Statement of Applicability - Version 1

Issue Date: 14/04/2026
Business Use Only

Sec	ISO/IEC 27001:2022 Annex A controls	Control Type	IS Properties	CS Concepts	Applicable	Control detail	Key driver	Justification for exclusion	Responsibility
5	**Organisational Controls**								
5.1	**Policies for Information Security** **Control:** 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.	Preventative	Confidentiality Integrity Availability	Identify	Yes	Detailed in all procedures with ISMS framework, Policies are maintained within Shred-x & Med-X's IMS System	CO, AR ABP		SRX
5.2	**Information Security Roles and Responsibilities** **Control:** Information Security Roles and Responsibilities should be defined and allocated according to the organisational needs.	Preventative	Confidentiality Integrity Availability	Identify	Yes	ISMS Manual (Section 3.3 & 5.2) and updated policies in place, commitment requirements are stipulated in individual position descriptions and provided training.	CO, ABP		SRX
5.3	**Segregation of Duties** **Control:** Conflicting duties and conflicting areas of responsibility should be segregated.	Preventative	Confidentiality Integrity Availability	Protect	Yes	ISMS Manual (Section 3.3 & 5.2) and updated policies in place Refer to the Access Control Management Policy	CO, ABP		SRX
5.4	**Management Responsibilities** **Control:** Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organisation.	Preventative	Confidentiality Integrity Availability	Identify	Yes	Recruitment now controlled by People & Culture in liaison with Management. Policies are established, communicated and available by request.	LR, CO		SRX
5.5	**Contact with authorities** **Control:** The organisation should establish and maintain contact with relevant authorities.	Preventative Corrective	Confidentiality Integrity Availability	Identify Protect Respond Recover	Yes	Established Communications Plan & Business Continuity Plan & ISMS Manual - System Controls (A5)	LR, CO, AR, ABP		SRX
5.6	**Contact with special interest groups** **Control:** The organisation should establish and maintain contact with special interest groups or other special security forums and professional associations.	Preventative Corrective	Confidentiality Integrity Availability	Protect Respond Recover	Yes	Special interest groups are identified, ISMS Manual - System Controls (A5)	LR, CO, AR, ABP		SRX
5.7	**Threat intelligence** **Control:** Information relating to information security threats should be collected and analysed to produce threat intelligence.	Preventative Detective Corrective	Confidentiality Integrity Availability	Identify Respond Recover	Yes	Special interest groups who offer threat intelligence to the organisation are identified, ISMS Manual - System Controls (A5) Ongoing Threat Intelligence is provided by the FIS team	LR, CO, AR, ABP		FIS
5.8	**Information security in project management** **Control:** Information security should be integrated into project management.	Preventative	Confidentiality Integrity Availability	Identify Protect	Yes	Aligns to Freightways (FIS) procedures. Shred-X and Med X maintain documented procedures which include considerations for information security respective to the mapped process.	CO, ABP		SRX / FIS
5.9	**Inventory of information and other associated assets** **Control:** An inventory of information and other associated assets, including owners, should be developed and maintained.	Preventative	Confidentiality Integrity Availability	Identify	Yes	Detailed in company procedures and Corporate asset register is maintained	ABP		SRX
5.10	**Acceptable use of information and other associated assets** **Control:** Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to the Asset Management Policy, Acceptable Use Policy and Email Use Policy Detailed in company procedures and a Corporate asset register is maintained	CO, ABP		SRX / FIS
5.11	**Return of assets** **Control:** Personnel and other interested parties as appropriate should return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to the Asset Management Policy & the change of employment and termination process, detailed in company procedures and a corporate asset register is maintained	ABP		SRX
5.12	**Classification of information:** **Control:** Information should be classified according to the information security needs of the organisation base on confidentiality, integrity, availability and relevant interested party requirements.	Preventative	Confidentiality Integrity Availability	Identify	Yes	Refer to the Information Classification Policy & Asset Management Policy	LR, CO, ABP		SRX
5.13	**Labelling of information** **Objective:** To facilitate the communication of classification of information and support automation of information processing and management. **Control:** An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organisation.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to the Information Classification Policy & Asset Management Policy	CO, ABP		SRX
5.14	**Information Transfer** **Control:** Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organisation and between the organisation and other parties.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to the Asset Management Policy	CO, ABP		SRX
5.15	**Access Control** **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.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Access control policy in place and up to date Controlled via IT Manager and Freightways Access Control Management Policy	LR, CO, ABP		SRX / FIS
5.16	**Identity Management** **Control:** The full life cycle of identities should be managed.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Controlled with Leadership Team and IT Manager and Internal IT Team User Authentication Policy Access Control Management Policy	CO, ABP		SRX / FIS
5.17	**Authentication Information** **Control:** Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Controlled at restricted levels and detailed in procedures Controlled with Leadership Team and IT Manager and Internal IT Team Refer to the User Authentication Policy & Password Policy	CO, ABP		SRX / FIS
5.18	**Access Rights** **Control:** Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy on and rules for access control.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Controlled with Leadership Team and IT Manager and Internal IT Team Refer to the Access Control Management Policy	CO, ABP		SRX / FIS
5.19	**Information security in supplier relationships** **Control:** Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Preventative	Confidentiality Integrity Availability	Identify	Yes	Refer to the IT Supplier Security Policy & Access Control Management Policy. Detailed in all procedures with ISMS framework.	LR, CO, AR, ABP		SRX
5.20	**Addressing information security within supplier agreements** **Control:** Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	Preventative	Confidentiality Integrity Availability	Identify	Yes	Refer to the IT Supplier Security Policy & Access Control Management Policy. Detailed in all procedures with ISMS framework.	LR, CO, AR, ABP		SRX
5.21	**Managing information security in the ICT supply chain (Information and Communication Technology)** **Control:** Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Preventative	Confidentiality Integrity Availability	Identify	Yes	Detailed in all procedures with ISMS framework. Refer to the ISMS Manual - System Controls (A5).	LR, CO, AR, ABP		SRX
5.22	**Monitoring, review and change management of supplier services** **Control:** The organisation should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Preventative	Confidentiality Integrity Availability	Identify	Yes	Detailed in all procedures with ISMS framework. Refer to the ISMS Manual - System Controls (A5). IT Supplier Security Policy.	LR, CO, ABP		SRX
5.23	**Information security for use of cloud services** **Control:** Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organisation's information security requirements.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to the IT Supplier Security Policy. Detailed in all procedures with ISMS framework. Refer to the ISMS Manual - System Controls (A5). Additionally, FIS is wrapping this into a forthcoming policy on third party management, in addition to cloud service review process	LR, CO, AR, ABP		SRX / FIS
5.24	**Information security incident management planning and preparation**								

Legend

Applied?	
Yes	Control implemented and effective
No	Control not implemented
Partial	Control implemented but not fully effective
N/A	Control not applicable to ISMS scope

Key driver	
LR	Legal requirement
CO	Contractual obligation
CC	Client commitment
BR	Business requirement derived from risk assessment
ABP	Adopted best practice
N/A	Control not applicable to ISMS scope

Responsibility	
SRX	
FIS	
SRX / FIS	
SRX / FRW	

Statement of Applicability - Version 1

Issue Date: 14/04/2026
Business Use Only

	ISO/IEC 27001:2022 Annex A controls	Control Type	IS Properties	CS Concepts	Applicable	Control detail	Key driver	Justification for exclusion	Responsibility
	Control: The organisation should plan and prepare for managing information security incidents by determining, establishing and communicating information security incident management processes, roles and responsibilities.	Corrective	Confidentiality Integrity Availability	Respond Recover	Yes	Refer to the Procedure for Information Security Incident Response & Disaster Recovery Plan Policy All incident management activities are completed in tandem with FIS	LR, CO, ABP		FIS
5.25	**Assessment and decision on information security events**								
	Control: The organisation should assess information security events and decide if they are to be categorised as information security incidents.	Detective	Confidentiality Integrity Availability	Detect Respond	Yes	Procedure for Information Security Incident Response Disaster Recovery Plan Policy All incident management activities are completed in tandem with FIS	LR, CO, ABP		FIS
5.26	**Response to information security incidents**								
	Control: Information security incidents should be responded to in accordance with the documented procedures.	Corrective	Confidentiality Integrity Availability	Respond Recover	Yes	Procedure for Information Security Incident Response Disaster Recovery Plan Policy All incident management activities are completed in tandem with FIS	LR, CO, ABP		FIS
5.27	**Learning from information security incidents**								
	Control: Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	Preventative	Confidentiality Integrity Availability	Identify Protect	Yes	Procedure for Information Security Incident Response Disaster Recovery Plan Policy All incident management activities are completed in tandem with FIS	LR, CO, ABP		FIS
5.28	**Collection of evidence**								
	Control: The organisation should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Corrective	Confidentiality Integrity Availability	Detect Respond	Yes	Procedure for Information Security Incident Response Disaster Recovery Plan Policy All incident management activities are completed in tandem with FIS	LR, CO, ABP		FIS
5.29	**Information security during disruption**								
	Control: The organisation should plan how to maintain information security at an appropriate level during disruption.	Preventative Corrective	Confidentiality Integrity Availability	Detect Respond	Yes	Shred-X and Med-X Business Continuity Management is outlined within Business Continuity Plan	LR, CO, AR, ABP		SRX / FIS
5.30	**ICT readiness for business continuity (Information and Communication Technology)**								
	Control: ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Corrective	Availability	Respond	Yes	Shred-X and Med-X Business Continuity Management is outlined within Business Continuity Plan	LR, CO, AR, ABP		SRX
5.31	**Legal, statutory, regulatory and contractual requirements**								
	Control: Legal, statutory, regulatory and contractual requirements relevant to information security and the organisation's approach to meet these requirements should be identified, documented and kept up to date.	Preventative	Confidentiality Integrity Availability	Identify	Yes	For a list of legislative and regulatory requirements please refer to document Legal & Compliance Register' covering employment law, privacy, intellectual property rights etc. Requirements are reviewed frequently in accordance with the internal auditing program.	LR, CO, ABP		SRX / FRW
5.32	**Intellectual property rights**								
	Control: The organisation should implement appropriate procedures to protect intellectual property rights.	Preventative	Confidentiality Integrity Availability	Identify	Yes	The organisation appropriately registers the business, domain names and products as applicable. Confidentiality agreements and non-disclosure agreements are applied throughout the organisation. IP Rights (such as domains) are handled via policy/execution/instruction from NZ. During aqusitionions, etc, oversight is provided via Marva and Stephen Micallef.	LR, CO, ABP		SRX / FRW
5.33	**Protection of records**								
	Control: Records should be protected from loss, destruction, falsification, unauthorised access and unauthorised release.	Preventative	Confidentiality Integrity Availability	Identify Protect	Yes	Shred-X & Med-X ensure the protection of digital records via back ups, malware protection, digital environment management, change management and operating procedures. Refer to the Data Protection Policy	LR, CO, ABP		SRX
5.34	**Privacy and protection of Personally Identifiable Information (PII)**								
	Control: The organisation should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Preventative	Confidentiality Integrity Availability	Identify Protect	Yes	Shred-X & Med-X adhere to the Australian Privacy Principles and manage all PII in accordance with the privacy policy.	LR, CO, ABP		SRX
5.35	**Independent review of information security**								
	Control: The organisation'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.	Preventative Corrective	Confidentiality Integrity Availability	Identify Protect	Yes	Shred-X/ Med-X is subject to Independent reviews which is controlled by Freightways audit program controls.	LR, ABP		SRX
5.36	**Compliance with policies, rules and standards for information security**								
	Control: Compliance with the organisation's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	Preventative Corrective	Confidentiality Integrity Availability	Identify Protect	Yes	Shred-X/Med-X will have its Information Security Management System regularly audited both internally by FIS Security team and other Auditors within the Freightways group in accordance with the internal audit program. Auditors have undertaken ISO internal auditor training through Advisera.com including certification. Shred-X/Med-X will be externally assessed by an accredited certification body.	ABP		SRX
5.37	**Documented operating procedures**								
	Control: Operating procedures for information processing facilities should be documented and made available to personnel who need them.	Preventative Corrective	Confidentiality Integrity Availability	Protect Recover	Yes	Documented Procedures and Work Instructions have been developed and are stored in the IMS.	LR, CO, ABP		SRX
6	**People Controls**								
6.1	**Screening**								
	Control: Background verification checks on all candidates to become personnel should be carried out prior to joining the organisation and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Detailed in Shred-X and Med-X Operational procedures for police and visa screening arrangements and as outlined in Freightways HR2 policy, reference checks and criminal conviction history checks are conducted. The criminal conviction history check is a mandatory requirement of all Shred- X and Med-X staff dealing in information management business units.	LR, CO, AR, ABP		SRX
6.2	**Terms and Conditions of Employment**								
	Control: The employment contractual agreements should state the personnel's and the organisation's responsibilities for information security.	Preventative	Confidentiality Integrity Availability	Protect	Yes	ISMS Manual (Section 3.3 & 5.2) and updated policies in place Position descriptions are in place for all staff and are acknowledged at the time of induction.	LR, CO, ABP		SRX
6.3	**Information security awareness, education and training**								
	Control: Personnel of the organisation and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organisation's information security policy, topic-specific policies and procedures, as relevant for their job function.	Preventative	Confidentiality Integrity Availability	Protect	Yes	FIS team provide supported material to People and Culture for Learning Platform	LR, CO		SRX
6.4	**Disciplinary Process**								
	Control: A disciplinary process should be formalised and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Preventative Corrective	Confidentiality Integrity Availability	Protect Respond	Yes	Detailed in policies and part of HR Management & corporate guidelines	LR, CO		SRX
6.5	**Responsibilities after termination or change of employment** **Objective:** To ensure personnel and other relevant interested parties understand the consequences of information security policy violation, to deter and appropriately deal with personnel and other relevant interested parties who committed the violation.								
	Control: 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.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Processing assets is outlined in the change of employment and termination process. Refer to ISMS Manual - System Controls (A6) All staff sign an NDA	LR, AR, ABP		SRX
6.6	**Confidentiality or non-disclosure agreements**								
	Control: Confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Preventative	Confidentiality Integrity Availability	Protect	Yes	NDA or CA with all staff and contractors as part of their employment agreement and/or in some case a separate agreement	LR, CO, AR, ABP		SRX
6.7	**Remote Working**								

Legend

Statement of Applicability - Version 1

Issue Date: 14/04/2026
Business Use Only

	ISO/IEC 27001:2022 Annex A controls	Control Type	IS Properties	CS Concepts	Applicable	Control detail	Key driver	Justification for exclusion	Responsibility
	Control: Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Please refer to the Mobile Phone Device Teleworking Policy in addition to the Working From Home Policy.	LR, CO, AR, ABP		SRX
6.8	**Information security event reporting**								
	Control: The organisation should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Detective	Confidentiality Integrity Availability	Detect	Yes	Shred-X/Med-X incident management and response plan is outlined within Incident Management Manual	LR, CO, ABP		SRX
7	**Physical controls**								
7.1	**Physical security perimeters**								
	Control: Security perimeters should be defined and used to protect areas that contain information and other associated assets.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to Physical Access Site Operations Security Policy, Visitor Access Policy & IT Asset Management Policy	LR, CO, ABP		SRX
7.2	**Physical entry**								
	Control: To ensure only authorized physical access to the organisation's information and other associated assets occurs.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to Physical Access Site Operations Security Policy, Visitor Access Policy & IT Asset Management Policy	LR, CO, ABP		SRX
7.3	**Securing offices, rooms and facilities**								
	Control: Physical security for offices, rooms and facilities should be designed and implemented.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to Physical Access Site Operations Security Policy, Visitor Access Policy & IT Asset Management Policy	LR, CO, ABP		SRX
7.4	**Physical security monitoring**								
	Control: Premises should be continuously monitored for unauthorised physical access.	Preventative Detective	Confidentiality Integrity Availability	Protect Detect	Yes	Refer to Physical Access Site Operations Security Policy & IT Asset Management Policy. SRX deploy CCTV and monitored access control systems.	CO, ABP		SRX
7.5	**Protecting against physical and environmental threats**								
	Control: Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to Physical Access Site Operations Security Policy, IT Asset Management Policy & Business Continuity Plan	LR, CO, ABP		SRX
7.6	**Working in secure areas**								
	Control: Security measures for working in secure areas should be designed and implemented.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to Physical Access Site Operations Security Policy & IT Asset Management Policy	LR, CO, ABP		SRX
7.7	**Clear desk and clear screen**								
	Control: Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	Preventative	Confidentiality	Protect	Yes	Refer to the Clear Desk and Unattended User Equipment Policy & Workstation Policy ISMS Manual - System Controls (A7)	LR, CO, AR, ABP		SRX
7.8	**Equipment siting and protection**								
	Control: Equipment should be sited securely and protected.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to the Workstation Policy, IT Asset Management Policy & Physical Access Site Operations Security Policy ISMS Manual - System Controls (A7)	LR, CO, ABP		SRX
7.9	**Security of assets off-premises**								
	Control: Off-site assets should be protected.	Preventative	Confidentiality Integrity Availability	Protect	Yes	ISMS Manual - System Controls (A7) Mobile Phone Device Teleworking Policy	LR, CO, ABP		SRX
7.10	**Storage Media**								
	Control: Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organisation's classification scheme and handling requirements.	Preventative	Confidentiality Integrity Availability	Protect	Yes	ISMS Manual - System Controls (A7) Refer to the Asset Management Policy. Disposal may only occur post approval from the IT Manager.	CO, ABP		SRX
7.11	**Supporting utilities**								
	Control: Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	Preventative Detective	Integrity Availability	Protect Detect	Yes	All business critical IP facilities are hosted in Azure which have mutiple redundancies for localized utility failures.	LR, CO, ABP		SRX
7.12	**Cabling security**								
	Control: Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	Preventative	Confidentiality Availability	Protect	Yes	Network configuration prevents unsolicted devices from gaining access to the SRX/MDX network. Network devices are in racks and cabinets with secured access. Sites are physically secured with CCTV, gates, doors, and visitor management policies.	LR, CO, ABP		SRX
7.13	**Equipment maintenance**								
	Control: Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	Preventative	Confidentiality Integrity Availability	Protect	Yes	ISMS Manual - System Controls (A7) Management maintains maintenance and support agreements on all systems and network infrastructure and supporting utilities. Details of which are maintained by IT Management and Leadership Team	LR, CO, ABP		SRX
7.14	**Secure disposal or re-use of equipment**								
	Control: 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.	Preventative	Confidentiality	Protect	Yes	Refer to the ISMS Disposal and Destruction Policy & Asset Management Policy.	LR, CO, ABP		SRX
8	**Technological controls**								
8.1	**User endpoint devices**								
	Objective: To protect information against the risks introduced by using user endpoint devices.								
	Control: Information stored on, processed by or accessible via user endpoint devices should be protected.	Preventative	Confidentiality Integrity Availability	Protect	Yes	ISMS Manual - System Controls (A8) Refer to the Mobile Phone Device Teleworking Policy, Asset Management Policy and Cyber Security Policy . This is controlled in tandem with the FIS IT team	LR, CO, ABP		FIS
8.2	**Privileged access rights**								
	Control: The allocation and use of privileged access rights should be restricted and managed.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Access Control Management Policy ISMS Manual - System Controls (A8) A number of systems provide and/or utilise multi factor authentication user access and in many cases enforce it especially with regard to privileged access. Privileged access is restricted to discrete administrative accounts which are isolated from standard user activities. Implementation of PAM-specific tooling in H2 2025 will further increase isolation/logging capability.	CO, ABP		FIS
8.3	**Information access restriction**								
	Control: Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Access Control Management Policy Information Classification Policy ISMS Manual - System Controls (A8) Least Privilege principal applied. Tech team specific user onboarding detail role based systems access.	ABP		FIS
8.4	**Access to source code**								
	Control: Read and write access to source code, development tools and software libraries should be appropriately managed.	Preventative	Confidentiality Integrity Availability	Protect	Yes	All source code is stored within Azure DevOps (formerly Visual Studio Team Services) and activity is logged and changes tracked and reviewable showing before and after changes at line-by-line level. Shred-X and Med-X align to the following - Freightways 'FISPO002 Secure Development Policy' Specically, actions taken within SRX do not generate source code, (dynamics and PowerBI) and access to source code is not a standardised requirement for SRX.	ABP		FIS
8.5	**Secure authentication**								

Legend

Statement of Applicability - Version 1

Issue Date: 14/04/2026
Business Use Only

	ISO/IEC 27001:2022 Annex A controls	Control Type	IS Properties	CS Concepts	Applicable	Control detail	Key driver	Justification for exclusion	Responsibility
	Control: Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to the Password Policy, Access Control Management Policy and User Authentication Policy All systems maintained or used by Shred-X or Med-X utilise secure log procedures of one kind or another and will lock out users after a defined number of unsuccessful attempts to protect against brute force log- on attempts. A number of systems provide and/or utilise multi factor authentication user access and in many cases enforce it especially with regard to privileged access. Secure Authentication is maintained in tandem with FIS.	CO, ABP		FIS
8.6	**Capacity management**								
	Control: The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	Preventative Detective	Integrity Availability	Identify Detect Protect	Yes	Several monitoring tools are utilised across systems within the corporate environment monitoring their performance, capacity and availability. •Operational Checklists •PRTG monitoring •New Relic monitoring •VMware with Operations Management, vRealise Operations •Site 24/7	LR, ABP		SRX
8.7	**Protection against malware**								
	Control: Protection against malware should be implemented and supported by appropriate user awareness.	Preventative Detective Corrective	Confidentiality Integrity Availability	Protect Detect	Yes	Layered connected threat defence; Trend Micro Smart Protection suite utilising Trend Micro Deep Security as a service and Apex One as a service, along with Cloud App Security and Hosted Email Security protecting server and workstations along email and Office365 platform. Malware protection is completed in tandem with FIS Refer to the Software Installation Policy, Acceptable Use Policy, Email Use Policy & Internet Usage and Filtering Policy	LR, CO, AR, ABP		FIS
8.8	**Management of technical vulnerabilities**								
	Control: Information about technical vulnerabilities of information systems in use should be obtained, the organisation's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	Preventative	Confidentiality Integrity Availability	Identify Protect	Yes	Shred-X and Med-X align to processes with Freightways document 'FISSTD002 Vulnerability Management Standard'.	LR, CO, AR, ABP		SRX / FIS
8.9	**Configuration management**								
	Control: Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	Preventative	Confidentiality Integrity Availability	Identify Protect	Yes	Shred-x and Med-X have defined acceptable configuration standards within the server security policy. Further documentation on device preparation and configuration is currently undergoing review. Trend XDR enforces security-related device permissions (USB, network access, exfil). Full RMM suite due for implementation H2 2025.	ABP	**Linked to previously excluded 14.2.5**	SRX / FIS
8.10	**Information deletion**								
	Control: Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	Preventative	Confidentiality	Protect	Yes	Refer to the ISMS Disposal and Destruction Policy	LR, CO, ABP		SRX / FIS
8.11	**Data masking**								
	Control: Data masking should be used in accordance with the organisation's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Preventative	Confidentiality	Protect	N/A		N/A	While sensitive information is held internally with regard HR (Staff) this is restricted to People & Culture (HR) staff and their systems only and the associated staff may access information related to themselves but is not shared with external parties where specified information may need to be masked. Systems servicing customers are not holding sensitive information and this relates to client service details typical business information provided by the client and not shared with other parties, only authorised Shred-X Staff have access as necessary to undertake required services. As such at this time there are no systems with information that require specific information to be masked from unauthorised parties.	SRX / FIS
8.12	**Data leakage prevention**								
	Control: Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Preventative Detective	Confidentiality	Protect Detect	Yes	Refer to Non-Disclosure Agreements, Acceptable Use Policy, Information Security Policy. The Trend platform provides DLP functionality and monitoring for removable storage, email, cloud storage usage (e.g. OneDrive, Google Drive)	CO, ABP		SRX / FIS
8.13	**Information backup**								
	Control: Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Corrective	Integrity Availability	Recover	Yes	Shred-X/Med-X currently use Azure Backup to deliver local resource protection and Azure Site Recovery to deliver geographic disaster recovery to key systems. Monitoring is alert-driven and raises incidents automatically in ITSM tooling which are investigated as P1 events.	CO, ABP		SRX
8.14	**Redundancy of information processing facilities**								
	Control: Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	Preventative	Availability	Protect	Yes	Shred-X Business Continuity Management is outlined within Business Continuity Plan. Redundancy of systems is assured through use of a trusted provider Azure AZ.	ABP		SRX / FIS
8.15	**Logging**								
	Control: Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	Detective	Confidentiality Integrity Availability	Detect	Yes	All IaaS servers whether hosted within corporate or Revera Homeland IaaS generating event logs. Critical Systems captured through Trend Micro Deep Security Log inspection. Azure hosted systems utilise Cloud Trail. Logs aggregated where possible and copy protected.	LR, CO, AR, ABP		SRX / FIS
8.16	**Monitoring activities**								
	Control: Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Detective Corrective	Confidentiality Integrity Availability	Detect Respond	Yes	Trend Micro Deep Security log inspection viewable from Trend Deep Security Manager by appropriately authorised individuals. Systems and services within Azure Services. Microsoft Azure tooling in place monitoring servers that are now running with Azure. Monitoring activities are managed in tandem with the FIS team. EDR is Trend, MDR is the Cybersecurity team/external SOC	LR, CO, AR, ABP		SRX / FIS
8.17	**Clock synchronization**								

Legend

Statement of Applicability - Version 1

Issue Date: 14/04/2026
Business Use Only

	ISO/IEC 27001:2022 Annex A controls	Control Type	IS Properties	CS Concepts	Applicable	Control detail	Key driver	Justification for exclusion	Responsibility
	Control: The clocks of information processing systems used by the organisation should be synchronized to approved time sources.	Detective	Integrity	Detect Respond	Yes	ISMS Manual - System Controls (A8) Domain controllers and systems are synchronised to Microsoft time servers.	LR, CO, AR, ABP		SRX
8.18	**Use of privileged utility programs**								
	Control: The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	Preventative	Confidentiality Integrity Availability	Protect	Yes	The use of privileged access programs is restricted to specific administrative jumphosts, that themselves are restricted to authorised users within the FIS and SRX IT teams. Use of privileged utility programs are managed in tandem with the FIS team.	ABP		FIS
8.19	**Installation of software on operational systems**								
	Control: Procedures and measures should be implemented to securely manage software installation on operational systems.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to the Software Installation Policy Software Installation is managed in tandem with the FIS team.	LR, CO, AR, ABP		FIS
8.20	**Networks security**								
	Control: Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	Preventative Detective	Confidentiality Integrity Availability	Protect Detect	Yes	Refer to the Network Security Policy Network Security is managed in tandem with the FIS team.	LR, CO, AR, ABP		FIS
8.21	**Security of network services**								
	Control: Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to the ISMS Manual - System Controls FIS maintains network infrastructure supporting both Shred-X/Med-X and some clients (other Freightways group companies) both at a datacentre level and branch network level.	LR, CO, AR, ABP		FIS
8.22	**Segregation of networks**								
	Control: Groups of information services, users and information systems should be segregated in the organisation's networks.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Segregation of networks is managed by FIS; At the branch network level, the network is segregated into 2 wired and 3 wireless network segments.	LR, CO, AR, ABP		FIS
8.23	**Web filtering**								
	Control: Access to external websites should be managed to reduce exposure to malicious content.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to the Internet Usage and Filtering Policy	LR, CO, AR, ABP		FIS
8.24	**Use of cryptography**								
	Control: Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Use of Cryptography is managed by FIS; Corporate guidelines on cryptographic controls are outlined in the Freightways document 'FISGL004 Cryptographic Guidelines'	LR, CO, ABP		FIS
8.25	**Secure development life cycle**								
	Control: Rules for the secure development of software and systems should be established and applied.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Shred-X/ Med-X have a customer portal which was originally developed internally and is currently maintained. Shred-X/ Med-X currently adhere to established FIS development, coding and testing standards/ Procedures.	ABP		SRX / FIS
8.26	**Application security requirements**								
	Control: formation security requirements should be identified, specified and approved when developing or acquiring applications.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Refer to the Application Control Policy and the ARB process (Architectural Review Board)	LR, ABP		SRX / FIS
8.27	**Secure system architecture and engineering principles**								
	Control: Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Shred-X/ Med-X have a customer portal which was originally developed internally and is currently maintained. Shred-X/ Med-X currently adhere to established FIS development, coding and testing standards/ Procedures.	ABP		SRX / FIS
8.28	**Secure coding**								
	Control: Secure coding principles should be applied to software development.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Shred-X/ Med-X have a customer portal which was originally developed internally and is currently maintained. Shred-X/ Med-X currently adhere to established FIS development, coding and testing standards/ Procedures.	ABP		SRX / FIS
8.29	**Security testing in development and acceptance**								
	Control: Security testing processes should be defined and implemented in the development lite cycle.	Preventative	Confidentiality Integrity Availability	Identify	Yes	Shred-X/ Med-X have a customer portal which was originally developed internally and is currently maintained. Shred-X/ Med-X currently adhere to established FIS development, coding and testing standards/ Procedures.	ABP		SRX / FIS
8.30	**Outsourced development**								
	Control: The organisation should direct, monitor and review the activities related to outsourced system development.	Preventative Detective	Confidentiality Integrity Availability	Identify Detect Protect	N/A		N/A	**The organisation does not complete outsourced software development/ coding activities**	SRX / FIS
8.31	**Separation of development, test and production environments**								
	Control: Development, testing and production environments should be separated and secured.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Shred-X/ Med-X have a customer portal which was originally developed internally and is currently maintained. Shred-X/ Med-X currently adhere to established FIS development, coding and testing standards/ Procedures.	ABP		SRX / FIS
8.32	**Change management**								
	Control: Changes to information processing facilities and information systems should be subject to change management procedures.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Shred-X and Med-X aligned to processes with Freightways change management procedures are also outlined in the FIS Confluence Wiki Article	LR, AR, ABP		SRX / FIS
8.33	**Test information**								
	Control: Test information should be appropriately selected, protected and managed.	Preventative	Confidentiality Integrity	Protect	Yes	Shred-X/ Med-X have a customer portal which was originally developed internally and is currently maintained. While intial testing materials were not captured at the time of portal development, any further ongoing development/ testing records are to be maintiained in accordance with FIS' development, coding and testing standards/ Procedures.	ABP		SRX
8.34	**Protection of information systems during audit testing**								
	Control: Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.	Preventative	Confidentiality Integrity Availability	Protect	Yes	Audit controls in place and managed at local level and Freightway Information Security team	LR,CO, ABP		SRX

Legend