Statement Of Applicability

Project Name:	ISO/IEC 27001: 2022
Version:	2
Status:	Complete
Date Created:	11/11/2025
Date Updated:	13/11/2025

Clause	Clause Description	Is Applicable?	Justification	Control Description
A.5	**Organizational controls.**			
A.5.1	**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.	True	The organisation understands Information Security Policies are a vital component of an effective ISMS and these will be used as the foundation for the ISMS. Policies are required to set the direction, show intent, and formally document the ISMS. Staff need to be aware of these policies to improve the effectiveness of the ISMS. Our policies will help us to protect Sensitive Data, Legal and Regulatory Compliance, Risk Management, Prevent Data Breaches, Maintaining Reputation and Trust, Operational Continuity and Employee Awareness and Training. The control is required due to a contractual obligation	Thomas' Information Security Policy outlines the organisation's commitment to information security, starting from board-level and extending to every employee, contractor, and partner working with Team Thomas. The policy has been reviewed, tailored to our specific requirements, and signed off by the Senior Leadership Team. Subordinate policies have also been developed to further enhance Thomas' commitment to information security. These policies have been processed through our document management system, ensuring they are reviewed by relevant stakeholders and formally approved.
A.5.2	**Information security roles and responsibilities.** Information security roles and responsibilities should be defined and allocated according to the organization needs.	True	Clear roles and responsibilities across the organization are crucial for the success of the ISMS. Formally identifying roles and responsibilities ensures an effective ISMS implementation, maintenance and maturity, guides compliance and Conformity, identifies and manages risks, provides communication and coordination, focuses on training and awareness, and ensures the continual monitoring and improvement of our ISMS. The control is needed to mitigate inherent risk to control objectives	The ISO Leadership Committee has assigned specific roles within the ISMS to ensure that they are effectively assigned and manage risks. Key roles are documented and any changes to scope or roles are reviewed and approved during the IMS Management Meetings.
A.5.3	**Segregation of duties.** Conflicting duties and conflicting areas of responsibility should be segregated.	True	Segregation of duties is integral to maintaining our robust ISMS. It ensures that critical tasks such as access control, change management, risk assessment, and other security-related functions are appropriately distributed among different roles or individuals. This distribution helps us establish a system of checks and balances, reducing our overall risk exposure and enhancing the integrity and reliability of our ISMS. The control is needed to mitigate inherent risk to control objectives The control is needed according to best practices	Employees are placed into groups based on the role that they will be fulfilling and given access to applications that they require access to be able to function in their job role. Roles are segregated in order to prevent security and fraud risks across specific applications using roles to ensure segregation of duties. Employees changing job roles must have this reviewed to ensure access risks are managed so that they continue to only have access to applications and data that they require access to. Email and tickets are used to notify the relevant team of joiners, movers and leavers to manage access requirements.
A.5.4	**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.	True	Management responsibilities are pivotal for the successful implementation and maintenance of our ISMS. Our Management Teams commitment, involvement, and active support ensure our ISMS is part of our culture and ensures the effectiveness of the security measures in place. Our management team provides leadership and direction, supports resource allocation, role models effective risk management, ensures compliance and conformance, champions continuous improvement, oversees communication and training and prioritises incident response and preparedness.	Management are involved in relevant aspects of the management system, with a focus on setting the tone and governance around how the system is implemented and managed. The ISO Leadership Team were involved in the development of the security policy and signed off on relevant documents. In addition, the risk management and implementation of controls were all agreed with management, and they are involved in regular ISO Management Review meetings, but also kept informed of any information security related issues.

Clause	Clause Description	Is Applicable?	Justification	Control Description
			The control is needed to mitigate inherent risk to control objectives	
A.5.5	**Contact with authorities.** The organization should establish and maintain contact with relevant authorities.	True	Maintaining a channel of contact with relevant authorities is crucial for our organisation's ISMS, ensuring compliance, staying informed about legal requirements, accessing resources and guidance, and establishing a cooperative approach towards securing sensitive data and systems. The control is required due to a contractual obligation	A list of contacts in case of information security or data privacy related issues within the contact list contained in the Business Continuity Management Policy. The list aims to ensure correct and efficient contact with relevant stakeholders and the following types of contacts are included: • Emergency Services • Information Commissioners Office • Financial regulators • British Psychological Society • Corporate Owners This list is updated upon review annually and links to other relevant areas. The Disaster Recovery documents also have additional contacts for use within their scope.
A.5.6	**Contact with special interest groups.** The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	True	Special interest groups keep our organisation up to date in industry insights and best practices, facilitate networking and collaboration, provide education and training, provide opportunities for advocacy and influence, give us access to information sharing and threat intelligence, provide professional development and sometimes give validation and recognition. The control is needed according to best practices	The organisation encourages memberships of professional bodies, and security and industry specialist forums, by any member of staff. In addition, the organisation has joined the following specific groups for information sharing and threat management: • Hardware and software vendors as special interest groups in regard to security vulnerability patch and configuration management. • National Cyber Security Centre – Latest advice & guidance related to Cyber Security: https://www.ncsc.gov.uk • Information Commissioner's Office – Privacy & data protection guidance for organizations • Microsoft – security notifications and product updates – Weekly Digest: Microsoft Service Updates – Major Change Update Notification
A.5.7	**Threat intelligence.** Information relating to information security threats should be collected and analysed to produce threat intelligence.	True	The organisation leverage threat intelligence to fortify our information security practices and align with the ISO 27001 standard. Threat Intelligence provides the necessary insights the organisation needs to be proactive in addressing potential threats and vulnerabilities, ensuring a more robust and adaptive security posture. The control is needed according to best practices	The organisation uses a combination of manual and automated methods to gather threat intelligence, specifically gathering information from credible sources (vendors and other security groups) and automated solutions which constantly update the list of threats and suggested actions.
A.5.8	**Information security in project management.** Information security should be integrated into project management.	True	The organisation incorporates information security in project management to help create a more secure project environment, reducing vulnerabilities, and ensure that security is not an afterthought but an integral part of the project's success. The control is needed to mitigate inherent risk to control objectives	The organisation has integrated Information security into project management processes where Information security risks are identified and addressed as early in the process as possible. During specific project meetings, or as part of Sprint cycles, teams discuss new features and any information security risks and perform an information security review before any production release. When using any external service or provider, information security review is performed, and their project management activities must be aligned to ours.
A.5.9	**Inventory of information and other associated assets.** An inventory of information and other associated assets, including owners, should be developed and maintained.	True	The organisation maintains an accurate and up-to-date inventory of information and associated assets for effective information security management. Our software and data asset register provides the foundation for our risk assessment, resource allocation, incident response, and compliance, contributing to our robust security posture. The control is needed to mitigate inherent risk to control objectives The control is needed according to best practices	The organisation has asset registers to cover both physical and informational assets. The lists are amended each time a new laptop is bought, changed or retired, or a new software tool is implemented. The lists are reviewed regularly to ensure they are up-to-date.

Clause	Clause Description	Is Applicable?	Justification	Control Description
A.5.10	**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.	True	By establishing and consistently enforcing our acceptable use of technology and workspace policy, the organisation significantly reduce the risks associated with information and asset misuse, ensuring a more secure and compliant environment. Our policy fosters a culture of responsible information handling and contributes to our robust security posture. The control is needed to mitigate inherent risk to control objectives	Acceptable usage of asset rules is added in the Acceptable Use of Technology and Workspace Policy. All users are informed of their responsibilities and rules related to the usage of assets through communications and appropriate security awareness and are monitored for compliance.
A.5.11	**Return of assets.** Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	True	Asset return is an essential component of information security and asset management within our organisation. When employees leave the organisation or when assets are no longer needed, a structured and secure asset return process is critical to protect sensitive information, comply with regulations, control cost, and ensure efficient resource utilisation, all contributing to our secure and well-managed organisational environment. The control is needed to mitigate inherent risk to control objectives The control is needed according to best practices	The Off-boarding process is kicked off as soon as a member of the team or contractor hands in their notice. As part of the off-boarding process a checklist is then used to ensure that all steps are followed when a staff member leaves. The checklist includes provision for the return of hardware assets, such as laptops, and security assets, such as fobs. The list also ensures the organisation removes access to systems and buildings.
A.5.12	**Classification of information.** Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	True	The organisation classifies information by categorising data according to its sensitivity, importance, and the level of protection required, to ensure data protection, access control, risk management, compliance, and resource allocation, contributing significantly to our overall security posture. The control is needed to mitigate inherent risk to control objectives	The organizations Information Classification Policy defines how information is classified, managed and labelled across its lifecycle. Employees are required during onboarding to have read and understood the Information Classification Policy.
A.5.13	**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 organization.	True	The organisation labels our data to reflect the classification, sensitivity, and handling requirements of that information. This is so that the sensitivity of that data is communicated, access control is guided, compliance is facilitated, and our culture of information security is promoted. The control is needed to mitigate inherent risk to control objectives	The organisation has an information classification policy that defines how employees classify documents that they work on with the different labels that have been defined. All new employees are trained during onboarding as well as all employees on an annual basis to ensure that they are aware of the information classification policy, processes and the correct labelling hierarchy.
A.5.14	**Information transfer.** Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	True	The organisation ensures secure information transfer so that the organisation maintains the CIA (Confidentiality, Integrity and Availability) of data. By implementing encryption, secure protocols, access controls, and user education, the organisation effectively manages information transfer securely and mitigate potential risks associated with data movement. The control is related to a regulatory or certification requirement	Information transfer controls are designed to address risks related to how information is transferred. The Information Classification and Information Management policies define the rules applied. All projects where critical information is shared with third parties must assess the third parties for risks, implement controls in line with the process and identify major issues which need to be resolved with an agreed timeline. Any transfer of personal data must be covered by appropriate data protection clauses either as a separate document or as part of contractual documentation. The organisation does not use email to supply critical data, the primary recommendation for data transfer is through the use of SharePoint, with approved external domains being given rights for information to be shared. In addition, physical media is avoided and should never be used. Confidential information should only be disclosed to third parties under an NDA or confidentiality clause in the relevant contract. Contracts, agreements and other relevant documents will be stored electronically and secured.
A.5.15	**Access control.** Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.	True	Access control is one of the primary focus areas of our ISMS. Our securely designed access controls protect our information and associated devices and infrastructure against unauthorised access and information access. A defined access control policy is in place to set the direction and principles for access control.	Access Management is defined in an Access Control Policy which aims to set the principles and is the basis for the access control process throughout the business. All users requiring access follow a user access process which governs all aspects of access, from requesting access, access changes and termination of access with the following guiding principles: Deny-by-default, Need-to-know, Least privilege, Role-based Access Control (RBAC).

Clause	Clause Description	Is Applicable?	Justification	Control Description
			The control is needed to mitigate inherent risk to control objectives The control is needed according to best practices	User registration and de-registration controls are formalized in the Access Control Policy and Authorised Access to Information Procedure. This process is managed by a request process where access is requested and authorized by designated people. The deregistration process is matched to the termination process and ensures that staff access is removed when staff are terminated or leave.
A.5.16	**Identity management.** The full life cycle of identities should be managed.	True	Identity management plays an important role in ensuring that the right people have the appropriate access to information and systems. Our identity management practices allow us to strengthen our access control measures, enhance information security, manage the lifecycle of our user identities, ensure appropriate access, and reduce the risk of unauthorised access or security breaches. The control is needed to mitigate inherent risk to control objectives The control is needed according to best practices	User registration and de- registration controls are formalized in the Access Control Policy and Authorised Access to Information Procedure. This process is managed by a request process where access is requested and authorized by designated people. The deregistration process is matched to the termination process and ensures that staff access is removed when staff are terminated or leave.
A.5.17	**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.	True	Authentication information are the credentials and mechanisms the organisation uses to verify the identity of individuals or entities seeking access to our systems, networks, or applications. These help us enhance the security of authentication information, reduce the risk of unauthorised access, and improve our security and resilience. The control is needed according to best practices The control is needed to mitigate inherent risk to control objectives	The allocation of secret authentication information, such as passwords, is required to be governed through a formal process. Users agree to follow the organizations practices when using secret authentication information. When first given access, the users are given a temporary password which they are required to change on first login and password controls are enforced through automated solutions. When the need to change a password occurs this is done through a self-service reset, or a temporary password will be set for the user to login then immediately change. Secret authentication information should be kept confidential and not written down, or stored in, an unsecure manner. and under no circumstance should be shared. The organisation follows best practice, using the default Microsoft password rules. Passwords are not required to be changed unless there is a concern or compromise, then the password will be changed immediately.
A.5.18	**Access rights.** Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	True	Access rights, refer to the level of privileges or permissions granted to individuals or entities within our organisation, to access specific resources, systems, or information. By effectively managing access rights, the organisation reduces the risk of unauthorised access and enhance the confidentiality and integrity of our information. The control is needed to mitigate inherent risk to control objectives The control is needed according to best practices	Access Management is defined in an Access Control Policy which sets the direction and principles for access control. When staff are first given roles or change roles or require different access then a process is in place to ensure that this access is documented and authorised and modified to ensure its added and removed where required. For terminated staff or resignations access is removed when its required. User access is reviewed on a bi- annual basis by the admins/system owners to ensure that authorized users have correct access and that no expired users or other unauthorized use is occurring. Any evidence is kept by the admins and stored in a ticket or SharePoint folder.
A.5.19	**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.	True	Due to the amount of service providers/external parties used by the organisation (including cloud providers) and the risks identified these controls are vital for the success of the ISMS. Suppliers may have access to the organisation's information and controls need to be applied to them. The control is needed to mitigate inherent risk to control objectives	There is a Supplier Management Policy in place which outlines the following core security aspects: 1) Security Principles 2) Access Control 3) Risk Assessments 4) Change Management The policy defines the process for suppliers, and all applicable suppliers are managed as per this policy which is implemented and reviewed and updated on an annual basis. All supplier details are documented in the software asset register or approved suppliers list together with confirmation that these steps have been followed.
A.5.20	**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.	True	Due to the amount of service providers/external parties used by us (including cloud providers), and the risks identified, these controls are vital for the success of the ISMS. Suppliers may have access to our information, so controls need to be applied. By addressing information security in supplier relationships through a comprehensive and	Suppliers have the following key sections covered within their contracts: the work and its scope; confidentiality; privacy; legal and regulatory requirements e.g. adherence to GDPR and or other applicable legislation; data security and protection; intellectual property rights; limitation of liability; payment terms and termination. In addition, suppliers are further

Clause	Clause Description	Is Applicable?	Justification	Control Description
			proactive approach, the organisation minimises risks, protects sensitive information, and fosters a secure and collaborative environment with external partners, contributing to the overall resilience of our ISMS. The control is needed to mitigate inherent risk to control objectives	questioned around the organisations security and privacy policies to ensure that they meet to the required levels. In addition, the organisation will get them to sign NDA agreements, if this is not covered within the contractual terms. The contract in place is reinforced by adding Data Protection Addendums to ensure compliance with Privacy requirements (i.e. GDPR). All supplier details are documented in the supplier registers.
A.5.21	**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.	True	Managing information security in our supply chain is crucial for us to ensure the protection of our sensitive information throughout the procurement and sourcing processes. Our robust approach to information security in the supply chain helps us to mitigate risks, enhance resilience and information security, and foster a secure and resilient supply chain ecosystem. The control is needed to mitigate inherent risk to control objectives	Suppliers (including ICT suppliers) have the following key sections covered within their contracts: the work and its scope; confidentiality; privacy; legal and regulatory requirements e.g. adherence to GDPR and or other applicable legislation; data security and protection; intellectual property rights; limitation of liability; payment terms and termination. In addition, suppliers are further questioned around the organisations security and privacy policies to ensure that they meet to the required levels. In addition, the organisation will get them to sign NDA agreements, if this is not covered within the contractual terms. The contract in place is reinforced by adding Data Protection Addendums to ensure compliance with Privacy requirements (i.e. GDPR). All supplier details are documented in the supplier registers.
A.5.22	**Monitoring, review and change management of supplier services.** The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	True	Monitoring, reviewing, and managing changes in supplier services are integral components of our proactive and resilient information security strategy. The outcomes of the reviews, and details of the changes inform our risk assessments and treatment, help us stay vigilant, allow us to respond effectively to changes, and promote a secure and reliable supply chain environment. The control is needed to mitigate inherent risk to control objectives The control is needed according to best practices	Reviews of contracts are conducted with suppliers on their renewal. The review includes ensuring that the contract aligns to the requirements set out in the information security policy for suppliers. All supplier details are documented in the supplier asset register. All changes performed by suppliers where possible are communicated to us and where this has a direct impact on operational systems tie into our change management process. As part of the contract review and/or supplier audit process, changes from suppliers are reviewed and the security implications documented if relevant.
A.5.23	**Information security for use of cloud services.** Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.	True	Information security in the use of cloud services is essential for us to safeguard data, ensure compliance, manage risks, and maintain the trust of our customers and stakeholders. The control is needed to mitigate inherent risk to control objectives	Suppliers (including Cloud suppliers) have the following key sections covered within their contracts: the work and its scope; confidentiality; privacy; legal and regulatory requirements e.g. adherence to GDPR and or other applicable legislation; data security and protection; intellectual property rights; limitation of liability; payment terms and termination. In addition, suppliers are further questioned around the organisations security and privacy policies to ensure that they meet to the required levels. In addition, the organisation will get them to sign NDA agreements, if this is not covered within the contractual terms. The contract in place is reinforced by adding Data Protection Addendums to ensure compliance with Privacy requirements (i.e. GDPR). All supplier details are documented in the supplier registers.
A.5.24	**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.	True	Information security incident management planning helps us respond effectively to security incidents, reduce their impact, and continuously improve our information security practices. Our proactive and systematic approach safeguards information assets and maintains the integrity and resilience of our ISMS. The control is needed to mitigate inherent risk to control objectives The control is needed according to best practices	An incident management policy and procedure are in place to ensure a quick, effective and orderly response to address weaknesses, events and security incidents. The incident response team is responsible for responding to security incidents. The procedure includes details on how to respond to incidents and has been reviewed and approved by management.
A.5.25	**Assessment and decision on information security events.** The organization should assess information security events and decide if they are to be categorized as information security incidents	True	The incident management process defines that once a security weakness or event has been logged this will be assessed by the incident response team which will include relevant stakeholders. The response team also determines if the incident involves a breach of PI, if so, it will be reported to the relevant stakeholders. If the concern is determined not to be an incident, feedback as to why will be provided then the non-incident will be closed.	The incident management process defines that once a security weakness or event has been logged how this will be assessed by the incident response team which will include relevant stakeholders. The response team also determines if the incident involves a breach of PI, if so, it will be reported to the relevant stakeholders. An incident owner will be assigned. If the concern is determined not to be an incident, feedback as to why will be provided then the non-incident will be closed.

Clause	Clause Description	Is Applicable?	Justification	Control Description
			The control is needed according to best practices	
A.5.26	**Response to information security incidents.** Information security incidents should be responded to in accordance with the documented procedures.	True	Responding to information security incidents in accordance with our documented procedures is a fundamental aspect of effective incident management. It ensures consistency, efficiency, legal compliance, and the ability to learn and improve from each incident, ultimately contributing to a more resilient and secure information environment. The control is needed according to best practices	Response is included in the incident management procedure and aims to ensure that teams respond quickly and effectively. The incident manager will be responsible for leading a group of resources to resolve the incident including keeping the various stakeholders updated as to their progress. Additionally, as part of the resolution process, the team will complete the incident reporting requirements. Once the incident has been resolved a meeting will be scheduled and run to determine the learnings gained from the incident and what mitigating strategies have been put in place to ensure the incident doesn't happen again in the future.
A.5.27	**Learning from information security incidents.** Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	True	Learning from security incidents is crucial for us because it contributes to our continuous improvement culture, gives us enhanced resilience, and a more robust information security posture. Reviewing major incidents enables us to identify vulnerabilities, strengthening security controls, improve incident response, enhance threat intelligence, focus awareness, training and education, implement corrective actions, build a proactive security culture, meet compliance requirements, prevent recurrence, and maintain trust and reputation. Learning from security incidents is an integral part of our proactive and maturing ISMS. It allows us to continuously improve our security posture, mitigate risks, and respond effectively to threats. The control is needed according to best practices	Previous incidents and results are documented, shared and stored for access and therefore searchable, which enables any incident response teams to leverage data from past events. When incidents are closed, this generally requires there to be a resolution and preventive measure put into place. In the event of a recurring issue, the incident is escalated to help ensure the correct prioritisation for a successful deployment of a preventive measure is achieved.
A.5.28	**Collection of evidence.** The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	True	Procedures for the identification, collection, acquisition, and preservation of evidence are in place to support effective incident response, legal compliance, and maintain the integrity of information security investigations. Our formal evidence procedures ensure that security incidents are detected and give us data to prosecute the attackers. Our defined evidence procedures improve the investigation process by ensuring that evidence preservation is a focus. The control is related to a regulatory or certification requirement The control is needed to mitigate inherent risk to control objectives The control is needed according to best practices	The following is completed as part of the incident reporting requirements: • Collect evidence as soon as possible – either during or right after. • Store the evidence forensically securely in case of possible legal actions. • Determine the root cause and the related aspects of why it happened and who was involved. • Follow-up, if required, with the relevant regulators. • Ensure all involved response activities are properly logged for later analysis. • Communicate details to the leadership team for them to further communicate to various individuals or organisations on a need-to-know basis.
A.5.29	**Information security during disruption.** The organization should plan how to maintain information security at an appropriate level during disruption.	True	Planning how to maintain information security at an appropriate level during disruptions is crucial to ensure the resilience and continuity of business operations in the face of various challenges. Planning for information security during disruptions is a proactive and strategic approach that helps us navigate challenges, protect critical assets, and ensure the continuity of business operations. It is an integral component of our business resilience and risk management. The control is needed to mitigate inherent risk to control objectives	The organisation has created a Business Continuity Plan (BCP) which outlines the procedures that need to be followed in the event that a crisis or disaster occurs, these plans have specific security events and response plans documented. The BCP has been reviewed and approved by the management team and shall continue to be reviewed annually to ensure that any changes to the organisations structure or the technical infrastructure are reflected in the BCP. Security is considered as part of this process. All critical systems, services and data have high availability protection. Backups of all critical data is configured, and systems can be recovered from key points in time.
A.5.30	**ICT readiness for business continuity.** ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	True	Aligning ICT readiness with business continuity objectives is integral to our resilience. It ensures that our ICT systems are prepared to withstand disruptions, respond effectively to incidents, and contribute to overall business continuity goals. Regular testing and continuous improvement are essential elements of our process.	The organisation has created specific ICT scenarios within the Business Continuity Plan (BCP) which outlines the procedures that need to be followed in the event that a crisis or disaster occurs, and these plans have specific security events and response plans documented. The BCP has been reviewed and approved by the management team and shall continue

Clause	Clause Description	Is Applicable?	Justification	Control Description
			The control is needed to mitigate inherent risk to control objectives	to be reviewed annually to ensure that any changes to the organisations structure or the technical infrastructure are reflected in the BCP. Security is considered as part of these processes. All critical systems, services and data have high availability protection. Backups of all critical data is configured, and systems can be recovered from key points in time.
A.5.31	**Legal, statutory, regulatory and contractual requirements.** Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date.	True	Staying informed about and adhering to legal, statutory, regulatory, and contractual requirements is essential for ensuring the security of information, managing risks, maintaining compliance, and safeguarding our organisation's reputation. The control is related to a regulatory or certification requirement	The organisation has identified the applicable legislation, regulation and contractual requirements within our scoping exercise and risks understood and the applicable critical requirements were added to the ISMS and controls implemented. The organisation monitors the applicable legislation and reviews it as part of the normal course of business and is included as part of the management reviews.
A.5.32	**Intellectual property rights.** The organization should implement appropriate procedures to protect intellectual property rights.	True	Compliance to intellectual property rights is required to prevent fines and penalties related to illegal software usage. Implementing procedures to protect intellectual property rights is not only a legal necessity but is also a strategic imperative for our organisation to help us thrive in a competitive and innovation-driven business environment. It safeguards our investments, fosters innovation, and contributes to our long-term success. The control is related to a regulatory or certification requirement	Thomas International UK Ltd. IPR The organisation protects its Intellectual Property Rights (IPR) through the use of appropriate confidentiality provisions in its contractual arrangements with employees, contractors and third-party suppliers and partners. Staff and contractors will where appropriate mark information as owned by or the confidential information of the organisation and protect it including use of copyright statements in materials and assets produced by the organisation (e.g. customer proposals, presentation materials, code base).Registration of design, patent, trademarks, domain names to the appropriate authorities and following those relevant registration and management practices with records held both in the organisation and relevant third-party providers. Third-party IPR All staff will comply with the terms of any customer, supplier or other stakeholders' agreements and these will be documented. For generic third-party licences e.g. opensource and proprietary software that is free to use then the person downloading the software needs to be aware of its limitations and obligations and any software used on business devices or for business purposes must comply the Software Procurement Policy. Any purchased software needs to be registered in the asset register with licence numbers where appropriate. No third-party software shall be copied without approval or licences to do so.
A.5.33	**Protection of records.** Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	True	Protecting records from loss, destruction, falsification, unauthorised access, and unauthorised release is integral to legal compliance, operational continuity, maintaining trust, and safeguarding sensitive information. It is a fundamental aspect of effective information governance and risk management within our organisation. The control is related to a regulatory or certification requirement	Organization records are kept protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements. (i.e. GDPR) All information of value is stored securely in official organisation storage locations backed up with the various cloud providers or using local requirements in accordance with our controls. Retention periods result in specific records kept in line with the relevant retention policies. Employees are trained annually about sharing data externally, both how to do it safely and what is and what is not allowed to be shared based on the labels.
A.5.34	**Privacy and protection of PII.** The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	True	Compliance to privacy controls is a critical focus area as there are international laws governing how Personally identifiable information (PII) is managed. Not complying with these laws could result in fines and other penalties. Identifying and meeting requirements related to the preservation of privacy and protection of PII is not only a legal obligation but also a strategic and ethical imperative. It helps build trust, mitigate risks, and position our organisation as a responsible steward of sensitive personal information. The control is related to a regulatory or certification requirement	The rules related to Privacy and Protecting PI are in the data privacy policy and the implementation of specific processes and controls documented in supporting processes. All staff handling personal information are aware of the data protection and privacy principles through training and communication and ensure personal data should be dealt with in accordance with this. All staff undergo annual training on data protection to ensure that they are aware of any changes that have been brought in and to ensure that data protection is always at the front of mind when handling data.

Clause	Clause Description	Is Applicable?	Justification	Control Description
A.5.35	**Independent review of information security.** The organization's 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.	True	Reviewing our organisation's approach to managing information security is essential for maintaining the effectiveness of security measures, staying compliant with regulations, and adapting to the evolving threat landscape. It is a proactive and strategic approach to safeguarding information assets and maintaining our overall security posture. The control is required due to a contractual obligation	External parties provide independent reviews of our information security. Reviews are performed on an annual basis by an authorised ISO27001 auditor to ensure that ISO accreditation is up to standard and that the necessary procedures are in place and plan and that the organisation conduct internal audits to support the certification. Additionally, the organisation annually completes a penetration test performed by an independent 3rd party. Other reviews will be considered depending on risk and specific requirements. Any significant changes to working procedures are added to the audit in order to stay compliant.
A.5.36	**Compliance with policies, rules and standards for information security.** Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	True	Regular reviews of compliance with information security policies, topic-specific policies, rules, and standards are essential for maintaining the effectiveness of our security measures, staying current with regulatory requirements, adapting to business changes, and continuously improving our organisation's overall security posture. Internal compliance checks are a vital aspect of our organisations risk profile and controls are implemented to ensure that the controls, documentation and overall ISMS status are reviewed regularly by managers within their area of responsibility. The control is needed to mitigate inherent risk to control objectives The control is needed according to best practices	Issues related to Security policy compliance will be picked up during security incidents or during discussions related to the ISMS. In addition, during the management review with the ISMS stakeholder's compliance with the security policies will be discussed and any actions should be included going forward will be agreed.
A.5.37	**Documented operating procedures.** Operating procedures for information processing facilities should be documented and made available to personnel who need them.	True	Documenting operating procedures for information processing facilities and making them available to personnel is fundamental for promoting consistency, efficiency, compliance, risk management, and overall effectiveness in the operation of information systems within our organisation. It supports our commitment to best practices, quality, and the ongoing improvement of our information processing capabilities. The control is needed according to best practices	The organisation makes use of cloud-based applications and systems, so many traditional operations such as computer start-up and shutdown, backup etc. are not relevant or are the responsibility of the service provider. Our assurance relating to operational procedures within the above is managed through controls relating to Supplier relationships. For other processes relevant documents for operating procedures will be made readily available to employees along with a number of processes related to Information Security including: • Change management • Capacity management • Controls against malware • Information backup • Logging & monitoring • Technical vulnerability management • Information transfer policies and procedures The necessary documents are stored within SharePoint and Hicomply and are made available to employees.
A.6	**People Controls.**			
A.6.1	**Screening.** Background verification checks on all candidates to become personnel should be carried out prior to joining the organization 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.	True	Conducting background verification checks on candidates before joining our organisation is a comprehensive risk management strategy that protects us, our employees, and our stakeholders. It helps ensure legal compliance, maintain a safe and trusted work environment, and prevent potential issues that could adversely impact our organisation's reputation and success. The control is related to a regulatory or certification requirement	The checks the organisation carries out internally include Right to Work verification, identity confirmation (e.g. reviewing passports), collecting any role-specific qualifications or certificates from new joiners and references. All records of these checks are maintained on Thom.
A.6.2	**Terms and conditions of employment.** The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.	True	Including information security responsibilities in employment contractual agreements is our proactive approach to establishing a strong security culture, ensuring legal compliance, and mitigating the risk of security incidents. It helps create a shared understanding of the	All employees sign a standard set of terms and conditions (included in employment contracts) prior to joining, which includes specific clauses on data protection and information security responsibilities. Contractor agreements are reviewed to ensure inclusion of data protection and security

Clause	Clause Description	Is Applicable?	Justification	Control Description
			critical role that our employees play in safeguarding our organisation's information assets. The control is needed to mitigate inherent risk to control objectives The control is required due to a contractual obligation	terms. The organisation does not engage contractors who fail to meet these requirements.
A.6.3	**Information security awareness, education and training.** Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	True	Investing in information security awareness, education, and training for our team is our proactive strategy that enhances our organisation's overall security posture, reduces risks, and fosters a culture of security consciousness and responsibility. The control is required due to a contractual obligation The control is needed to mitigate inherent risk to control objectives	There is an ongoing security awareness programme in place which is continuously monitored and measured. The information security awareness and training of personnel aims to mitigate information security risks by making staff aware of possible attacks and apply their knowledge in their day- to-day roles. Training is updated annually and when there are any major changes.
A.6.4	**Disciplinary process.** A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	True	Formalising and communicating our disciplinary process for information security policy violations is our strategic approach that ensures consistency, deterrence, legal compliance, and overall effectiveness in maintaining a secure information environment within our organisation. The control is related to a regulatory or certification requirement The control is needed according to best practices	The disciplinary process is documented within HR procedures and communicated to all employees. It includes provisions for handling violations of information security policies. Employees acknowledge these procedures upon signing their employment contracts. HR manages the process, with security incidents integrated into disciplinary actions.
A.6.5	**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.	True	Defining, enforcing, and communicating ongoing information security responsibilities after termination or change of employment is essential for protecting sensitive information, preventing insider threats, ensuring legal compliance, and upholding our organisation's overall security posture. The control is needed to mitigate inherent risk to control objectives	Upon termination of employment, access to all systems is stopped, and organisation assets such as laptops, phones and building access are returned. The employment contract includes clauses on confidentiality and the handling of employer property during and after employment, which all employees agree to prior to starting. The leaver is sent an offboarding letter which outlines the leaver process and remains them of the confidentiality restrictions.
A.6.6	**Confidentiality or non-disclosure agreements.** Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	True	Identifying, documenting, regularly reviewing, and having the right people sign confidentiality or non-disclosure agreements are essential practices for protecting our organisation's sensitive information, maintaining trust, and ensuring legal compliance. These agreements are a fundamental component of our comprehensive information security strategy. The control is required due to a contractual obligation	Confidentiality provisions are included in legal terms that clients and suppliers sign when they sign-up. Clients who wish to share data prior to signing up need to sign a non-disclosure agreement (NDA). Training is provided to all staff outlining the process and requirement of having NDAs or confidentiality agreements in place with both clients and suppliers.
A.6.7	**Remote working.** Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	True	Security measures for remote work are essential to address the challenges and risks associated with accessing, processing, and storing information outside our organisation's premises. These measures are integral to maintaining a secure and resilient information environment in the context of evolving work practices. The control is needed according to best practices The control is needed to mitigate inherent risk to control objectives	The organisation has defined the rules around the use of working remotely within the Acceptable Use of Technology and Workspace, Device and Hybrid Working Policies and the organization has been designed with remote working as a core part of the way work gets done and combines controls to robustly deal with the risks associated with remote working. (i.e. Malware. encryption, access control, security awareness).
A.6.8	**Information security event reporting.** The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	True	Providing a mechanism for employees to report observed or suspected information security events in a timely manner is our proactive strategy for early detection, rapid response, and overall resilience in the face of evolving cybersecurity threats. It is an integral component of our comprehensive information security program. The control is needed according to best practices	An incident management policy and procedure is in place to ensure that a quick, effective and orderly response to address weaknesses, events and security incidents. The incident response team is responsible for responding to security incidents. Staff are informed and trained on how to identify and report these incidents. The procedure includes details on how to respond to incidents and the roles related to incident management. The policy and procedure has been reviewed and approved by management and is reviewed on an annual basis to ensure that it remains up to date.
A.7	**Physical controls.**			

Clause	Clause Description	Is Applicable?	Justification	Control Description
	...			
A.7.1	**Physical security perimeters.** Security perimeters should be defined and used to protect areas that contain information and other associated assets.	True	Defining and protecting our physical security perimeters is critical to protect our information and associated assets by preventing unauthorised access, deterring threats, and facilitating a more controlled and secure office environment. The control is needed to mitigate inherent risk to control objectives	Any office in scope has a physical perimeter via own access doors. Which includes either key and or code entry and is communicated to new joiners as part of the onboarding process. Keys and fobs are recorded on the central asset register.
A.7.2	**Physical entry.** Secure areas should be protected by appropriate entry controls and access points.	True	Protecting our secure areas with appropriate entry controls and access points helps safeguard information, assets, and personnel, contributing to the overall resilience and integrity of our operations. The control is needed to mitigate inherent risk to control objectives	Any office in scope has its own access control in place tailored to the building, which include key and or code entry which is communicated to new joiners as part of the onboarding process. Keys and fobs are recorded on the central asset register.
A.7.3	**Securing offices, rooms and facilities.** Physical security for offices, rooms and facilities should be designed and implemented.	True	Designing and implementing physical security for offices, rooms, and facilities helps mitigate potential threats and vulnerabilities, contributing to the overall resilience and security of our organisation. The control is needed to mitigate inherent risk to control objectives	Any office in scope has its own access control in place tailored to the building, which include key and or code entry, and is recorded on the asset register which is reviewed as part of onboarding and offboarding processes. Any areas with restricted access are secured via a key which is held centrally by the Operations Team. All visitors are required to sign-in via QR code and are provided with a "Guest" lanyard to wear which documents H&S information, alongside guest Wi-Fi instructions.
A.7.4	**Physical security monitoring.** Premises should be continuously monitored for unauthorized physical access.	True	Continuous monitoring of our premises for unauthorised physical access is vital to our security strategy, helping us protect our assets, ensure compliance, and respond effectively to potential threats. The control is needed to mitigate inherent risk to control objectives	Any in scope office that is storing information or equipment deemed critical to the business will be monitored through the use of a Closed-Circuit-Television (CCTV), the CCTV will be installed to cover all exit and entry points.
A.7.5	**Protecting against physical and environmental threats.** Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.	True	The design and implementation of protection measures against physical and environmental threats are essential for ensuring safety, preserving assets, maintaining business continuity, and meeting regulatory requirements. It is a critical aspect of our responsible infrastructure management and contributes to the overall resilience of our systems in the face of various challenges. The control is related to a regulatory or certification requirement	Any in scope office has regulatory fire systems in place, initially installed by the respective landlords. The landlord in each premises has overall responsibility for the maintenance and upkeep of the building fire systems, with Thomas having responsibility for fire protection and prevention within its demise (including upkeep of fire extinguishers, emergency list testing and risk assessment records). Thomas also ensures training for all employees on H&S, applicable for both office and remote workers. The Business Continuity Policy documents the process for additional physical and environmental threats.
A.7.6	**Working in secure areas.** Security measures for working in secure areas should be designed and implemented.	True	Security measures for working in secure areas are designed and implemented with the aim of safeguarding our people, information, assets, and the overall integrity of the secure environment. The measures are crucial for safeguarding sensitive information, preventing unauthorised access, ensuring employee and visitor safety, and maintaining the overall integrity of our critical environments. The control is needed to mitigate inherent risk to control objectives The control is needed according to best practices	Any office in scope has its own access control in place tailored to the building, which include key and or code entry which is communicated to new joiners as part of the onboarding process. Keys and fobs are recorded on the central asset register. The staff are trained to report anyone who isn't a staff member and who is inside the office space without authorisation.
A.7.7	**Clear desk and clear screen.** Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	True	Defining and appropriately enforcing clear desk rules for papers and removable storage media, as well as clear screen rules for information processing facilities, help protect sensitive information, prevent data breaches, and promote a culture of security within our organisation. The control is needed to mitigate inherent risk to control objectives The control is needed according to best practices	Staff are trained to clear their desks of any confidential data when they are not at their desks, with printing discouraged. This is documented in our Acceptable Use of Technology and Workspace Policy. Training takes place during onboarding, then annually thereafter. This is monitored, staff are reminded of the policy if documents are found left on a desk, with further action taken for repeat offenders. Additionally, a policy is in place that automatically locks a user's machine if there is no activity after 15 minutes.
A.7.8	**Equipment siting and protection.** Equipment should be sited securely and protected.	True	Securing and protecting our equipment safeguards against physical damage, theft, environmental factors, and cybersecurity threats. The control is needed to mitigate inherent risk to control objectives	Equipment Is protected and sited away from any threats or unauthorised access and usage and has access controls in place protecting it. In addition, equipment is stored securely based on its confidentiality.

Clause	Clause Description	Is Applicable?	Justification	Control Description
			The control is required due to a contractual obligation	
A.7.9	**Security of assets off-premises.** Off-site assets should be protected.	True	Protecting our off-site assets safeguards our data, ensures business continuity, complies with regulations, and mitigates risks that could impact operations, reputation, and financial stability. The control is needed to mitigate inherent risk to control objectives The control is required due to a contractual obligation	Equipment is secured to the premises where possible. If the equipment cannot be secured, staff will report any removal of assets without authorization. Authorised equipment can be removed if its reason is documented and the equipment is protected against unauthorised access through access controls and encryption.
A.7.10	**Storage media.** Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	True	Managing storage media through its life cycle in alignment with our classification scheme and handling requirements is integral to maintaining our data security, ensuring regulatory compliance, minimising environmental impact, and overall effective risk management. Our holistic approach considers the entire life span of storage media from acquisition to disposal. The control is related to a regulatory or certification requirement	The rules around the usage of storage media are defined in the Information Classification, Protection of Electronic Data, Device and Acceptable Use of Technology and Workspace policies. Laptops are managed by additional controls such as Encryption and Anti-virus, patching is automated, with users made aware of their role to ensure that updates take place and devices function well. The organisation restricts the use of removable media unless requested for a specific business-related purpose and approved by management. All applicable devices' hard drives are encrypted to ensure that any data kept on them is secure. Devices that are lost or stolen are remotely wiped where possible to ensure that the data contained on them is removed. Devices that are exchanged internally are wiped of all data before the new user starts using the device. Devices that come to the end of their useful life are wiped to ensure that the data is completely irrecoverable and then sent for full data cleansing and recycling.
A.7.11	**Supporting utilities.** Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	True	Protecting information processing facilities from power failures and disruptions caused by failures in supporting utilities ensured operational resilience, data integrity, and overall business continuity. It involves implementing a combination of backup power systems, redundancy, and contingency planning to mitigate the impact of unexpected power-related events. The control is needed to mitigate inherent risk to control objectives	The data centre has been designed to protect against threats by ensuring that all critical/necessary business equipment have secured power and are supported by a UPS or any form of backup power.
A.7.12	**Cabling security.** Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	True	Protecting cables carrying power, data, or supporting information services is essential for maintaining the security, integrity, and reliability of our critical systems and infrastructure. It involves implementing physical safeguards, encryption measures, and best practices to minimise the risks associated with interception, interference, or damage. The control is needed according to best practices	Safe routing and channelling of power and network cables are in place in order to reduce the risks of interception or tampering.
A.7.13	**Equipment maintenance.** Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	True	Maintaining equipment correctly ensures the reliable operation of critical systems, protects against security threats, and supports compliance with regulatory requirements, ultimately safeguarding the availability, integrity, and confidentiality of information. The control is related to a regulatory or certification requirement	Equipment maintenance is performed annually or dependent on the devices condition and issues and there is a list if equipment and maintained dates stored by the relevant team.
A.7.14	**Secure disposal or re-use of equipment.** Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	True	Disposal of equipment containing storage media is critical to ensure that sensitive data and licensed software is removed so that they cannot be accessed, stolen or used by unauthorised parties. The control is related to a regulatory or certification requirement	Devices' hard drives are encrypted to ensure that any data kept on them is secure. Devices that are exchanged are securely wiped of all data to ensure that the next user has a clean drive and new profile created. Devices that come to

Clause	Clause Description	Is Applicable?	Justification	Control Description
			The control is needed to mitigate inherent risk to control objectives	the end of their useful life are securely wiped to ensure that the data is completely irrecoverable.
A.8	**Technological controls.**			
A.8.1	**User endpoint devices.** Information stored on, processed by or accessible via user endpoint devices should be protected.	True	Protecting information on user endpoint devices is integral to our information security strategy. It involves implementing a combination of technical controls, security policies, and user awareness training to mitigate risks and safeguard sensitive data throughout its lifecycle. The control is needed according to best practices	User devices are managed centrally through a combination of controls configured via Microsoft Intune and Defender. Laptops are managed by controls such as Encryption, Anti-virus, patching which users are made aware of their role to ensure that they function well. The devices are monitored through dashboards where available and are reported on regularly. Devices that are lost or stolen are remotely wiped where possible to ensure that the data contained on them is removed.
A.8.2	**Privileged access rights.** The allocation and use of privileged access rights should be restricted and managed.	True	A defined access control policy with supporting processes for privileged access is vital to set a direction and principles for access control. Privileged access is a major risk area because of what these accounts are able to access and the services they are able to perform. Malicious parties will target these accounts and use them to access information and perform Malicious attacks. The control is needed to mitigate inherent risk to control objectives	The Access Control policy defines that there are additional controls for privileged access accounts. The privileged access accounts must be authorised and monitored more frequently than regular access users.
A.8.3	**Information access restriction.** Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	True	Access control (least privileged access methodology) protects data, ensures compliance, and mitigates risks associated with unauthorised access by preventing unauthorised users from accessing information and application systems. The control is needed to mitigate inherent risk to control objectives	Information access restriction is implemented in accordance with the Access Control Policy and Authorised Access to Information Procedure, this defines the principles and process related to how access information and application systems work. There are defined controls in place regarding how access is managed from the network, operating system and application level which at every level include controls designed to restrict access to Information and applications. Wherever possible applications are designed or selected such that menus do not show options for which a user is not authorised.
A.8.4	**Access to source code.** Read and write access to source code, development tools and software libraries should be appropriately managed.	True	Appropriate management of development tools and software libraries is essential for maintaining our stable, secure, and efficient development environment. It supports the entire software development lifecycle, from initial coding to testing, deployment, and maintenance, contributing to the long-term success of software projects. Program source code one of the organizations most valuable assets and needs to be protected from unauthorized access to ensure its confidentiality, integrity and availability. The control is needed to mitigate inherent risk to control objectives	The organisation manages access to source code, development tools and software libraries through role-based access groups, enforced branch protection rules and mandatory peer review. Source code is treated as a core business asset and is protected to ensure confidentiality, integrity and availability throughout the software development lifecycle.
A.8.5	**Secure authentication.** Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	True	Preventative controls maintain risk by implementing technology and establishing topic-specific secure authentication procedures that ensure human and non-human users and identities undergo a robust and secure authentication procedure when attempting to access ICT resources. The control is needed to mitigate inherent risk to control objectives	The allocation of secret authentication information, such as passwords, is required to be governed through a formal process. Users agree to follow the organizations practices when using secret authentication information. When first given access, the users are given a temporary password which they are required to change on first login and password controls are enforced through automated solutions. When the need to change a password occurs this is done either face to face or in a manner that ensures the person is able to confirm their identity.
A.8.6	**Capacity management.** The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	True	Capacity Management supports the network security controls by designing capacity requirements and monitoring the network devices (including servers) for capacity issues which could affect the availability of the devices. This includes security related threats and general operational issues.	The organisation actively monitors system resource usage across servers, APIs, databases and related infrastructure to ensure sufficient capacity is maintained for reliable SaaS service delivery. Alerting thresholds support proactive scaling and remediation when usage approaches defined limits.

Clause	Clause Description	Is Applicable?	Justification	Control Description
			The control is needed to mitigate inherent risk to control objectives	
A.8.7	**Protection against malware.** Protection against malware should be implemented and supported by appropriate user awareness.	True	Malware Controls are a vital defence against malicious attacks which could come from outside or inside the organization's network. The malware controls the organisation has in place reduce the impacts of Malicious attacks and ensures that the information security team has visibility. The control is needed to mitigate inherent risk to control objectives The control is required due to a contractual obligation	A malware protection procedure is in place to combat the risks related to malware. The procedure directs and defines protection for infrastructure from common exploits and vulnerabilities. Anti-virus and Anti-malware software are implemented on all devices and details of software, and its current status are included on a dashboard where the AV status is monitored.
A.8.8	**Management of technical vulnerabilities.** Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	True	Our vulnerability and penetration testing policy ensures the organisation are regularly conducting testing for vulnerabilities across our network and aims to help us to identify and resolve vulnerabilities across the organization's infrastructure and reduces the risks related to Malicious attacks. The control is related to a regulatory or certification requirement The control is needed to mitigate inherent risk to control objectives	The organisation identifies, assesses and remediates vulnerabilities across infrastructure and application code using scheduled scanning, penetration testing and dependency analysis. Remediation timelines are assigned based on severity to ensure vulnerabilities are resolved efficiently and proportionately.
A.8.9	**Configuration management.** Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	True	The organisation has established documents that govern how the organisation implements, monitors and reviews the use of configurations across our network. The control is needed to mitigate inherent risk to control objectives	The organisation maintains documented configuration standards for systems and services, aligned to vendor guidance and industry frameworks including ISO27001 and NIST. Configuration states are monitored for drift, and changes follow controlled and auditable processes. 1. Server configuration hardening based on vendor and ISO27001 recommendations. 2. Application configurations managed as code and stored in version control. 3. Monitoring and alerting to detect configuration drift from approved baselines.
A.8.10	**Information deletion.** Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	True	Our data retention policy ensures the organisation retains information for the appropriate amount of time, considering any prevailing laws and regulatory guidelines. Alongside this our IT Asset Management Policy defines how assets should be managed and destructed. The control is related to a regulatory or certification requirement	The organisation has developed a policy and related procedure defining the retention periods for data and agreed this with management. This includes specific time periods and details on what to do with the data. Data should be archived for as long as required and then deleted when no longer needed.
A.8.11	**Data masking.** Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	True	Our cryptography controls policy defines where the organisation needs to apply data masking techniques and the controls the organisation needs to put in place to help the business remain compliant with what's asked of it by legal authorities and regulatory agencies. The control is needed to mitigate inherent risk to control objectives	The organisation applies data masking where it is necessary and applicable to restrict access to personal or sensitive information in line with our cryptography and access control policies. Masking ensures data cannot be reconstructed and is used especially in non-production environments.
A.8.12	**Data leakage prevention.** Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	True	Our Data Loss Prevention Procedures help to control and reduce the risk of data leakage, with technical controls implemented to prevent the disclosure and/or extraction of information, either by internal and/or external personnel, or logical systems. The control is needed to mitigate inherent risk to control objectives	DLP is managed by aligning information to the classification and handling rules and implementing controls aligned to these rules. The use of critical information such as PI is being monitored and where possible its transfer is monitored and/or blocked.
A.8.13	**Information backup.** Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	True	Our operating procedures defined the controls the organisation has in place for critical systems and the backup and recovery of information in these systems. Having these controls in place protects us against risks related to the loss or corruption of information.	Backup principles and rules are defined in the BCP and ISMS Operating Procedures and are formally managed across various areas to ensure that Backups for all identified systems are backed up and stored securely. To ensure recovery is possible a comprehensive recovery plan has been created. Database backups are periodically tested by restoring to a test

Clause	Clause Description	Is Applicable?	Justification	Control Description
			The control is needed to mitigate inherent risk to control objectives	environment and running smoke tests against that environment to ensure there are no operational issues, and all storage and database backups are encrypted at rest.
A.8.14	**Redundancy of information processing facilities.** Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	True	Our BCP focuses on our information security continuity risks and ensures that the business will react effectively and respond to disasters or major incidents. The control is needed to mitigate inherent risk to control objectives	Availability is defined in the BCP, and all components are architected with consideration of redundancy. Primary datacentres and failover secondary datacentres have been utilized. Implementation of automated or manual failovers, depending on suitability. Backups are also performed as per A.8.13 When a component uses a manual failover, documentation and runbooks are stored and available to developers and operations. Manual failovers are regularly tested to ensure they are working as expected and are secure.
A.8.15	**Logging.** Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	True	Logging and monitoring controls gives us the ability to identify and respond to malicious attacks and other security incidents. Our logging and monitoring policy guides us on what the organisation needs to maintain and monitor. The control is needed to mitigate inherent risk to control objectives	Logging and monitoring controls are applied to each area, our logging and monitoring policy defines how logs are captured, stored and regularly reviewed. Logs are securely stored for a defined period and then archived off for storage.
A.8.16	**Monitoring activities.** Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	True	Logging and monitoring controls gives us the ability to identify and respond to malicious attacks and other security incidents. Our logging and monitoring policy guides us on what the organisation needs to maintain and monitor. The control is needed to mitigate inherent risk to control objectives	Logging and monitoring controls are applied to each area, the Logging and Monitoring Policy defines how logs are captured, stored and regularly reviewed. Logs are securely stored for a defined period and then archived off for storage. Logs are stored across various areas: 1. Security solutions (i.e. Anti-virus, EDR) 2. Applications – (i.e. Web applications, List of internal applications) 3. Operating systems (MS Entra) 4. Network devices (i.e. Firewalls) 5. Cloud Providers (Microsoft 365, Azure) 6. Other specific areas deemed to be useful. Access to the logs is restricted through using limiting to access groups of authorised users and monitoring the access to the logs.
A.8.17	**Clock synchronization.** The clocks of information processing systems used by the organization should be synchronized to approved time sources.	True	Logging and monitoring controls give the organization the ability to identify and respond to malicious attacks and other security incidents. Without a process defining how logs are recorded and kept with rules related to clock synchronisation it is not possible to have an effective incident detection and response process. The control is needed according to best practices	All systems synchronize to approved network time sources (Azure Stratum 1 time servers) to ensure consistent timestamping of logs and events. Time accuracy enables reliable event correlation and incident investigation.
A.8.18	**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.	True	Some utility programs allow users to override system and application controls and can be used to access information or perform system tasks so need to be protected. The control is needed to mitigate inherent risk to control objectives	Privileged utility systems are strictly prohibited unless an exception is granted authorisation by the relevant stakeholders. When these applications are used then they are tightly controlled through limiting access, using strong password controls (i.e. multi-factor authentication (MFA)) and ensuring that the applications use is monitored.
A.8.19	**Installation of software on operational systems.** Procedures and measures should be implemented to securely manage software installation on operational systems.	True	The organisation has procedures to control the installation of software on operational systems, preventing unauthorised software being installed on operational systems and the related risks of malware and unsupported software leading to operational issues. The control is needed to mitigate inherent risk to control objectives	Administrator access is highly restricted and is only given if requested and approved by management. Changes to operational systems, such as, Software installations, are controlled via our internal ticketing system with approvals required dependant on the request. Changes impacting our platform are made to the development environment first, and only on success are changes made to other environments.
A.8.20	**Networks security.** Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	True	Our Network Security Policy gives guidance on the controls the organisation needs to have in place to guard against unauthorised access to networks, mitigating risks of information security. The control is needed to mitigate inherent risk to control objectives	A network security policy was created that defines how networks will be managed and setup. The network design is documented and designed to protect the perimeter and information assets within. Networks are encrypted and access controls and monitoring in place to protect from any unauthorized access.

Clause	Clause Description	Is Applicable?	Justification	Control Description
A.8.21	**Security of network services.** Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	True	Our Network Security Policy gives guidance on the controls the organisation needs to have in place to guard against unauthorised access to networks, mitigating risks of information security. The control is needed to mitigate inherent risk to control objectives	A network security policy was created that defines how networks will be managed and setup. The network design is documented and designed to protect the perimeter and information assets within. Networks are encrypted and access controls and monitoring in place to protect from any unauthorized access.
A.8.22	**Segregation of networks.** Groups of information services, users and information systems should be segregated in the organization's networks.	True	Our Network Security Policy defines how networks should be segregated to guard against unauthorized access to networks, mitigating risks of information security. The control is needed to mitigate inherent risk to control objectives	A network security policy was created that defines how networks will be managed and setup. The network design is documented and designed to protect the perimeter and information assets within through appropriate segregation to prevent users from accessing unauthorized networks. Networks are encrypted and access controls and monitoring in place to protect from any unauthorized access.
A.8.23	**Web filtering.** Access to external websites should be managed to reduce exposure to malicious content.	True	Filtering the websites accessible enables us to eliminate security risks such as malware infection that may arise as a result of access to external websites with malicious content. The control is needed to mitigate inherent risk to control objectives	The organisation makes use of blocking at the network level and/or through Microsoft Defender, this blocks users from accessing sites that are not authorised. In addition, the site lists are updated and security incidents related to user access issues are reported on.
A.8.24	**Use of cryptography.** Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	True	The cryptographic (encryption) controls are an integral part of the ISMS and are required to manage the risks of unauthorized access to information. Encryption is an additional layer of security which allows for information to be encrypted both when transmitted or stored and is required for legal/regulatory requirements. The control is related to a regulatory or certification requirement	Cryptography usage is defined in the Cryptographic Controls Policy. The purpose of this policy is to protect the confidentiality, integrity and availability of the organization 's Information by applying appropriate levels of Cryptographic control. Encryption is used widely both for storage and transmission and the rules contained in the documentation must be applied. The policy is designed to ensure that cryptographic controls (i.e. the use of encryption technologies) is applied in a consistent, adequate and proportionate manner and that key material is formally managed. All critical or confidential data transferred outside of the organization must be encrypted where possible, as described in the Information Classification Policy.
A.8.25	**Secure development life cycle.** Rules for the secure development of software and systems should be established and applied.	True	Security controls being implemented for the development function ensures that systems are developed and maintained with security controls designed and implemented throughout the life cycle. These controls aim to ensure that risks related to security weaknesses are managed to protect systems. The control is needed to mitigate inherent risk to control objectives	Our engineering teams follow a defined secure development lifecycle that incorporates security requirements, threat considerations, code review and documented change control from design through to release and maintenance.
A.8.26	**Application security requirements.** Information security requirements should be identified, specified and approved when developing or acquiring applications.	True	This enables us to protect information assets stored on or processed through applications by identifying and applying appropriate information security requirements. The control is needed to mitigate inherent risk to control objectives	Security requirements for new and existing applications are defined and reviewed as part of the development and change process. Requirements align to OWASP guidance and relevant regulatory considerations
A.8.27	**Secure system architecture and engineering principles.** Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.	True	Security controls being implemented for the development function ensures that systems are developed and maintained with security controls designed and implemented throughout the life cycle. Secure engineering principles govern these processes by ensuring that security is integrated into the overall process. The control is needed to mitigate inherent risk to control objectives	The organisation applies secure architecture and engineering principles to ensure systems are designed, implemented and maintained in a secure and reliable manner. Changes to platforms or applications undergo review, testing and post-release validation.
A.8.28	**Secure coding.** Secure coding principles should be applied to software development.	True	The organisation prevents security risks and vulnerabilities that may arise as a result of poor software coding practices by designing, implementing, and reviewing appropriate secure software coding principles. The control is needed to mitigate inherent risk to control objectives	Developers follow secure coding standards and implement defensive programming techniques to prevent common coding vulnerabilities. Secure coding is reinforced through tooling, peer review and continuous improvement.

Clause	Clause Description	Is Applicable?	Justification	Control Description
A.8.29	**Security testing in development and acceptance.** Security testing processes should be defined and implemented in the development life cycle	True	Security controls being implemented for the development function ensures that systems are developed and maintained with security controls designed and implemented throughout the life cycle. These controls aim to ensure that risks related to security weaknesses are managed to protect systems. The control is needed to mitigate inherent risk to control objectives	Security testing is embedded within the development lifecycle and includes static analysis, dependency scanning and dynamic application security testing. Identified vulnerabilities are prioritised and remediated based on severity.
A.8.30	**Outsourced development.** The organization should direct, monitor and review the activities related to outsourced system development.	True	This enables us to ensure that the established information security requirements are adhered to when the system and software development is outsourced to external suppliers. The control is needed to mitigate inherent risk to control objectives	Where development is outsourced, third parties are required to follow our secure development standards, protect confidential information and allow monitoring of deliverables and security performance.
A.8.31	**Separation of development, test and production environments.** Development, testing and production environments should be separated and secured.	True	Separating the development, testing and operational environments is a fundamental ISMS control to ensure that developers cannot make unauthorized changes between environments which could result in security and operational issues to the environment. The control is needed to mitigate inherent risk to control objectives	Development, testing and production environments are logically separated, and access is restricted by role to prevent unauthorized changes and reduce operational risk. Temporary elevated access is controlled and logged.
A.8.32	**Change management.** Changes to information processing facilities and information systems should be subject to change management procedures.	True	Change Management is a fundamental ISMS control and ensures that there is a framework to manage how changes are documented, analysed and managed across their life cycle to positively enhance information security requirements. Unmanaged changes can result in major operational and information security risks. The control is needed to mitigate inherent risk to control objectives The control is needed according to best practices	All changes will go through a formal change process approved. The changes will be logged and stored. Software changes are tested in a test environment or offline version prior to implementation. Only authorized users are able to make any changes to software.
A.8.33	**Test information.** Test information should be appropriately selected, protected and managed.	True	Ensuring that Test data is not a copy of Production data is a vital control as it prevents live data being used in less secure environments reducing risks related to unauthorized access and breaches. The control is needed to mitigate inherent risk to control objectives	Test environments use sanitised and anonymised data. The use of live or identifiable production data in test environments is prohibited, and data handling follows approved policies and controls.
A.8.34	**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.	True	This control is required to manage the risks related to how audits impact on operations and how information provided to auditors is securely managed. The control is needed to mitigate inherent risk to control objectives	Data shared with auditors will be provided via a secure mechanism, specifically the Hicomply platform and if required Thomas' SharePoint. This process is in place to ensure that sensitive data is not sent externally via email or other means. This is confirmed during the audit and confirmed to them. The team is made aware of this during their onboarding process.