This self-assessment questionnaire is designed to indicate your readiness for ISO 27001:2013. We hope you find it useful.

4 Context of the organisation

4.1 Organisation and Content	
Have we determined the external and internal issues that are relevant to our business and that will affect the ability to achieve the intended outcome(s) of its ISMS?	☐
4.2 External Parties	
Have we determined the interested parties that are relevant to the ISMS and the requirements of these interested parties relevant to information security?	☐
4.3 Scope of the System	
Have we determined the boundaries and applicability of the ISMS to establish and document its scope?	☐
Have we considered the external and internal issues, the needs and expectations of interested parties and the interfaces and dependencies between activities performed by the business, and those that are performed by other organisations?	☐
4.4 Information Security Management System	
Have we established, implemented, maintained and continually improved an ISMS in accordance with the requirements of this international standard?	☐

5 Leadership

5.1 Leadership and Commitment	
Has top management demonstrated leadership and commitment to the ISMS by:	
a) Ensuring the information security policy and the information security objectives are established and compatible with the strategic direction of the organisation?	☐
b) Ensuring the integration of the ISMS requirements into the organisation's processes?	☐
c) Ensuring that the resources needed for the ISMS are available?	☐
d) Communicating the importance of effective information security management and conforming to the ISMS requirements?	☐
e) Ensuring that the ISMS achieves its intended outcome(s)?	☐
f) Directing and supporting persons to contribute to the effectiveness of the ISMS?	☐
g) Promoting continual improvement and supporting other relevant management?	☐
5.2 Policy	
Have we established an information security policy that:	
a) Is appropriate to the purpose of the organisation?	☐
b) Includes information security objectives (see 6.2) or provides the framework for setting information security objectives?	☐

c) Includes a commitment to satisfy applicable requirements related to information security and includes commitment to continual improvement of the ISMS?	☐
Is the information security policy:	
a) Available as documented information?	☐
b) Communicated within the organisation and available to interested parties?	☐
5.3 Organisational Roles, Responsibilities and Authorities	
Have we ensured that the responsibilities and authorities for roles relevant to information security are assigned and communicated?	☐
Have we assigned the responsibility and authority for:	
a) Ensuring that the ISMS conforms to the requirements of this International Standard?	☐
b) Reporting on the performance of the ISMS to top management?	☐

6 Planning

6.1 Risks and Opportunities	
6.1.1 General	
Have we considered the internal and external issues for our ISMS (see 4.1), the requirements of interested parties (see 4.2) and determined the risks and opportunities that need to be addressed to:	
a) Ensure it can achieve the intended outcomes?	☐
b) Prevent, or reduce undesired effects and achieve continual improvement?	☐
Have we planned:	
a) Actions to address these risks and opportunities?	☐
b) How to integrate and implement the actions in our ISMS processes and evaluate the effectiveness of these actions?	☐
6.1.2 Information Security Risk Assessment	
Have we defined and applied an information security risk assessment process that:	
a) Establishes and maintains information security risk criteria that includes the risk acceptance criteria and the criteria for performing information security risk assessments?	☐
b) Ensures that repeated information security risk assessments produce consistent valid and comparable results?	☐
c) Identifies the information security risks through a risk assessment process, to identify risks associated with the loss of confidentiality, integrity and availability for information and identify the risk owners?	☐
d) Analyses the information security risks and assess the potential consequences that would result if the risks identified were to materialise, assess the realistic likelihood of the occurrence of the risks identified and determine the levels of risk?	☐

e) Evaluates the information security risks and compares the results of risk analysis with the risk criteria established and prioritises the analysed risks for risk treatment?	☐
Do we retain documented information about the information security risk assessment process?	☐
6.1.3 Information Security Risk Management	
Have we defined and applied an information security risk treatment process to:	
a) Select appropriate information security risk treatment options, taking account of the risk assessment results?	☐
b) Determine (and design as required) all controls that are necessary to implement the information security risk treatment option(s) chosen?	☐
c) Compare the controls determined with those in Annex A and verify that no necessary controls have been omitted?	☐
d) Produce a Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A?	☐
e) Formulate an information security risk treatment plan?	☐
f) Obtain risk owners approval of the information security risk treatment plan and acceptance of the residual information security risks?	☐
Do we retain documented information about the information security risk treatment process?	☐
6.2 Information Security Objectives	
Have we established information security objectives at relevant functions and levels that:	
a) Are consistent with the information security policy?	☐
b) Are measurable (if practicable)?	☐
c) Take into account applicable information security requirements and results from risk assessments and risk treatment?	☐
d) Are communicated?	☐
e) Are updated as appropriate?	☐
Do we retain documented information on the information security objectives?	☐
When planning how to achieve our information security objectives, have we determined:	
a) What will be done and what resources will be required?	☐
b) Who will be responsible?	☐
c) When it will be completed and how will the results be evaluated?	☐

7 Support

7.1 Resources	
Have we determined and provided the resources needed for the implementation, maintenance and continual improvement of the ISMS?	☐
7.2 Competence	
Have we:	
a) Determined the necessary competence of person(s) doing work under its control that affects its information security performance?	☐
b) Ensured that these persons are competent on the basis of appropriate education, training or experience?	☐
c) Where applicable, taken actions to acquire the necessary competence and evaluate the effectiveness of the actions taken?	☐
d) Retained appropriate documented information as evidence of competence?	☐
7.3 Awareness	
Are persons under our business control aware of:	
a) The information security policy?	☐
b) Their contribution to the effectiveness of the ISMS, including the benefits of improved information security performance and the implications of not conformation with the ISMS requirements?	☐
7.4 Communication	
Have we determined the need for internal and external communications relevant to the ISMS including what to communicate, when to communicate and with whom to communicate?	☐
Have we determined who shall communicate and by the processes by which the communication shall be affected?	☐
7.5 Documented Information	
Have we implemented documented information required by the standard and determined necessary for the effectiveness of the ISMS?	☐
When creating and updating documented information, have we ensured appropriate:	
a) Identification and description (eg a title, date, author or reference number)?	☐
b) Format (eg language, software version, graphics) and media (eg paper, electronic)?	☐
c) Review and approval for suitability and adequacy for the effectiveness of the ISMS?	☐
Do we have processes to control documented information to ensure it is:	
a) Available and suitable for use, where and when it is needed?	☐
b) Adequately protected (eg from loss of confidentiality, improper use or loss of integrity)?	☐

Do these processes address the following activities (if applicable):	
a) Distribution, access, retrieval and use?	☐
b) Storage and preservation, including the reservation of legibility?	☐
Do we identify and control documented information of external origin, determined as necessary for the planning and operation of the ISMS?	☐

8 Operation

8.1 Operational Planning and Control	
Have we planned, implemented and controlled the processes needed to meet:	
a) Information security requirements and implemented the actions determined in 6.1?	☐
b) To achieve information security objectives determined in 6.2?	☐
Have we kept documented information to have confidence that the processes have been carried out as planned?	☐
Have we controlled and planned changes and reviewed the consequences of unintended changes, taking action to mitigate any adverse effects as necessary?	☐
Have we ensured that outsourced processes are determined and controlled?	☐
8.2 & 8.3 Information Security Risk Assessment & Treatment	
Do we perform information security risk assessments at planned intervals or when significant changes are proposed or occur?	☐
Do we retain documented information of the results of the information security risk assessments?	☐
Have we implemented an information security risk treatment plan?	☐
Do we retain documented information of the results of the information security risk treatment?	☐

9 Performance Evaluation

9.1 Monitoring, Measurement, Analysis and Evaluation	
Have we determined:	
a) What needs to be monitored and measured, including information security processes and controls?	☐
b) The methods for monitoring, measurement, analysis and evaluation to ensure valid results (methods selected should produce comparable and reproducible results to be considered valid)?	☐
c) When the monitoring and measuring shall be performed?	☐
d) Who shall monitor and measure?	☐

e) When the results from monitoring and measurement shall be analysed and evaluated, and who shall analyse and evaluate these results?	☐
Do we retain appropriate documented information as evidence of the monitoring and measurement results?	☐
9.2 Internal Audit	
Do we conduct internal audits at planned intervals to provide information on whether the ISMS is effectively implemented and maintained, and conforms to the organisation's own requirements for its ISMS and the requirements of this international standard?	☐
Have we:	
a) Planned, implemented and maintained an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting, taking into consideration the importance of the processes concerned and the results of previous audits?	☐
b) Defined the audit criteria and scope for each audit?	☐
c) Selected auditors and conducted audits that ensure objectivity and the impartiality of the audit process?	☐
d) Ensured that the results of the audits are reported to relevant management and retained documented information as evidence of the audit programme and the audit results?	☐
9.3 Management Review	
Does the management review include consideration of:	
a) The status of actions from previous management reviews?	☐
b) Changes in external and internal issues that are relevant to the ISMS?	☐
c) Feedback on the information security performance, including trends in nonconformities and corrective actions, monitoring and measurement results, audit results, and fulfillment of information security objectives?	☐
d) Feedback from interested parties?	☐
e) Results of risk assessment and status of risk treatment plan?	☐
f) Opportunities for continual improvement?	☐
Do the outputs of the management review include decisions related to continual improvement opportunities and any needs for changes to the ISMS?	☐
Do we retain documented information as evidence of the results of management review?	☐

10 Improvement

10.1 Nonconformity and Corrective Action	
When a nonconformity occurs, do we:	
a) React to the nonconformity, taking actions to control and correct it and deal with the consequences?	☐

b) Review the nonconformity, determining the cause and determining if similar nonconformities exist, or could potentially occur and eliminate the causes to prevent re-occurrence?	☐
c) Implement any action needed and review the effectiveness of any corrective actions taken?	☐
d) Make changes to the ISMS if necessary?	☐
Are the corrective actions appropriate to the effects of the nonconformities encountered?	☐
Do we retain documented information as evidence of the nature of the nonconformities and any subsequent actions taken, and the results of any corrective action?	☐
10.2 Continual Improvement	
Do we continually improve the suitability, adequacy and effectiveness of the ISMS?	☐

Appendix A

A.5 Information Security Policies	
A.5.1 Management Direction for Information Security	
A5.1.1 Policies for Information Security – Have we developed a set of policies for information security and communication to employees and relevant parties?	☐
A.5.1.2 Review of the Policies for Information Security – Do we review the policies for information security at planned intervals or if significant changes occur?	☐
A.6 Organisation of Information Security	
A.6.1 Internal Organisation	
A.6.1.1 Information security roles and responsibilities – Are all information security responsibilities defined and allocated?	☐
A.6.1.2 Segregation of Duties – Have we ensured conflicting duties and areas of responsibility are segregated?	☐
A.6.1.3 Contact with Authorities – Do we maintain appropriate contacts with relevant authorities?	☐
A.6.1.4 Contact with Special Interest Groups – Do we maintain appropriate contacts with special interest groups, forums and associations?	☐
A.6.1.5 Information Security in Project Management – Do we ensure information security is addressed in project management, regardless of the type of project?	☐
A.6.2 Mobile Devices and Teleworking	
A.6.2.1 mobile Device Policy – Have we implemented a policy and supporting security measures for mobile devices?	☐
A.6.2.2 Teleworking – Have we implemented a policy and supporting security measures for teleworking sites?	☐

A.7 Human Resource Security	
A.7.1 Prior to Employment	
A.7.1.1 Screening – do we perform background verification checks on all candidates for employment?	☐
A.7.1.2 Terms and Conditions of Employment – Do all contractual agreements with employees and contractors state their responsibilities for information security?	☐
A.7.2 During Employment	
A.7.2.1 Management Responsibilities – Does management ensure all employees and contractors act in accordance with the organisation's policies and procedures?	☐
A.7.2.2 information Security Awareness, Education and Training – Do all employees and contractors (where appropriate) receive awareness education and training?	☐
A.7.2.3 Disciplinary Process – Do we have a formal disciplinary process for an information security breach?	☐
A.7.3 Termination and Change of Employment	
A.7.3.1 Termination or Change of Employment Responsibilities – Do we ensure information security responsibilities and duties that remain valid after termination are communicated and enforced?	☐
A.8 Asset Management	
A.8.1 Internal Organisation	
A.8.1.1 Inventory of Assets – Do we have an inventory of assets which identifies information, and other assets associated with information and information processing facilities?	☐
A.8.1.2 Ownership of Assets – Do all assets maintained in the inventory have an owner?	☐
A.8.1.3 Acceptable Use of Assets – Are rules for the acceptable use of information and of assets documented and implemented?	☐
A.8.1.4 Return of Assets – Have we ensured all assets are returned upon termination of agreements / employment?	☐
A.8.2 Information Classification	
A.8.2.1 Classification of Information – Is information classified in terms of legal requirements, value, criticality and sensitivity?	☐
A.8.2.2 Labelling of Information – Have we an appropriate set of procedures for information labelling?	☐
A.8.2.3 Handling of Assets – Have we implemented procedures for handling assets?	☐
A.8.3 Media Handling	
A.8.3.1 Management of Removable Media – Have we implemented procedures for removable media?	☐
A.8.3.2 Disposal of Media – Is media disposed of securely using formal procedures?	☐
A.8.3.3 Physical Media Transfer – Is media containing information protected against unauthorised access, misuse or corruption during transportation?	☐

A.9 Access Control	
A.9.1 Business Requirements of Access Control	
A.9.1.1 Access Control Policy – Have we established a documented access control policy?	☐
A.9.1.2 Access to Networks and Network Services – Do we ensure users only have access to the network and network services that they have been specifically authorised to use?	☐
A.9.2 User Access Management	
A.9.2.1 User Registration and De-Registration – Has a formal user registration and de-registration process been implemented?	☐
A.9.2.2 User Access Provisioning – Do we have a formal user access process to assign or revoke access rights?	☐
A.9.2.3 Management of Privileged Access rights – Is the allocation and use of privileged access rights restricted and controlled?	☐
A.9.2.4 Management of Secret Authentication Information of Users – Is the allocation of secret authentication information controlled?	☐
A.9.2.5 Review of User Access Rights – Are user access rights reviewed at regular intervals?	☐
A.9.2.6 Removal or Adjustment of Access Rights – Are access rights to information and information processing facilities removed upon termination?	☐
A.9.3 User Responsibilities	
A.9.3.1 Use or Secret Authentication Information – Do we ensure users follow practices for secret authentication information?	☐
A.9.4 System and Application Access Control	
A.9.4.1 Information Access Restriction – Is access to information and application system functions restricted?	☐
A.9.4.2 Secure Log-On Procedures – Do we ensure where required access to systems and application is controlled by a secure log-on procedure?	☐
A.9.4.3 Password Management System – Is our password management interactive and do we ensure quality passwords?	☐
A.9.4.4 Use of Privileged Utility Programs – Do we ensure the use of utility programs that can override system controls are restricted and tightly controlled?	☐
A.9.4.5 Access Control to Program Source Code – Is access to program source code restricted?	☐
A.10 Cryptography	
A.10.1 Cryptographic Controls	
A.10.1.1 Policy on the Use of Cryptographic Controls – do we have a policy on the use of cryptographic controls?	☐
A.10.1.2 Key Management – Do we have a policy for cryptographic keys through their whole lifecycle?	☐

A.11 Physical and Environmental Security	
A.11.1 Secure Areas	
A.11.1.1 Physical Security Perimeter – Do we ensure security perimeters are used to protect areas that contain either sensitive or critical information and information processing facilities?	☐
A.11.1.2 Physical Entry Controls – Do authorised personnel only have access to secure areas?	☐
A.11.1.3 Securing Offices, Rooms and Facilities – Do we ensure the physical security for offices, rooms and facilities?	☐
A.11.1.4 Protecting Against External and Environmental Threats – Do we have adequate controls for protection against natural disasters, malicious attacks or accidents?	☐
A.11.1.5 Working in Secure Areas – Do we have procedures for working in secure areas?	☐
A.11.1.6 Delivery and Loading Areas – Are access points such as delivery and loading areas controlled and, if possible, isolated from information from information processing facilities?	☐
A.11.2 Equipment	
A.11.2.1 Equipment Siting and Protection – Is equipment sited and protected to reduce the risks from environmental threats and unauthorised access?	☐
A.11.2.2 Supporting Utilities – Is equipment protected from power failures and other disruptions?	☐
A.11.2.3 Cabling Security – Is power and telecommunications cabling carrying data protected from interception, interference or damage?	☐
A.11.2.4 Equipment Maintenance – Do we ensure equipment is maintained?	☐
A.11.2.5 Removal of Assets – Do we ensure equipment, information or software is not taken off-site without prior authorisation?	☐
A.11.2.6 Security of Equipment and Assets Off-Premises – Is adequate security applied to off-site assets?	☐
A.11.2.7 Secure disposal or Re-use of Equipment – Is all storage media verified to ensure all sensitive data and software is removed prior to disposal or re-use?	☐
A.11.2.8 Unattended User Equipment – Does all unattended equipment have appropriate protection?	☐
A.11.2.9 Clear Desk and Clear Screen Policy – Has a clear desk policy for papers, removable storage media and a clear screen policy been adopted?	☐
A.12 Operations Security	
A.12.1 Operational Procedures and Responsibilities	
A.12.1.1 Documented Operating Procedures – Have operating procedures been documented and made available to all users who need them?	☐
A.12.1.2 Change Management – Are changes to business processes, information processing facilities and systems controlled?	☐

A.12.1.3 Capacity Management – Are resources monitored, tuned and projections made for future capacity requirements to ensure system performance?	☐
A.12.1.4 Separation of Development, Testing and Operational Environments – Do we ensure development, testing and operational environments are separated?	☐
A.12.2 Protection from Malware	
A.12.2.1 Controls Against Malware – Are detection, prevention and recovery controls in place for malware?	☐
A.12.3 Backup	
A.12.3.1 Information Backup – Are backup copies of information, software and system images taken and tested regularly?	☐
A.12.4 Logging and Monitoring	
A.12.4.1 Event Logging – Are event logs recording user activities, exceptions, faults and information security events kept and regularly reviewed?	☐
A.12.4.2 Protection of Log Information – Have we ensured logging facilities and log information is protected against tampering and unauthorised access?	☐
A.12.4.3 Administrator and Operator Logs – Are system administrator and system operator activities logged and regularly reviewed?	☐
A.12.4.4 Clock Synchronisation – Are all clocks of all relevant information processing systems synchronised to a single reference time source?	☐
A.12.5 Control of Operational Software	
A.12.5.1 Installation of Software on Operational Systems – Do we control the installation of software on operational systems?	☐
A.12.6 Technical Vulnerability Management	
A.12.6.1 Management of Technical Vulnerabilities – Is technical vulnerability information obtained in a timely fashion and is our exposure to such vulnerabilities evaluated and measures taken to address the risk?	☐
A.12.6.2 Restrictions on Software Installation – Have we ensured rules governing the installation of software by users are implemented?	☐
A.12.7 Information Systems Audit Considerations	
A.12.7.1 Information Systems Audit Controls – Do we ensure audit requirements and activities involving verification of operational systems are planned and minimise disruption?	☐
A.13 Communication Security	
A.13.1 Network Security Management	
A.13.1.1 Network Controls – Are networks controlled to protect information?	☐
A.13.1.2 Security of Network Services – Are service levels, management and security requirements of all network services identified and included in network services agreements, for both in-house or outsourced services?	☐
A.13.1.3 Segregation in Networks – Are groups of information services, users and information systems segregated on networks?	☐

A.13.2 Information Transfer	
A.13.2.1 Information Transfer Policies and Procedures – Are policies, procedures and controls in place to protect the transfer of information with all types of communication facilities?	☐
A.13.2.2 Agreements on Information Transfer – Are agreements in place regarding the secure transfer of information between the organisation and external parties?	☐
A.13.2.3 Electronic Messaging – Do we ensure information involved in electronic messaging is appropriately protected?	☐
A.13.2.4 Confidentiality or Nondisclosure Agreements – Are confidentiality or nondisclosure agreements regularly reviewed and documented?	☐
A.14 System Acquisition, Development and Maintenance	
A.14.1 Security Requirements of Information Systems	
A.14.1.1 Information Security Requirements Analysis and Specification – Are information security requirements included in the requirements for new information systems or enhancements to existing systems?	☐
A.14.1.2 Securing Application Services on Public Networks – Have we ensured information involved in application services passing over public networks are protected from fraudulent activity, contract dispute and unauthorised disclosure and modification?	☐
A.14.1.3 Protecting Application Services Transactions – Do we ensure information involved in application service transactions is protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay?	☐
A.14.2 Security in Development and Support Processes	
A.14.2.1 Secure Development Policy – Are rules for the development of software and systems established and applied?	☐
A.14.2.2 System Change Control Procedures – Are changes to systems within the development lifecycle controlled by change control procedures?	☐
A.14.2.3 Technical Review of Applications after Operation Platform Changes – When operating platforms are changed are business critical applications reviewed and tested?	☐
A.14.2.4 Restrictions on Changes to Software Packages – Are modifications to software packages discouraged and all changes strictly controlled?	☐
A.14.2.5 Secure System Engineering Principles – Are principles for engineering secure systems documented, maintained and applied?	☐
A.14.2.6 Secure Development Environment – Do we appropriately protect secure development environments for system development and integration efforts?	☐
A.14.2.7 Outsourced Development – Do we supervise and monitor the activity of outsourced system development?	☐
A.14.2.8 System Security Testing – Do we test security functionality during development?	☐

A.14.2.9 System Acceptance Testing – Do we ensure acceptance testing programs are established for new information systems, upgrades and new versions?	☐
A.14.3 Test Data	
A.14.3.1 Protection of Test Data – Is test data selected carefully, protected and controlled?	☐
A.15 Supplier Relationships	
A.15.1 Information Security in Supplier Relationships	
A.15.1.1 Information Security Policy for Supplier Relationships – Are information security requirements for supplier's access to the organisation's assets agreed and documented?	☐
A.15.1.2 Addressing Security within Supplier Agreements – Have we ensured all relevant information security requirements are in place and agreed with each supplier that may access, process, store, communicate or provide IT infrastructure components for us?	☐
A.15.1.3 Information and Communication Technology Supply Chain – Do agreements with suppliers include requirements to address information security risks associated with services and product supply chain?	☐
A.15.2 Supplier Service Delivery Management	
A.15.2.1 Monitoring and Review of Supplier Services – Do we regularly monitor, review and audit supplier services?	☐
A.15.2.2 Managing Changes to Supplier Services – Are changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, management effectively?	☐
A.16 Information Security Incident Management	
A.16.1 Management of Information Security Incidents and Improvements	
A.16.1.1 Responsibilities and Procedures – Are responsibilities and procedures in place to ensure a quick, effective and orderly response to incidents?	☐
A.16.1.2 Reporting Information Security Events – Are events reported through appropriate management channels as quickly as possible?	☐
A.16.1.3 Reporting Information Security Weaknesses – Are workers using our systems and services required to note and report any observed or suspected information security weaknesses?	☐
A.16.1.4 Assessment of and Decision on Information Security Incidents – Are information security events assessed and a decision made as to whether they are classified as incidents?	☐
A.16.1.5 Response to Information Security Incidents – Are incidents responded to in accordance with the documented procedure?	☐
A.16.1.6 Learning from Information Security Incidents – Is knowledge gained from analysing and resolving incidents used to reduce the likelihood or impact of future incidents?	☐
A.16.1.7 Collection of Evidence – Have we implemented procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence?	☐

A.17 Information Security Aspects of Business Continuity	
A.17.1 Information Security Continuity	
A.17.1.1 Planning Information Security Continuity – Have we determined our requirements for information security and the continuity of information management in the event of a disaster or crisis?	☐
A.17.1.2 Implementing Information Security Continuity – Have we documented and established procedures and controls to ensure continuity for information security during a disaster or crisis?	☐
A.17.1.3 Verify, Review and Evaluate Information Security Continuity – Have we verified the information security continuity controls at regular intervals in order to ensure that they are effective?	☐
A.17.2 Redundancies	
A.17.2.1 Availability of Information Processing Facilities – Do we have sufficient redundancy to meet availability requirements?	☐
A.18 Compliance	
A.18.1 Compliance with Legal and Contractual Requirements	
A.18.1.1 Identification of Applicable Legislation and Contractual Requirements – Are all relevant legislative, regulatory, contractual requirements and our approach to meet these requirements documented and kept up to date?	☐
A.18.1.2 Intellectual Property Rights – Are procedures in place to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software?	☐
A.18.1.3 Protection of Records – Are records protected from loss, destruction, falsification, unauthorised access and unauthorised release?	☐
A.18.1.4 Privacy and Protection of Personally Identifiable Information – Do we ensure privacy and protection of personally identifiable information as required?	☐
A.18.1.5 Regulation of Cryptographic Controls – Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	☐
A.18.2 Information Security Reviews	
A.18.2.1 Independent Review of Information Security – Do we ensure our approach to managing information security (ie control objectives, controls, policies, processes and procedures) is reviewed independently at planned intervals or when significant change occurs?	☐
A.18.2.2 Compliance with Security Policies and Standards – Do our managers regularly review the compliance of information processing and procedures within their area of responsibility?	☐
A.18.2.3 Technical Compliance Review – Are systems regularly reviewed for compliance with our policies and standards?	☐