GuardWare INSIGHT helps organisations conform to ISO/IEC 27001:2022

1 Content

2 Executive Summary

ISO/IEC 27001 is an internationally recognized standard for information security management systems (ISMS). It provides a systematic approach to managing sensitive company information so that it remains secure. This includes the people, processes, and IT systems by applying a risk management process.

Annex A of ISO 27001 provides a set of controls that can be used to manage information security risks.

Annex A of ISO/IEC 27001:2022 provides a comprehensive set of security controls that organizations can implement to address information security risks. These controls are organized into four themes, each covering different aspects of information security management. These controls cover areas such as organizational policies, physical security, personnel security, and technology. The 2022 version of the standard has streamlined and reorganized the controls compared to previous versions.

GuardWare INSIGHT is applicable as below.

- Organizational Controls – GuardWare Applicable in 18 controls out of 37
- People Controls – GuardWare Applicable in 6 controls out of 8
- Technological Controls – GuardWare Applicable in 20 controls out of 34

Below is a summary mapping of GuardWare INSIGHT to the various controls followed by detailed explanation.

2.1 Summary Mapping:

Organizational Controls – GuardWare Applicable in 18 controls out of 37

Control Name / Title	GuardWare INSIGHT - Applicability
Policies for Information Security	Applicable
Information Security Roles and Responsibilities	Not applicable.
Segregation of Duties	Applicable

Management Responsibilities	Not applicable.
Contact with Authorities	Not applicable.
Contact with Special Interest Groups	Not applicable.
Threat Intelligence	Applicable
Information Security in Project Management	Not applicable.
Inventory of Information and Other Associated Assets	Applicable
Acceptable Use of Information and Other Associated Assets	Applicable
Return of Assets	Applicable
Classification of Information	Applicable
Labelling of Information	Applicable
Information Transfer	Applicable
Access Control	Applicable
Identity Management	Not applicable.
Authentication Information	Not applicable.
Access Rights	Not applicable.
Information Security in Supplier Relationships	Not applicable.
Addressing Information Security within Supplier Agreements	Not applicable.
Managing Information Security in the ICT Supply Chain	Not applicable.
Monitoring, Review and Change Management of Supplier Services	Not applicable.
Information Security for Use of Cloud Services	Applicable
Information Security Incident Management Planning and Preparation	Applicable
Assessment and Decision on Information Security Events	Not applicable.
Response to Information Security Incidents	Applicable
Learning From Information Security Incidents	Not applicable.
Collection of Evidence	Applicable
Information Security During Disruption	Applicable
ICT Readiness for Business Continuity	Not applicable.
Legal, Statutory, Regulatory and Contractual Requirements	Applicable
Intellectual Property Rights	Not applicable.
Protection of Records	Applicable
Privacy and Protection of PII	Applicable
Independent Review of Information Security	Not applicable.
Compliance With Policies, Rules and Standards	Applicable
Documented Operating Procedures Standards for Information Security	Not applicable.

People Controls – GuardWare Applicable in 6 controls out of 8

Control Name / Title	GuardWare INSIGHT - Applicability
Screening	Not applicable.
Terms and Conditions of Employment	Not applicable.
Information Security Awareness, Education and Training	Applicable
Disciplinary Process	Applicable
Responsibilities After Termination or Change of Employment	Applicable
Confidentiality or Non-Disclosure Agreements	Applicable
Remote Working	Applicable
Information Security Event Reporting	Applicable

Technological Controls – GuardWare Applicable in 20 controls out of 34

Control Name / Title	GuardWare INSIGHT - Applicability
User Endpoint Devices	Applicable
Privileged Access Rights	Applicable
Information Access Restriction	Applicable
Access to Source Code	Applicable
Secure Authentication	Not applicable.
Capacity Management	Applicable
Protection Against Malware	Applicable
Management of Technical Vulnerabilities	Applicable
Configuration Management	Applicable
Information Deletion	Applicable
Data Masking	Not applicable.
Data Leakage Prevention	Applicable
Information Backup	Not applicable
Redundancy of Information Processing Facilities	Not applicable
Logging	Applicable
Monitoring Activities	Applicable
Clock Synchronization	Not applicable
Use of Privileged Utility Programs	Applicable
Installation of Software on Operational Systems	Applicable
Networks Security	Not applicable
Security of Network Services	Applicable
Segregation of Networks	Not applicable
Web filtering	Applicable
Use of Cryptography	Not applicable
Secure Development Life Cycle	Not applicable
Application Security Requirements	Not applicable
Secure System Architecture and Engineering Principles	Not applicable
Secure Coding	Not applicable
Security Testing in Development and Acceptance	Not applicable
Outsourced Development	Not applicable
Separation of Development, Test and Production Environments	Applicable
Change Management	Applicable
Test Information	Applicable
Protection of Information Systems During Audit Testing	Applicable

3 Detailed Mapping

3.1 Organizational Controls (37 controls):

These controls focus on the overall governance and management of information security within the organization. Key areas include information security policies, roles and responsibilities, asset management, supplier relationships, and incident management.

Control Name / Title	Description	GuardWare INSIGHT - Applicability
Policies for Information Security	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur. ISO 27001:2022 Annex A 5.1 Policies for Information Security	GuardWare INSIGHT serves as a critical enforcement tool for information security policies. By automating data governance processes, including data identification, classification, secure handling, and secure disposal, GuardWare facilitates compliance with established policies. The system also generates comprehensive statistical reports, aiding management in reviewing and improving the effectiveness of these policies.
Information Security Roles and Responsibilities	Information security roles and responsibilities should be defined and allocated according to the organisation needs. ISO27001:2022 Annex A 5.2 Information Security Roles and Responsibilities	Not applicable.
Segregation of Duties	Conflicting duties and conflicting areas of responsibility should be segregated. ISO 27001:2022 Annex A 5.3 Segregation of Duties	GuardWare INSIGHT partially addresses this requirement by monitoring access controls to ensure that only authorized users access information, thereby mitigating the risks associated with conflicting duties.
Management Responsibilities	Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization. ISO 27001 Annex A 5.4 Management Responsibilities	Not applicable.
Contact with Authorities	The organisation should establish and maintain contact with relevant authorities. ISO 27001 Annex A 5.5 Contact with Authorities	Not applicable.

Contact with Special Interest Groups	The purpose of ISO 27001 Annex A 5.6 is to ensure the appropriate flow of information takes place with respect to information security.	Not applicable.
Threat Intelligence	ISO 27001 Annex A 5.7 is preventive, detective and corrective control that ensure you provide awareness of the organisations threat environment so that the appropriate mitigation actions can be taken.	GuardWare INSIGHT acts as a preventive, detective, and corrective control, enhancing the organization's awareness of its threat environment and enabling appropriate mitigation actions for the secure handling of sensitive data.
Information Security in Project Management	Information security should be integrated into project management. ISO 27001:2022 Annex A 5.8 Information security in project management	Not applicable.
Inventory of Information and Other Associated Assets	An inventory of information and other associated assets, including owners, should be developed and maintained. ISO 27001:2022 Annex A 5.9 Inventory of information and other associated assets	GuardWare INSIGHT assists in maintaining an inventory of information by conducting data discovery scans, ensuring comprehensive asset management.
Acceptable Use of Information and Other Associated Assets	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented. ISO 27001:2022 Annex A 5.10 Acceptable use of information and other associated assets	GuardWare INSIGHT is the critical compliance and governance tool designed to enforce the Acceptable Use of Information and its Related Assets. It monitors all access, movement, and storage of sensitive data, alerting the user if any misuse occurs, indicating a violation of the company's Acceptable Use Policies.
Return of Assets	Personnel and other interested parties as appropriate should return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement. ISO 27001:2022 Annex A 5.11 Return of Assets	From an information security perspective, GuardWare INSIGHT ensures that all data within a user's possession is accounted for, enabling organizations to enforce the return or destruction of unauthorized data as per their directives.
Classification of Information	Information should be classified according to the information security needs of the organisation based on confidentiality, integrity, availability and relevant interested party requirements. ISO 27001:2022 Annex A 5.12 Classification of Information	GuardWare INSIGHT plays a pivotal role in the classification process by identifying and categorizing stored information through data discovery scans, aligning with organizational security needs.
Labelling of Information	An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organisation. ISO 27001:2022 Annex A 5.13 Labelling Of Information	GuardWare INSIGHT partially supports this requirement by ensuring that sensitive data is appropriately labelled during its lifecycle within the organization.

Information Transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organisation and between the organisation and other parties. ISO 27001:2022 Annex A 5.14 Information Transfer	GuardWare INSIGHT ensures that information transfer, both within the organization and with third parties, adheres to secure, company-defined procedures, maintaining data integrity during transfer.
Access Control	Rules to control physical and logical access to information and other associated assets should be established	GuardWare INSIGHT enforces access control policies by continuously monitoring and verifying that only authorized users have access to critical files and information.
Identity Management	The full lifecycle of identities should be managed. ISO 27001:2022 Annex A 5.16 Identity Management.	Not applicable.
Authentication Information	Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information. ISO 27001:2022 Annex A 5.17 Authentication Information	Not applicable.
Access Rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy on and rules for access control. ISO 27001:2022 Annex A 5.18 Access Rights	Not applicable.
Information Security in Supplier Relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services. ISO 27001:2022 Annex A 5.19 Information Security In Supplier Relationships	Not applicable.
Addressing Information Security within Supplier Agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship. ISO 27001:2022 Annex A 5.20 Addressing information security within supplier agreements	Not applicable.
Managing Information Security in the ICT Supply Chain	Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain. ISO 27001:2022 Annex A 5.21 Managing information security in the ICT supply chain.	Not applicable.
Monitoring, Review and Change Management	The organisation should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Not applicable.

of Supplier Services	ISO 27001:2022 Annex A 5.22 Monitor, review and change management of supplier services	
Information Security for Use of Cloud Services	Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organisation's information security requirements. ISO27001:2022 Annex A 5.23 Information security for use of cloud services	GuardWare INSIGHT ensures that only company-approved cloud services are utilized, and through the GW Cloud Connector, it monitors environments like O365 and SharePoint for any risky activities.
Information Security Incident Management Planning and Preparation	The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities. ISO 27001:2022 Annex A 5.24 Information security incident management planning and preparation	GuardWare INSIGHT functions as an essential tool in incident detection and evidence gathering, facilitating the organization's readiness for information security incidents.
Assessment and Decision on Information Security Events	The organisation should assess information security events and decide if they are to be categorised as information security incidents. ISO 27001:2022 Annex A 5.25 Assessment and decision on information security events	Not applicable.
Response to Information Security Incidents	Information security incidents should be responded to in accordance with the documented procedures. ISO 27001:2022 Annex A 5.26 Response to information security incidents	GuardWare INSIGHT serves as an enforcement mechanism to ensure that corrective actions are effectively applied in response to information security incidents.
Learning From Information Security Incidents	Knowledge gained from information security incidents should be used to strengthen and improve the information security controls. ISO 27001:2022 Annex A 5.27 Learning from information security incidents	Not applicable.
Collection of Evidence	The organisation should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events. ISO 27001:2022 Annex A 5.28 Collection of Evidence	GuardWare INSIGHT is instrumental in the detection of incidents and the collection and preservation of evidence, ensuring compliance with security protocols.
Information Security During Disruption	The organisation should plan how to maintain information security at an appropriate level during disruption. ISO 27001:2022 Annex A 5.29 Information Security During Disruption	GuardWare INSIGHT is a crucial tool that safeguards against the mishandling of information during disruptions, ensuring continuous protection.
ICT Readiness for Business Continuity	ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Not applicable.

	ISO 27001:2022 Annex A 5.30 ICT Readiness for Business Continuity	
Legal, Statutory, Regulatory and Contractual Requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organisations approach to meet these requirements should be identified, documented and kept up to date. ISO 27001:2022 Annex A 5.31 Legal, statutory, regulatory and contractual requirements	GuardWare INSIGHT ensures compliance with relevant legal, statutory, regulatory, and contractual requirements by acting as a robust enforcement tool.
Intellectual Property Rights	The organisation should implement appropriate procedures to protect intellectual property rights. ISO 27001:2022 Annex A 5.32 Intellectual Property Rights.	Not applicable.
Protection of Records	Records should be protected from loss, destruction, falsification, unauthorised access and unauthorised release. ISO 27001:2022 Annex A 5.33	GuardWare INSIGHT is a monitoring and alerting tool that prevents the unauthorized access, loss, or release of sensitive records, safeguarding organizational data.
Privacy and Protection of PII	The organisation should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements. ISO 27001:2022 Annex A 5.34 Privacy and Protection of PII	GuardWare INSIGHT aids in identifying and securing the storage of sensitive Personally Identifiable Information (PII), ensuring compliance with applicable laws and regulations.
Independent Review of Information Security	The organisations approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur. ISO 27001:2022 Annex A 5.35 Independent review of information security	Not applicable.
Compliance With Policies, Rules and Standards	Compliance with the organisations information security policy, topic-specific policies, rules and standards should be regularly reviewed. ISO 27001:2022 Annex A 5.36 Compliance with policies, rules and standards for information security	GuardWare INSIGHT monitors and ensures user adherence to organizational policies, rules, and standards, supporting continuous compliance.
Documented Operating Procedures Standards for Information Security	Operating procedures for information processing facilities should be documented and made available to personnel who need them. ISO 27001:2022 Annex A 5.37	Not applicable.

3.2 People Controls (8 controls):

These controls focus on ensuring that employees and contractors are aware of and adhere to the organization's information security requirements. This includes training, awareness, and disciplinary processes related to information security.

Control Name / Title	Description	GuardWare INSIGHT - Applicability
Screening	Background verification checks on all candidates to become personnel should be carried out prior to joining the organisation and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. ISO27001:2022 Annex A 6.1 Screening	Not applicable.
Terms and Conditions of Employment	The employment contractual agreements should state the personnel's and the organisations responsibilities for information security. ISO 27001:2022 Annex A 6.2 Terms of Employment	Not applicable.
Information Security Awareness, Education and Training	Personnel of the organisation and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organisations information security policy, topic-specific policies and procedures, as relevant for their job function. ISO 27001:2022 Annex A 6.3 Information Security Awareness, Education and Training	GuardWare INSIGHT, through the Real-Time Automated User Education module (SASI), enhances information security awareness and training. The system's automated auditing of user actions provides valuable insights, supporting ongoing education and awareness initiatives tailored to specific job functions.
Disciplinary Process	A disciplinary process should be formalised and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation. ISO 27001:2022 Annex A 6.4 Disciplinary Process	GuardWare INSIGHT functions as an essential user monitoring tool, gathering evidence when employees violate information security policies. This evidence supports the disciplinary process, ensuring appropriate actions are taken in response to infractions.
Responsibilities After Termination or Change of Employment	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.	GuardWare INSIGHT plays a critical role during employee offboarding or role changes by monitoring and enforcing information security responsibilities. The system identifies sensitive information in the possession of departing staff and

	ISO 27001:2022 Annex A 6.5 Responsibilities after termination or change of employment	ensures compliance with non-disclosure agreements (NDAs) and other ongoing obligations.
Confidentiality or Non-Disclosure Agreements	Confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties. ISO 27001:2022 Annex A 6.6 Confidentiality or Non-Disclosure Agreements	GuardWare INSIGHT actively monitors for potential breaches of confidentiality or non-disclosure agreements by alerting when sensitive information covered under an NDA is mishandled, such as being forwarded to personal email accounts or uploaded to unauthorized third-party sites.
Remote Working	Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises. ISO 27001:2022 Annex A 6.7 Remote Working	GuardWare INSIGHT is particularly effective in securing remote work environments. The endpoint agent monitors all access, transfer, and storage of information, including web and application usage, and alerts in case of risky behaviour. The system also oversees VPN usage and privileged access commands, while the GW Cloud Monitor extends coverage to O365 environments, safeguarding company data accessed from personal devices.
Information Security Event Reporting	The organisation should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner. ISO 27001:2022 Annex A 6.8 Information Security Event Reporting	GuardWare INSIGHT provides real-time monitoring of data access, movement, and storage, generating timely alerts when risks are detected. Alerts can be routed to the IT department or directly to information owners, ensuring a swift response. Additionally, the Real-Time Automated User Education module not only educates users on risky actions but also offers a mechanism to report security concerns, fostering a culture of shared responsibility for information security across the organization.

3.3 Technological Controls (34 controls):

These controls focus on the technical measures that need to be implemented to protect information assets. This includes areas like access control, cryptography, security of network services, and software development.

Control Name / Title	Description	GuardWare INSIGHT - Applicability
User Endpoint Devices	Information stored on, processed by or accessible via user endpoint devices should be protected. ISO 27001:2022 Annex A 8.1 User Endpoint Devices	GuardWare INSIGHT's endpoint agent comprehensively monitors all information transfers and storage activities, ensuring robust oversight. It includes monitoring web and application access, with alerts for potential security risks, such as visits to unsafe websites or the use of high-risk applications. Furthermore, the agent oversees the use of unsecured connections, including VPN usage, and privileged access to ensure compliance with security protocols. The GuardWare INSIGHT Cloud Monitor extends these protections to the O365 environment, monitoring email and SharePoint activities, thereby safeguarding corporate data even when accessed via personal devices.
Privileged Access Rights	The allocation and use of privileged access rights should be restricted and managed. ISO 27001:2022 Annex A 8.2 Privileged Access Rights	GuardWare INSIGHT monitors privileged access by administrators through vigilant oversight of the usage of privileged applications and administrative commands to ensure that all activities adhere to the organization's security policies.
Information Access Restriction	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control. ISO27001:2022 Annex A 8.3 Information Access Restriction	GuardWare INSIGHT fully supports the implementation of access control policies for sensitive information. It ensures a complete, non-repudiable audit trail, providing alerts to information owners and IT security for reviewing any instances of unauthorized access. This guarantees that only authorized personnel have access to sensitive data.

Access to Source Code	Read and write access to source code, development tools and software libraries should be appropriately managed. ISO 27001:2022 Annex A 8.4 Access To Source Code	Partially applicable - GuardWare INSIGHT provides monitoring of development applications to manage access to source code, ensuring compliance with security standards.
Secure Authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control. ISO 27001:2022 Annex A 8.5 Secure Authentication	Not applicable.
Capacity Management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements. ISO 27001:2022 Annex A 8.6 Capacity Management	Partially applicable - GuardWare INSIGHT conducts software and hardware audits. Software audits assess the usage of various applications across the organization, identifying whether licenses are fully utilized or if additional ones are necessary. Hardware audits ensure endpoint devices operate optimally, detecting memory shortages and determining if cleanup is required.
Protection Against Malware	Protection against malware should be implemented and supported by appropriate user awareness. ISO 27001:2022 Annex A 8.7 Protection Against Malware	Partially applicable - GuardWare INSIGHT provides protection against malware by monitoring the installation and usage of high-risk applications, thereby mitigating the potential for infections.
Management of Technical Vulnerabilities	Information about technical vulnerabilities of information systems in use should be obtained, the organisations exposure to such vulnerabilities should be evaluated and appropriate measures should be taken. ISO 27001:2022 Annex A 8.8 Management of Technical Vulnerabilities	GuardWare INSIGHT identifies technical vulnerabilities, particularly focusing on the risky handling of data. Upon identification, these risks are addressed through appropriate technical reconfigurations of network security and IT management tools, ensuring ongoing protection.
Configuration Management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed. ISO 27001:2022 Annex A 8.9 Configuration Management	Not applicable

Information Deletion	The ISO 27001 standard defines ISO 27001 Annex A 8.10 as: Information stored in information systems, devices or in any other storage media should be deleted when no longer required. – ISO 27001:2022 Annex A 8.10 Information Deletion	GuardWare INSIGHT provides comprehensive Data Discovery features that enable organizations to scan local devices and file servers for stored data. This process enforces data availability and retention policies by identifying data that is no longer required and should be deleted. It also ensures that all data is accounted for, properly backed up, and not stored in insecure locations such as local device hard disks, which are typically not backed up.
Data Masking	Data masking should be used in accordance with the organisation's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration. ISO 27001:2022 Annex A 8.11 Data Masking	Not applicable.
Data Leakage Prevention	ISO 27001:2002 Annex A 8.12 is preventive control and a detective control that is to detect and prevent the unauthorised disclosure and extraction of information by individuals or systems.	GuardWare INSIGHT offers extensive Data Leak Prevention capabilities, monitoring all access, movement, and storage of data across various channels. This includes emails, printing, web uploads, cloud applications, mobile synchronization, cloud shares, chat connections, work-from-home user logins, administrator logins, privileged application usage, and more. GuardWare INSIGHT also tracks time spent on applications and websites, monitors installed software, controls media usage, and ensures the security of data access on personal devices.
Information Backup	The ISO 27001 standard defines ISO 27001 Annex A 8.13 as: Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup. – ISO 27001:2022 Annex A 8.13 Information Backup	Not applicable

Redundancy of Information Processing Facilities	The ISO 27001 standard defines ISO 27001 Annex A 8.14 as: Information processing facilities should be implemented with redundancy sufficient to meet availability ISO27001:2022 Annex A 8.14 Redundancy of Information Processing Facilities	Not applicable
Logging	The ISO 27001 standard defines ISO 27001 Annex A 8.15 as: Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed. ISO27001:2022 Annex A 8.15 Logging	GuardWare INSIGHT provides comprehensive event logging, capturing detailed information on all risk-related incidents, including user devices, dates, times, incident types, applications involved, and data impacted. All logs are protected, encrypted, and immutable, with a full audit trail of administrative access. The system offers multiple alert mechanisms to ensure that any risks are promptly identified and addressed.
Monitoring Activities	The ISO 27001 standard defines ISO 27001 Annex A 8.16 as: Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents. ISO27001:2022 Annex A 8.16 Monitoring	GuardWare INSIGHT provides comprehensive event logging, capturing detailed information on all risk-related incidents, including user devices, dates, times, incident types, applications involved, and data impacted. All logs are protected, encrypted, and immutable, with a full audit trail of administrative access. The system offers multiple alert mechanisms to ensure that any risks are promptly identified and addressed.
Clock Synchronization	The clocks of information processing systems used by the organisation should be synchronised to approved time sources. ISO27001:2022 Annex A 8.17 Clock Synchronisation	Not applicable
Use of Privileged Utility Programs	The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled ISO27001:2022 Annex A 8.18 Use of Privileged Utility Programs	GuardWare INSIGHT monitors privileged access by administrators through vigilant oversight of the usage of privileged applications and administrative commands to ensure that all activities adhere to the organization's security policies.

Installation of Software on Operational Systems	Procedures and measures should be implemented to securely manage software installation on operational systems. ISO27001:2022 Annex A 8.19 Installation of Software on Operational Systems	Partially applicable - GuardWare INSIGHT monitors the usage and installation of potentially harmful applications on operational systems, helping to prevent infections and maintain system integrity.
Networks Security	Networks and network devices should be secured, managed and controlled to protect information in systems and applications. ISO27001:2022 Annex A 8.20 Network Security	Not applicable
Security of Network Services	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored. ISO27001:2022 Annex A 8.21 Security of Network Services	Partially applicable - GuardWare INSIGHT monitors users and devices when they operate outside the corporate network, such as in home environments, providing a layer of security for remote operations.
Segregation of Networks	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored. ISO27001:2022 Annex A 8.22 Segregation of Networks	Not applicable
Web filtering	Access to external websites should be managed to reduce exposure to malicious content. ISO27001:2022 Annex A 8.23 Web Filtering	Partially applicable - GuardWare INSIGHT partially addresses web filtering by monitoring web access and providing the capability to block access to non-organizational websites, thereby reducing exposure to malicious content.
Use of Cryptography	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented. ISO27001:2022 Annex A 8.24 Use of Cryptography	Not applicable
Secure Development Life Cycle	Rules for the secure development of software and systems should be established and applied.	Not applicable

	ISO27001:2022 Annex A 8.25 Secure Development Life Cycle	
Application Security Requirements	The organisation should direct, monitor and review the activities related to outsourced system development. ISO27001:2022 Annex A 8.30 Outsourced Development	Not applicable
Secure System Architecture and Engineering Principles	Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities. ISO27001:2022 Annex A 8.27 Secure Systems Architecture and Engineering Principles	Not applicable
Secure Coding	Secure coding principles should be applied to software development. ISO27001:2022 Annex A 8.28 Secure Coding	Not applicable
Security Testing in Development and Acceptance	Security testing processes should be defined and implemented in the development life cycle. ISO27001:2022 Annex A 8.29 Security Testing in Development and Acceptance	Not applicable
Outsourced Development	The organisation should direct, monitor and review the activities related to outsourced system development. ISO27001:2022 Annex A 8.30 Outsourced Development	Not applicable
Separation of Development, Test and Production Environments	Rules for the secure development of software and systems should be established and applied. ISO27001:2022 Annex A 31 Separation of Development, Test and Production Environments	GuardWare INSIGHT ensures the separation of development, test, and production environments by monitoring access to applications, websites, and information flows, ensuring that each environment is secured and isolated according to best practices.
Change Management		GuardWare INSIGHT facilitates change management by ensuring the security of information during staff transitions, application updates, or other process-related modifications, maintaining the

		integrity of the organization's information assets.
Test Information	Test information should be appropriately selected, protected and managed. ISO27001:2022 Annex A 8.33 Test Information	GuardWare INSIGHT ensures that test information is appropriately selected, protected, and managed, preventing the mishandling of operational data during testing phases.
Protection of Information Systems During Audit Testing	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management. ISO27001:2022 Annex A 8.34 Protection of information systems during audit testing	GuardWare INSIGHT safeguards operational information during audit testing, ensuring that data is not mishandled and that security controls remain effective throughout the assessment process.