Statement of Applicability ISO 27001:2022

Document reference number: ISM-NOT-008
Organisation: Jisc
Issue: 11
Last updated: 05/03/2025
Approval status: Approved

Contents

5. Organisational controls

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
5.1	Organisational controls	Policies for information security	Information security policy and topic-specific policies shall 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.	x	x		Yes	Yes	To ensure that a set of policies for information security have been defined, approved by management, published, and communicated to employees and relevant external parties.
5.2	Organisational controls	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organisation needs.	x	x		Yes	Yes	To provide clarity on specific Information Security responsibilities.
5.3	Organisational controls	Segregation Of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	x	x		Yes	Yes	Conflicting duties and areas of responsibility must be segregated in order to reduce the opportunities for unauthorised or unintentional modification or misuse of any of the organisation's assets.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
5.4	Organisational controls	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies, and procedures of the organization.		x		Yes	Yes	This control ensures that the responsibilities placed upon managers includes requirements to; Ensure that those they are responsible for understand the information security threats, vulnerabilities and controls relevant to their job roles.
5.5	Organisational controls	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	x	x	x	Yes	Yes	To ensure that legal, contractual and governance requirements are being met.
5.6	Organisational controls	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.		x		Yes	Yes	To ensure that changes in the Information Security landscape and industry best practice are considered when planning changes to the ISMS.
5.7	Organisational controls	Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	x	x		Yes	Yes	This control is used as a preventive, detective and corrective control that ensure that Jisc has awareness of the organisations threat environment so that the appropriate mitigation actions can be taken.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
5.8	Organisational controls	Information security in project management	Information security shall be integrated into project management.	x	x		Yes	Yes	To ensure that the security by design principle is applied and that security is hard baked into all projects.
5.9	Organisational controls	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed, and maintained.		x		Yes	Yes	To ensure that assets associated with information and information processing facilities are identified and an inventory of these assets is established and maintained.
5.10	Organisational controls	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented, and implemented.		x		Yes	Yes	To ensure that assets associated with information and information processing facilities are identified and an inventory of these assets is established and maintained.
5.11	Organisational controls	Return of assets	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract, or agreement.		x		Yes	Yes	To ensure that all employees and external party users return all of the organizational assets in their possession upon termination of their employment, contract, or agreement.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
5.12	Organisational controls	Classification of information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability, and relevant interested party requirements.		x		Yes	Yes	To ensure that all Information is classified in terms of legal requirements, value, criticality and sensitivity to any unauthorised disclosure or modification.
5.13	Organisational controls	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.		x		Yes	Yes	To ensure that an appropriate set of procedures for information labelling have been developed and implemented in accordance with the information classification scheme adopted by the organisation.
5.14	Organisational controls	Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	x	x		Yes	Yes	To ensure that formal transfer policies, procedures and controls are in place to protect the transfer of information through the use of all types of communication facilities.
5.15	Organisational controls	Access control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and		x		Yes	Yes	To ensure that access to networks is carried out in a controlled manner and that the minimisation of privileges principal is maintained.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
			information security requirements.						
5.16	Organisational controls	Identity management	The full life cycle of identities shall be managed.		x		Yes	Yes	To ensure Jisc can identify who (users, groups of users) or what (applications, systems, and devices) is accessing data or IT assets at any given moment, and how those identities are granted access rights.
5.17	Organisational controls	Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.		x		Yes	Yes	This control allows Jisc to take appropriate steps to protect user credentials, such as passwords and security questions, from unauthorised access.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
5.18	Organisational controls	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified, and removed in accordance with the organization's topic-specific policy on and rules for access control.		x		Yes	Yes	This control is used ensure that Jisc can implement procedures and controls to assign, modify, and revoke access rights to information systems consistent with its access control policy.
5.19	Organisational controls	Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.		x		Yes	Yes	To ensure that Information security requirements for mitigating the risks associated with supplier's access to the organization's assets are agreed with the supplier and documented.
5.20	Organisational controls	Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.		x		Yes	Yes	To ensure that all relevant information security requirements have been established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
5.21	Organisational controls	Managing information security in the information and communication technology (ICT) supply chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.		x		Yes	Yes	This control allows the risk within the ICT supply chain by establishing an “agreed level of security” between the parties.
5.22	Organisational controls	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.		x		Yes	Yes	Selected to monitor contractual requirements, to reduce the risk of software vulnerabilities in products and services supplied to us, and to manage physical security of facilities within the certification scope.
5.23	Organisational controls	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization’s information security requirements.		x		Yes	Yes	Selected to outline the processes that are required for the acquisition, use, management of and exit from cloud services, in relation to the organisation’s unique information security requirements.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
5.24	Organisational controls	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing, and communicating information security incident management processes, roles, and responsibilities by defining, establishing, and communicating information security incident management processes, roles, and responsibilities.	x	x		Yes	Yes	To ensure that Management responsibilities and procedures are established to ensure a quick, effective, and orderly response to information security incidents.
5.25	Organisational controls	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.		x		Yes	Yes	This control has been selected to allow the identification, prioritisation, and categorisation of information security incidents.
5.26	Organisational controls	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.		x		Yes	Yes	This control has been selected to ensure that Information security incidents shall be responded to in accordance with the documented procedures.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
5.27	Organisational controls	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.		x		Yes	Yes	to ensure that knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
5.28	Organisational controls	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition, and preservation of evidence related to information security events.		x		Yes	Yes	To ensure that the organization shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.
5.29	Organisational controls	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.		x		Yes	Yes	Selected to allow for the operational adjustments that Jisc will adopt when facing disruption, to protect information and preserve company assets.
5.30	Organisational controls	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained, and tested based on business continuity objectives and ICT continuity requirements.		x		Yes	Yes	This control has been selected to ensure that create processes and procedures have been created to ensure IT readiness in the event of a BCP event.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
5.31	Organisational controls	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 shall be identified, documented, and kept up to date.	x	x	x	Yes	Yes	A business impact analysis aims to establish how disruption of any kind could affect business continuity, regardless of the types of impacts and organisational variables involved.
5.32	Organisational controls	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	x	x	x	Yes	Yes	This control has been selected to ensure that appropriate procedures have been implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products.
5.33	Organisational controls	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access, and unauthorized release.	x	x	x	Yes	Yes	This control has been selected to ensure that to ensure records are protected from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislatory, regulatory, contractual, and

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
									business requirements.
5.34	Organisational controls	Privacy and protection of personal identifiable information (PII)	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	x	x	x	Yes	Yes	This control has been selected to allow the production of guidelines and procedures that meet the legal, statutory, regulatory, and contractual obligations of Jisc with respect to the storage, privacy, and protection of Personal Identifiable Information (PII) in all its form.
5.35	Organisational controls	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	x	x		Yes	Yes	This control has been selected to ensure that Jisc's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) are reviewed independently at planned intervals or when significant changes occur.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
5.36	Organisational controls	Compliance with policies, rules, and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules, and standards shall be regularly reviewed.	x	x		Yes	Yes	This control has been selected to ensure compliance with policies, rules, and standards for information.
5.37	Organisational controls	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	x	x		Yes	Yes	This control has been selected to ensure that operating procedures have been documented and made available to all users who need them.

6. People controls

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
6.1	People controls	Screening	Background verification checks on all candidates to become personnel shall 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.	x	x	x	Yes	Yes	This control has been selected to ensure that appropriate checks are carried out in accordance with the relevant laws, regulations, and ethics, and they are proportional to the business requirements.
6.2	People controls	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	x	x	x	Yes	Yes	It is a legal requirement for these to be in place. The contractual agreement with employees and contractors must state their and the Jisc's responsibilities for information security.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
6.3	People controls	Information security awareness, education, and training	Personnel of the organization and relevant interested parties shall 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.		x		Yes	Yes	This control ensures that all employees and relevant contractors receive appropriate awareness education and training to do their job well and securely.
6.4	People controls	Disciplinary process	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.		x	x	Yes	Yes	To ensure that any serious breaches of the organisations ISMS can be dealt with appropriately.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
6.5	People controls	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced, and communicated to relevant personnel and other interested parties.	x	x		Yes	Yes	To ensure that when an employee leaves employment or changes their role that adequate processes and controls are in place.
6.6	People controls	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed, and signed by personnel and other relevant interested parties.	x	x		Yes	Yes	To ensure that requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed, and documented.
6.7	People controls	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed, or stored outside the organization's premises.		x		Yes	Yes	To ensure that appropriate security measures are applied to off-site assets taking into account the different risks of working outside the organization's premises.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
6.8	People controls	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.		x		Yes	Yes	Selected to reduce the impact incidents, including exploited vulnerabilities, malware infections, and loss or theft of information in transfer.

7. Physical controls

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
7.1	Physical controls	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	x	x		Yes	Yes	To ensure that security perimeters have been defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
7.2	Physical controls	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	x	x		Yes	Yes	To ensure that secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
7.3	Physical controls	Securing offices, rooms, and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	x	x		Yes	Yes	To ensure that physical security for offices, rooms and facilities has been designed and applied.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
7.4	Physical controls	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.		x		Yes	Yes	Selected as a preventive control/detective control that ensures Jisc detect and deter unauthorised physical access.
7.5	Physical controls	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 shall be designed and implemented.	x	x		Yes	Yes	To enable Jisc to measure the potential adverse effects of environmental and physical threats and to mitigate and/or eliminate these effects by putting in place appropriate measures.
7.6	Physical controls	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	x	x		Yes	Yes	To ensure that procedures for working in secure areas have been designed and applied.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
7.7	Physical controls	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.		x		Yes	Yes	To ensure that a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities has been adopted.
7.8	Physical controls	Equipment siting and protection	Equipment shall be sited securely and protected.		x		Yes	Yes	To ensure that equipment is sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
7.9	Physical controls	Security of assets off-premises	Off-site assets shall be protected.		x		Yes	Yes	To ensure that appropriate security measures are applied to off-site assets taking into account the different risks.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
7.10	Physical controls	Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation, and disposal in accordance with the organization's classification scheme and handling requirements.		x		Yes	Yes	Selected to allow the mitigation of risks associated with unauthorised access, usage, deletion, alteration, and transmission of confidential data held on storage media devices.
7.11	Physical controls	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.		x		Yes	Yes	To ensure that business critical systems equipment has been protected from power failures and other disruptions caused by failures in supporting utilities.
7.12	Physical controls	Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference, or damage.		x		Yes	Yes	To ensure that power and telecommunications cabling carrying data or supporting information services have been protected from interception, interference, or damage.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
7.13	Physical controls	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity, and confidentiality of information.		x		Yes	Yes	To ensure that equipment shall be correctly maintained to ensure its continued availability and integrity.
7.14	Physical controls	Secure disposal or re-use of equipment	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.		x		Yes	Yes	To ensure that all items of equipment containing storage media are verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

8. Technological controls

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
8.1	Technological controls	User endpoint devices	Information stored on, processed by or accessible via user end point devices shall be protected.		x		Yes	Yes	This control has been collected to allow Jisc to guard and uphold the security of information assets stored on or accessible from endpoint user devices. This is achieved by establishing suitable policies, procedures, and controls.
8.2	Technological controls	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.		x		Yes	Yes	To ensure that the allocation and use of privileged access rights is controlled.
8.3	Technological controls	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.		x		Yes	Yes	To ensure that access to information and application system functions is granted in accordance with the access control policy.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
8.4	Technological controls	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.		x		Yes	Yes	To ensure that access to program source code is restricted.
8.5	Technological controls	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.		x		Yes	Yes	To ensure that the allocation of secret authentication information shall be controlled through a formal management process.
8.6	Technological controls	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	x	x		Yes	Yes	To ensure that the use of resources is monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
8.7	Technological controls	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.		x		Yes	Yes	Detection, prevention, and recovery controls to protect against malware must be implemented, combined with appropriate user awareness.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
8.8	Technological controls	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.		x		Yes	Yes	To ensure that information about technical vulnerabilities of information systems being used are obtained in a timely fashion, the organisations exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. Control required for Cyber Essentials certification.
8.9	Technological controls	Configuration management	Configurations, including security configurations, of hardware, software, services, and networks shall be established, documented, implemented, monitored, and reviewed.		x		Yes	Yes	This control has been selected to ensure hardware, software, services, and networks function correctly with required security settings, and configuration is not altered by unauthorised or incorrect changes.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
8.10	Technological controls	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.		x		Yes	Yes	This control has been selected to prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory, and contractual requirements for information deletion. The Data Governance team are developing a plan to fully rollout a Deletion\Retention register implementation plan.
8.11	Technological controls	Data masking	Data masking shall 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.		x		Yes	Yes	This control has been selected to reduce the exposure of sensitive information, including personally identifiable data, by masking it and presenting only the data that is required to perform the task at hand.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
8.12	Technological controls	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store, or transmit sensitive information.		x		Yes	Yes	This is a preventive control and a detective control that is to detect and prevent the unauthorised disclosure and extraction of information by individuals or systems.
8.13	Technological controls	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.		x		Yes	Yes	This control has been selected to ensure that backup copies of information, software and system images are taken and tested regularly in accordance with an agreed backup policy.
8.14	Technological controls	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.		x		Yes	Yes	This control has been selected to enhance the accessibility of business services and information systems.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
8.15	Technological controls	Logging	Logs that record activities, exceptions, faults, and other relevant events shall be produced, stored, protected, and analysed.		x		Yes	Yes	This control has been selected to ensure that event logs recording user activities, exceptions, faults, and information security events must be produced, kept, and regularly reviewed. Logging facilities and log information must be protected against tampering and unauthorized access.
8.16	Technological controls	Monitoring activities.	Networks, systems, and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.		x		Yes	Yes	This control has been selected to ensure that networks, systems, and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.
8.17	Technological controls	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.		x		Yes	Yes	Selected to ensure that the detection of exploitation of software vulnerabilities, malware infections, physical intrusions, and loss of information in transfer is carried out.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
8.18	Technological controls	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.		x		Yes	Yes	To ensure that the use of computer programmes that might be capable of overriding system and application controls is strictly managed.
8.19	Technological controls	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.		x		Yes	Yes	Selected to reduce the risk of software vulnerabilities being introduced into systems.
8.20	Technological controls	Networks security	Networks and network devices shall be secured, managed, and controlled to protect information in systems and applications.	x	x		Yes	Yes	To ensure that networks are managed and controlled to protect information in systems and applications.
8.21	Technological controls	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented, and monitored.	x	x		Yes	Yes	To ensure that security mechanisms, service levels and management requirements of all network services have been identified and included in network services agreements.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
8.22	Technological controls	Segregation in networks	Groups of information services, users and information systems shall be segregated in the organization's networks.		x		Yes	Yes	To ensure groups of information services, users and information systems are segregated on networks.
8.23	Technological controls	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.		x		Yes	Yes	This control has been selected to assists Jisc in eliminating security risks such as malware infection from accessing external websites with malicious content.
8.24	Technological controls	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined, and implemented.		x		Yes	Yes	To ensure that a policy on the use of cryptographic controls for protection of information has been developed and implemented.
8.25	Technological controls	Secure development lifecycle	Rules for the secure development of software and systems shall be established and applied.		x		Yes	Yes	selected to ensure that Jisc adheres to the requirements for constructing secure software products, systems, and architecture.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
8.26	Technological controls	Application security requirements	Information security requirements shall be identified, specified, and approved when developing or acquiring applications.		x		Yes	Yes	Selected to ensure that Jisc defends their data assets stored on or processed by applications through the recognition and application of appropriate information security specifications.
8.27	Technological controls	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained, and applied to any information system development activities.		x		Yes	Yes	Selected to ensure that Jisc implements a secure system architecture and engineering principles to ensure that the design, implementation, and management of the information system are appropriate to the organisation's security requirements.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
8.28	Technological controls	Secure coding	Secure coding principles shall be applied to software development.		x		Yes	Yes	Selected to assists Jisc in preventing security risks and vulnerabilities that may arise due to poor software coding practices through developing, implementing, and reviewing appropriate secure software coding practices.
8.29	Technological controls	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.		x		Yes	Yes	Selected to allow Jisc to ensure that all security requirements are met when new applications, databases, software, or code are implemented.
8.30	Technological controls	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.		x		Yes	Yes	Selected to ensure that Jisc supervises and monitors the activity of outsourced system development.
8.31	Technological controls	Separation of development, test, and production environments	Development, testing and production environments shall be separated and secured.	x	x		Yes	Yes	Selected to ensure that the development, testing, and operational environments are separated to reduce the risks of

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
									unauthorized access or changes to the operational environment.
8.32	Technological controls	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	x	x		Yes	Yes	Selected to ensure changes to the organization, business processes, information processing facilities and systems that affect information security are controlled and do not unintentionally decrease Jisc's security posture.
8.33	Technological controls	Test information	Test information shall be appropriately selected, protected, and managed.	x	x		Yes	Yes	Selected to ensure that test data is selected carefully, protected, and controlled.

Nr.	Chapter	Topic	Control	Business / Contractual requirement	Risk Assessment Requirement	Legal Requirement	Applicable to our organisation (Yes/No)	Implemented in our organisation (Yes/No)	Reason for Selection / Exclusion
8.34	Technological controls	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.		x		Yes	Yes	Selected to minimise the impact of audit and other assurance activities on operational systems and business processes.