware products.

A.18.1.3 Protection of records - Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business 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.

- Thycotic's Secret Server comes with a Dual Control feature for reports and recorded sessions, requiring two sets of authentication before a report can be viewed. Dual Control is used to help facilitate the protection of personally identifiable information that may be contained in a report or recorded session in Secret Server.

A.18.1.5 Regulation of cryptographic controls - Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

A.18.2 Information security reviews

Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

A.18.2.1 Independent review of information security - The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

A.18.2.2 Compliance with security policies and standards - Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

A.18.2.3 Technical compliance review - Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

ISO 27001 CONTROL CHECKLIST

A.5 Information Security Policies

		Helps Meet
A.5.1.1	Policies for Information Security	✓
A.5.1.2	Review of the policies for information security	

A.6 Organization of Information Security

		Helps Meet
A.6.1.1	Policies for Information Security	✓
A.6.1.2	Review of the policies for information security	✓
A.6.1.3	Policies for Information Security	
A.6.1.4	Review of the policies for information security	
A.6.2.1	Mobile device policy	
A.6.2.2	Teleworking	✓

A.7 Human Resource Security

		Helps Meet
A.7.1.1	Priort to employment	
A.7.1.2	Terms and conditions of employment	
A.7.2.1	Management responsibilities	✓
A.7.2.2	Information security awareness, education and training	✓
A.7.2.3	Disciplinary process	
A.7.3.1	Termination or change of employment responsibilities	✓

A.8 Asset Management

		Helps Meet
A.8.1.1	Inventory of assets	✓

A.8.1.2	Ownership of assets	✓
A.8.1.3	Acceptable use of assets	✓
A.8.1.4	Return of assets	
A.8.2.1	Classification of information	
A.8.2.2	Labeling of information	
A.8.2.3	Handling of assetes	
A.8.3.1	Management of removable media	
A.8.3.2	Disposal of media	
A.8.3.3	Physical media transfer	

A.9 Access Control

		Helps Meet
A.9.1.1	Access control policy	✓
A.9.1.2	Access of networks and network services	✓
A.9.2.1	User registration and de-registration	✓
A.9.2.2	User access provisioning	✓
A.9.2.3	Management of privileged access rights	✓
A.9.2.4	Management of secret authentication informatoin of users	✓
A.9.2.5	Review of user access rights	✓
A.9.2.6	Removal or adjustment of access rights	✓
A.9.3.1	User responsibilities	✓
A.9.4.1	Information access restriction	✓
A.9.4.2	Secure log-on procedure	✓
A.9.4.3	Password management system	✓
A.9.4.4	Use of privileged utility programs	✓
A.9.4.5	Access control to program source code	✓

A.10 Cryptography

		Helps Meet
.10.1.1	Policy on the use of cryptographic controls	✓
A.10.1.2	Key Management	✓

A.11 Physical and Environmental Security

		Helps Meet
A.11.1.1	Physical security perimeter	
A.11.1.2	Physical entry control	

A.11.1.3	Securing offices, rooms and facilities	
A.11.1.4	Protecting against external and environmental threats	
A.11.1.5	Working in secure areas	
A.11.1.6	Delivery and loading areas	
A.11.2.1	Equipment siting and protection	
A.11.2.2	Supporting utilities	
A.11.2.3	Cabling security	
A.11.2.4	Equipment maintenance	
A.11.2.5	Removal of assets	
A.11.2.6	Security of equipment and assets off-premises	
A.11.2.7	Secure disposal or re-use of equipment	
A.11.2.8	Unattended user equipment	
A.11.2.9	Clear desk and clear screen policy	

A.12 Operations Security

		Helps Meet
A.12.1.1	Documented operating procedures	
A.12.1.2	Change management	
A.12.1.3	Capacity management	
A.12.1.4	Seperation of development, testing and operational environments	
A.12.2.1	Controls against malware	✓
A.12.3.1	Information backup	✓
A.12.4.1	Event logging	✓
A.12.4.2	Protection of log information	✓
A.12.4.3	Administrator and operator logs	✓
A.12.4.4	Clock synchronization	✓
A.12.5.1	Installation of software on operational systems	✓
A.12.6.1	Management of systems audit controls	✓
A.12.6.2	Restrictions on software installation	✓
A.12.7.1	Information systems audit controls	✓

A.13 Communications Security

		Helps Meet
A.13.1.1	Network Controls	✓
A.13.1.2	Security of network services	✓
A.13.1.3	Segregation in networks	
A.13.2.1	Information transfer policies and procedures	
A.13.2.2	Agreements on information transfer	

A.13.2.3	Electronic messaging	
A.13.2.4	Confidentiality or non-disclosure agreements	

A.14 System acquisition, development and maintenance

		Helps Meet
A.14.1.1	Information security requirements analysis and specification	✓
A.14.1.2	Securign application services on public networks	
A.14.1.3	Protecting application services transactions	
A.14.2.1	Secure development policy	
A.14.2.2	System changes control procedures	
A.14.2.3	Technical review of applications after operating platform changes	
A.14.2.4	Restrictions on changes to software packages	
A.14.2.5	Secure system engineering principles	
A.14.2.6	Secure development environment	✓
A.14.2.7	Outsoruced development	✓
A.14.2.8	System security testing	
A.14.2.9	System acceptance testing	
A.14.3.1	Protection of test data	

A.15 Supplier Relationships

		Helps Meet
A.15.1.1	Information security policy for supplier relationships	✓
A.15.1.2	Addressing security within supplier agreements	✓
A.15.1.3	Information and communications technology supply chain	✓
A.15.2.1	Monitoring and review of supplier services	✓
A.15.2.2	Managing changes to supplier sevices	✓

A.16 Information Security Incident Management

		Helps Meet
A.16.1.1	Responsibilities and procedures	✓
A.16.1.2	Reporting information security events	✓
A.16.1.3	Reporting information security weaknesses	
A.16.1.4	Assessment of and decision on information security events	✓
A.16.1.5	Response to information security incidents	
A.16.1.6	Learning from information security incidents	
A.16.1.7	Collection of evidence	✓

A.17 Information Security Aspects of Business Continuity Management

		Helps Meet
A.17.1.1	Planning information security continuity	
A.17.1.2	Implementing informatoin security continuity	✓
A.17.1.3	Verify, review and evaluate information security continuity	✓
A.17.2.1	Availability of information processing facilities	✓

A.18 Compliance

		Helps Meet
A.18.1.1	Indentification of applicable legislation and contractual requirements	
A.18.1.2	Intellectual property rights	
A.18.1.3	Protection of records	
A.18.1.4	Privacy and protection of personally identifiable information	✓
A.18.1.5	Regulation of cryptographic controls	✓
A.18.2.1	Independent review of information security	✓
A.18.2.2	Compliance with security policies and standards	✓
A.18.2.3	Technical compliance review	✓