Price: AUD 35

Information Security Code: 2018

published by:

TQCS International Pty Ltd

Head Office: 117A Tapleys Hill Road
HENDON SA 5014 AUSTRALIA
ph: +61 8 8347 0603 fax: +61 8 8445 9423
email: info@tqcsi.com website: www.tqcsi.com

Preface

This **Information Security Code** was developed by TQCS International Pty Ltd (TQCSI). TQCSI is accredited by the Joint Accreditation System of Australia and New Zealand (JAS-ANZ) as a certification body for auditing and certifying organisation's management systems based on international standards.

This Code is intended to be used as a guide for organisations who are implementing a management system to address information security. The Code is not intended as a replacement for ISO 27001 (Information security management systems). Rather, it is based on that international standard and is designed to fill a void for those smaller organisations who wish to meet fundamental information security requirements but have no current requirement for certification to the international standard or who do not have the resources to implement a full Information Security Management System. However, as businesses grow or the demand increases, the Code is designed for the management system to be easily developed to meet the requirements of ISO 27001.

This **Information Security Code** has been specifically prepared for small business in response to a demand by government and major customers to maintain security of all information. Organisations who are certified against the **Information Security Code** can demonstrate to their customers an ability to identify, risk assess and manage information security under a management system which is audited and certified by an independent, third party certification body. Importantly, they also demonstrate the ability to reliably work with larger organisations who have achieved certification to ISO 27001. Appropriately certified organisations may exhibit the **TQCSI Information Security Code** certification mark.

The Code itself is represented by the bold type contained herein. To assist in its interpretation, explanations of the relevance of each clause have been included in italics.

Contents

1 Scope

This Information Security Code specifies management system requirements for use by organisations to provide objective evidence of their capability to manage information security. It aims to provide a framework for a reliable and practical management system, tailored for smaller businesses who supply larger organisations certified to ISO 27001 or businesses wishing to improve their own operations through the adoption of a management system.

The Code is aimed at achieving secure information in all mediums. It relies on management identifying and documenting its own processes, and encouraging continual improvement. Accordingly, organisations should document procedures to address each clause of this Code.

This Code also requires organisations to assess and treat information security risks that are relevant to their business through a Statement of Applicability.

2 References

This Code makes reference to ISO 27001, Information security management systems - Information technology – Security techniques - Information security management systems – Requirements.

3 Definitions

For the purposes of this Code, the following definitions apply:

- **Consequence: outcome of an occurrence effecting an objective**
- **Correction: action to eliminate a nonconformance**
- **Corrective action: action to eliminate the cause of a nonconformance and to prevent recurrence**
- **Information security: preservation of confidentiality, integrity and availability of information**
- **Interested party: person or organisation that can affect, be affected by or perceive themselves to be affected by a decision or activity**
- **Likelihood: chance of something happening**
- **Nonconformance: non-fulfilment of a requirement**
- **Objective: result to be achieved**
- **Organisation: company, business or whatever term is used the identify the organisation**
- **Procedure: a procedure, standard operating procedure (SOP), work instruction (WI) or other document used to direct employees in the conduct of an activity**
- **Risk: effect of uncertainty on objectives**

- **Risk treatment: process to modify risk**
- **Residual risk: risk remaining after risk treatment**
- **Senior Manager: owner or most senior manager in the business**
- **Target: one or more actions required to achieve an objective.**

4 Context of the Organisation

4.1 Issues and Interested Parties

The Organisation is to determine and understand external and internal issues, and those interested parties, that are relevant to the Organisation's information security.

Explanation: Management must be aware of those external issues and internal issues which are relevant to the organisation, and understand their impact on information security (eg relevant legislation, contracts, physical security, internet, software control, database management, etc). Similarly, management must be aware of any authority or other party which may have an interest in or an effect on the organisation's information security (eg major customers, competitors, employees, neighbouring businesses, internet service providers, dependencies with external organisations/providers, potential malicious threats etc).

These issues and interested parties need not necessarily be documented but management should be sufficiently aware of them to ensure they are considered during operational decision making.

4.2 Information Security Management System

The Organisation is to establish, implement, maintain and continually improve a documented Information Security Management System to meet the requirements of this Code.

Explanation: A manual or set of procedures is required describing how the organisation meets the requirements of each clause of this Code. It need not be a voluminous document but must describe the roles and responsibilities of management and employees, and how the various tasks required of this Code are to be undertaken. Once documented, the Information Security Management System must be implemented through training of employees and relevant record keeping.

Management systems do not stop once certification is achieved and, similarly, the Information Security Management System must be maintained so that it continually improves and security information objectives are achieved.

5 Leadership

5.1 Commitment

The Senior Manager and management team is to demonstrate leadership and commitment to information security by providing sufficient resources to ensure the Information Security Management System is effectively maintained.

Explanation: Senior management must ensure that sufficient resources are provided in terms of people, time and other resources to maintain an effective, active Information Security Management System.

5.2 Information Security Policy

The Senior Manager is to define the Organisation's commitment to information security in the form of an Information Security Policy, which is relevant to the Organisation's goals.

The Policy must be documented, available to the public upon request and understood by employees.

Explanation: The true concept of the Information Security Management System is that all important aspects of management control, which could affect information security and the Organisation's legal responsibilities in this area, should be documented and continually improve. Therefore, it is the responsibility of the Senior Manager to document a policy that can be interpreted by employees as the Organisation's formal commitment to the management system that has been developed.

The Policy should make reference to the Organisation's overall, aspirational objectives for information security. It should express commitment to compliance with legal and regulatory requirements, understanding of the needs and expectations of interested parties, and commitment to continual improvement. The Organisation should ensure that the Policy, once developed, is understood by all employees. The Policy should be available to the public through means such as tenders, websites and promotional literature.

5.3 Responsibility

The Senior Manager is to ensure that responsibilities relevant to information security are described and communicated, including responsibility for maintaining and reporting on the Information Security Management System.

Explanation: Management must ensure that the various roles and responsibilities relevant to information security are clearly assigned, communicated and understood. The effectiveness of the System should be monitored and communicated.

6 Planning

6.1 Risk Assessment

The Organisation is to assess the risk of information security to identify risks associated with the loss of confidentiality, integrity and availability of information. When assessing the risk, the Organisation is to assess the potential consequences that would result against the realistic likelihood of the occurrence of the risk without controls in place to determine the level of risk. Once assessed, the information security risks are to be prioritised for risk treatment.

The Organisation is to document the risk assessment process, including the information security risk criteria.

Explanation: The key stages in a typical risk assessment process are as follows:

1) *Risk identification (taking into account the scope, context and criteria)*
2) *Risk Analysis (eg understanding the likelihood (probability) of the risk event occurring and the impact (consequences) if it did).*
3) *Risk Evaluation - this involves identifying the potential to mitigate the risk. The main risk treatment options are:*
    a. *Avoid - don't do the activity that creates the risk.*
    b. *Take the risk - this generally applies to opportunities (ie positive outcomes).*
    c. *Remove the risk source - action to prevent the cause of the risk.*
    d. *Change the likelihood - action to reduce the chances of the risk occurring.*
    e. *Change the consequence - action to minimise the impact of the risk (or maximise it in the case of an opportunity or benefit – a positive risk)*
    f. *Share the risk (eg by insuring the risk or contracting to share or limit it).*
    g. *Retain the risk - if the probability and impact are considered tolerable, the organisation may choose to accept the risk.*
4) *Risk Treatment. Once the risks and treatment options are understood, a decision is required to select the preferred treatment option, and to plan and take appropriate action. These actions are generally called the risk controls. As with other actions, these should be recorded and monitored, and identify the action, owner, target and completion dates, and the current status.*

6.2 Risk Treatment

The Organisation is to apply an information security risk treatment process to determine the controls required.

Those controls are then to be compared with those at Annex A to verify that no necessary controls have been omitted.

The Organisation is to develop, regularly review and maintain a Statement of Applicability that contains the necessary controls and justification for exclusions of any controls listed at Annex A.

<u>Explanation</u>: Further to the explanation described above for Clause 6.1, many organisations use a simple matrix to assess, score and prioritise risk treatment, such as the example below:

LIKELIHOOD	CONSEQUENCE				
	MINOR	**SERIOUS**	**SEVERE**	**MAJOR**	**CATASTROPHIC**
ALMOST CERTAIN	Significant	High	Extreme	Extreme	Extreme
LIKELY	Moderate	Significant	High	Extreme	Extreme
POSSIBLE	Moderate	Moderate	Significant	High	Extreme
UNLIKELY	Low	Low	Moderate	Significant	High
RARE	Low	Low	Moderate	Moderate	Significant

This allows priority to be given to the biggest risks (ie those with the highest overall likelihood x consequence). The Organisation should then identify what to do for each risk band (eg Extreme, High, etc), working from the highest to the lowest in priority order.

Annex A provides a useful framework to identify objectives and capture targets and controls to mitigate a range of risks that are relevant to information security. This can be used as a guide to identify and control common risks, but it is important to review this to ensure the specific risks to the Organisation are captured, understood and that appropriate controls and actions are put in place.

6.3 Objectives and Targets

The Organisation is to establish and monitor information security objectives and targets to ensure continual improvement of the Information Security Management System. Objectives and targets are to be documented and periodically reviewed by management.

<u>Explanation</u>: In addition to any overall, aspirational objectives described in the Information Security Policy, the Organisation is to establish particular objectives and targets relevant to its organisational performance goals and targets. These objectives and targets may arise from planning or through the risk assessment process above. For example, an Organisation may aim to address all risks in the medium risk category or above, and to reduce the impact of higher risks to an acceptable level. This is sometimes referred to as risk appetite. Annex A provides a framework as a basis for identifying objectives, targets and controls for information security.

Action taken is to be recorded and the objectives and targets are to be regularly reviewed (six monthly intervals as a minimum) to ensure performance progress.

The objectives and targets are to be recorded in some form of plan, which is to be retained on

file to verify continual improvement. This plan is often called an Improvement Plan or Management Plan.

Principal contractors may require this for a specific contract. Essentially, this requirement can be met by the business demonstrating that they have risk assessed processes relevant to the project or activity (Clause 6.1), that appropriate controls have been implemented (Clause 6.2), and that objectives and targets for improvement have been established (Clause 6.3).

7 Support

7.1 Competence and Awareness

The Organisation is to ensure employees are appropriately trained and have been deemed competent to perform their work which affects information security. Competence is to be assessed based on appropriate education, training or experience.

Documentation regarding competence is to be available to managers and supervisors who need to allocate tasks to respective employees. Records are to be retained as evidence of education and training, where relevant.

Employees are to be aware of the Information Security Management System and their specific information security requirements through an induction process or awareness program.

Explanation: All employees must be adequately qualified and competent to perform the function for which they are employed and their responsibilities to report information security issues. To enable this to be identified and planned, it is necessary to identify what skills are required in the business and provide training, where required.

Records are to be retained of qualifications (licences, etc) and training conducted by employees since joining the business.

Induction training for new employees is to be documented to ensure that employees have been trained in areas such as the appropriate use of organisation IT systems and procedures in order to maintain information security. Similar induction training is to be provided to sub-contractors, where appropriate.

7.2 Document Control

Documented policies, procedures and forms required by the Information Security Management System are to be appropriately controlled such that the status of documents is readily identifiable. Documents are to be appropriately approved and available for use by respective employees.

Documents from external authorities are to be identified and controlled.

Explanation: Maintaining appropriate documents relevant to the running of a business is good management practice that should be encouraged. Moreover, third party certification will be

based on documentary evidence verifying that the management system is being followed.

In order to ensure employees are using and responding to current documentation, it is necessary to record the existence of all controlled documentation, together with the relevant issue status. It, therefore, becomes a responsibility to ensure that all controlled documents are maintained current.

To ensure that procedures represent the existing method of operation, it is also necessary to provide a method of amendment to existing procedures.

As companies move to computerised documentation, the same philosophy must apply to ensure only the current, approved methods of conducting business is interpreted by employees.

The Senior Manager is to ensure that only authorised personnel can access information and that controlled access is appropriate to the nature of the information (ie its commercial or personal sensitivity for data such as HR records or commercial contracts).

7.3 Records

Records are to be retained to demonstrate the requirements of the Information Security Management System have been met.

Records are to be retained for sufficient time to ensure an appropriate investigation of information security issues can be undertaken.

Explanation: Records must be retained in an orderly and controlled fashion to prove the system is operating in accordance with the developed procedures and other instructions. This proof may be required by auditors to ensure that processes have been carried out as planned or, alternatively, may be a means of identification and traceability. It is, therefore, necessary to maintain records in a clear, concise and easy to use manner.

Records are to be retained on file or in archive for as long as they may be required. Legislation often governs the retention period for financial records but the retention period for other records is largely a decision for management.

In relation to information security management, one of the primary requirements is to demonstrate adequate control over access to the Organisation's systems and information, both by staff and any external bodies, and that information and access is adequately protected and maintained. This covers, both, electronic and physical access and security thereof.

8 Operation

8.1 Operational Planning

The Organisation is to ensure the controls listed in the Statement of Applicability and information security objectives are planned and implemented.

The Organisation is to ensure that outsourced processes are determined and controlled.

Explanation: Changes and improvements to the Information Security Management System need to be carefully planned and implemented to ensure adequate control throughout the change process. This includes ensuring adequate access control to data and equipment (both physical and electronic).

Day-to-day control also needs to be maintained to address business needs and mitigate against identified risks; eg by monitoring malware and installing required security upgrades and patches to ensure operational security. Routine access control will include adding and deleting user access and ensuring sufficient segregation of sensitive data access.

The supply chain also represents an information security risk, and the Organisation should ensure that any outsourced activities and external purchases comply with the Organisation's requirements, legislative standards and accepted good practice.

Planning also includes planning for emergency incidents, so that an effective response can be mobilised; eg if the Information Security Management System is compromised or access is lost, to enable sufficient business continuity.

8.2 Risk Review

The Organisation is to review information security risk assessments at planned intervals or when significate changes occur. The Organisation is also to implement the information security risk treatment plan.

The Organisation is to retain records of the results of risk assessment and risk treatment.

Explanation: See Section 6 for further details; the main feature of effective risk management is that risks are identified and actively managed. Normally, the Risk Register is maintained as a live document, so that information is current and reflects the changing nature of risks in a dynamic environment. It is usually evident if a Risk Register is used, maintained and shows recent updates. Periodic formal reviews of the overall effectiveness of the risk management system are normally planned to suit the nature and level of the risks to the business.

9 Performance Evaluation

9.1 Monitoring and Evaluation

The Organisation is to evaluate the effectiveness of the Information Security Management System. In doing so, the Organisation is to determine what needs to be monitored, how it will be monitored, when it will be monitored, who will monitor it and who will evaluate the results of the monitoring. Records of monitoring and evaluation are to be retained.

Explanation: Ongoing management and more formal periodic review is required in order to monitor the effectiveness of the overall system and key elements. This normally requires the Organisation to identify key measures of effectiveness and to put in place the mechanisms to track, report and review performance.

This should include compliance with, both, Organisation and legislative standards, and the tracking of nonconformances.

9.2 Internal Audit

The Organisation is to undertake regular internal audits of the Information Security Management System to ensure continued compliance. Internal audits are to be conducted on all sections of the Information Security Management System at least once each calendar year.

Records of internal audits are to be retained.

Explanation: Internal audits of the management system documentation relevant to the Information Security Management System must be conducted by the Organisation, at least annually or as determined by the nature and criticality of the risks to the business. Internal audits may be split into two or more audits completed throughout the year. Work sheets or checklists must record objective evidence of audit findings which should then be used to document corrections taken.

Operational procedures should also be audited or reviewed to ensure they still reflect the required process. These reviews should be conducted based on the risk of the process; some may be required six monthly or annually, others of lesser risk may only need to be reviewed 2, 3 or even 5 yearly.

Internal audit worksheets or checklists are to be retained as records to confirm that internal audits have been conducted. Similarly, a means of proving that a procedure has been reviewed must also be retained or recorded.

Appropriate trained employees are to conduct internal audits. Alternatively, a contracted auditor may be used in lieu.

10 Improvement

10.1 Nonconformances

The Organisation is to ensure information security related nonconformances are identified and appropriate immediate action taken. Records are to be maintained accordingly.

Explanation: When things go wrong, it is important to ensure immediate action is taken to resolve the issue. Procedures must be documented to allow employees to bring these issues to the attention of management without fear of retribution.

Similarly, the system must ensure employees are able to report information security issues to management in a timely manner.

Nonconformances result from many aspects of business, including customer complaints (internal and external), information from suppliers, product or service failure during operations, final product or service delivery and information security incidents and near misses. They may also be suggestions for improvement made by employees or customers.

Nonconformances occur in every business and the function of a management system, through continual improvement, is to reduce their frequency and impact. This is achieved by identifying responsibility for actions regarding nonconformances and documenting what immediate action is required.

10.2 Corrective Action

Where management considers nonconformances to be significant or repetitive, an investigation is to be conducted to identify the root cause of the issue and appropriate corrective action taken to reduce the likelihood of the issue occurring again. The investigation and results of corrective action are to be documented.

Explanation: At the core of any management system is the continual improvement process. Following the identification of significant nonconformances or repeating (trending) nonconformances identified, it is essential to conduct an analysis of those nonconformances to identify the action required to enable continual improvement and prevent a recurrence. This action is called 'corrective action' and requires a determination of the root cause of the problem and action taken to address the root cause. Sufficient evidence of corrective action must be retained to prove the continual improvement process is working.

Similarly, if an information security impact is identified or an incident or near miss occurs, the business must investigate the root cause of the impact in order to prevent recurrence.

Preventive action referred to in international standards is merely identifying a 'potential' issue and taking action to prevent its impact on the business. The same corrective action process may apply to preventive action.

Annex A

Reference Control Objectives and Controls

1	**Information Security Policies**
1.1	**Management direction for information security**
Objective	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
Target	Policies for information security, review of policies.
Example Controls	Documented policies for information security, communicated to employees etc. Periodic review of policies to ensure they are suitable, adequate and effective.
2	**Organisation of information security**
2.1	**Internal organisation**
Objective	To establish a management framework to initiate and control the implementation and operation of information security within the organisation.
Target	Roles and responsibilities, segregation of duties, contact with authorities and special interest groups, information security in project management.
Example Controls	Defined and allocated information security roles. Segregation of access and duties to prevent accidental or deliberate access misuse. Proper control of projects. Communication and reporting to relevant internal and external parties.
2.2	**Mobile devices and teleworking**
Objective	To ensure the security of teleworking and use of mobile devices.
Target	Mobile device policy, teleworking
Example controls	Policy and supporting security measures to control the risks from using mobile devices and information accessed, processed or stored at teleworking sites.
3	**Human Resource Security**
3.1	**Prior to employment**
Objective	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.
Target	Screening, terms and conditions of employment.
Example controls	Appropriate background checks on candidate employees, with commensurate access levels. Contract conditions to include responsibilities for information security.
3.2	**During employment**
Objective	To ensure that employees and contractors are aware of and fulfil their information security responsibilities.
Target	Management responsibilities, information security awareness, education and training, disciplinary process.
Target Controls	All employees and relevant contractors to receive awareness education and training and updates on policies and procedures relevant to their role. Management must oversee compliance and use a formal, documented, disciplinary process for breaches.
3.3	**Termination and change of employment**
Objective	To protect the organisation's interests as part of the process of changing or terminating employment.
Target	Termination or change of employment responsibilities.
Example controls	Document and follow the procedure to add, remove or amend access if an employee starts, leaves or changes role.
4	**Asset Management**
4.1	**Responsibility for assets**
Objective	To identify organisational assets and define appropriate protection responsibilities.

Target	Inventory of assets, ownership of assets, acceptable use of assets, return of assets.
Example Controls	Maintain and inventory of Information processing assets, with ownership. Document and track the acceptable use of assets, and retain them when people leave.
4.2	**Information classification**
Objective	To ensure that information receives an appropriate level of protection in accordance with its importance to the organisation.
Target	Classification of information, labelling of information, handling of assets.
Example controls	Identify key information assets with legal, critical, sensitive or high value significance. Procedurise labelling and control of them appropriately based on their classification.
4.3	**Media handling**
Objective	To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.
Target	Management of removable media, disposal of media, physical media transfer.
Example controls	Implement a procedure for controlling removable media, including transport and secure disposal when obsolete, to prevent unauthorised access, misuse or corruption.
5	**Access Control**
5.1	**Business requirements of access control**
Objective	To limit access to information and information processing facilities.
Target	Access control policy, access to networks and network services.
Example controls	Document, implement and monitor the access control policy, so that users only have access to services and areas they are authorised to use.
5.2	**User access management**
Objective	To ensure authorised user access and to prevent unauthorised access to systems and services.
Target	User registration and de-registration, user access provisioning, management of privileged access rights, management of secret authentication information of users, review of user access rights, removal or adjustment of rights.
Example controls	Implement a formal registration and de-registration process for user access rights. Control and restrict access to providing user rights and user authentication (passwords etc.) Asset owners should periodically review access, and access removed on leaving.
5.3	**User responsibilities**
Objective	To make users accountable for safeguarding their authentication information.
Target	Use of secret authentication information.
Example controls	Define and implement a policy on the use of secret authentication information (covering the use and control of secure passwords etc.)
5.4	**System and application access control**
Objective	To prevent unauthorized access to systems and applications.
Target	Information access restriction, secure logon procedures, password management system, use of privileged utility programs, access control to program source code.
Example controls	Restrict access based on the access control policy above. Use a secure log-on process for access to sensitive information. Implement a password management system that requires secure passwords. Restrict access to software that can override controls.
6	**Cryptography**
6.1	**Cryptographic controls**
Objective	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
Target	Policy on the use of cryptographic controls, key management.
Example controls	Include cryptographic controls in the IT use policy, covering their use, protection and lifetime, and implement it.

7	**Physical and environmental security**
7.1	**Secure areas**
Objective	To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.
Target	Physical security perimeter, physical entry controls, securing offices, rooms and facilities, protecting against external and environmental threats, working in secure areas, delivery and loading areas.
Example controls	Ensure secure perimeters prevent access to sensitive data and facilities, with access control preventing unauthorised access to offices, rooms and facilities. Take reasonable steps to protect from natural disasters, malicious attack and accidents. Where possible, isolate information processing areas from public areas or areas where unauthorised access could occur (eg delivery and loading areas).
7.2	**Equipment**
Objective	To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.
Target	Equipment siting and protection, supporting utilities, cabling security, equipment maintenance, removal of assets, security of equipment and assets off-premises, secure disposal or re-use of equipment, unattended user equipment, clear desk and clear screen policy.
Example controls	Site and protect equipment to prevent damage and unauthorised access. Provide protection for power or utility failure, and cable protection to prevent interception or damage if necessary. Maintain equipment adequately, apply adequate control to assets taken off-site or unattended, including wiping/secure disposal of obsolete storage media. Implement a clear desk policy for paperwork and a clear screen, clear removable media policy IT assets.
8	**Operations security**
8.1	**Operational procedures and responsibilities**
Objective	To ensure correct and secure operations of information processing facilities.
Target	Documented operating procedures, change management, capacity management, separation of development, testing and operational environments.
Example controls	Document the operating procedures, including in secure areas. Control changes to areas affecting information security (eg organisational, processes, IT systems). Ensure adequate resources. Separate development and testing from operational environments and fully test before deployment.
8.2	**Protection from malware**
Objective	To ensure that information and information processing facilities are protected against malware.
Target	Controls against malware.
Example controls	Implement controls to detect, prevent and recover from malware, with user training and awareness (eg education in phishing attacks).
8.3	**Backup**
Objective	To protect against loss of data.
Target	Information backup.
Example controls	Regular backup and testing of information, software and system images in line with a policy.
8.4	**Logging and monitoring**
Objective	To record events and generate evidence.
Target	Event logging, protection of log information, administrator and operator logs, clock synchronisation.
Example	Maintain and prevent unauthorised access to, and review event logs of user activity,

controls	exceptions, faults and security events. Synchronise system clocks.
8.5	**Control of operational software**
Objective	To ensure the integrity of operational systems.
Target	Installation of software on operational systems.
Example controls	Implement a procedure to control access to install software.
8.6	**Technical vulnerability management**
Objective	To prevent exploitation of technical vulnerabilities.
Target	Management of technical vulnerabilities, restrictions on software installation.
Example controls	Assess technical vulnerabilities regularly, assess risks and take action (eg timely updates to AV software and deployment software and system upgrades and patches, replacement of obsolete or unsupported applications and hardware).
8.7	**Information systems audit considerations**
Objective	To minimise the impact of audit activities on operational systems.
Target	Information systems audit controls.
Example controls	Schedule periodic audits to avoid undue impact on operations.
9	**Communications Security**
9.1	**Network security management**
Objective	To ensure the protection of information in networks and its supporting information processing facilities.
Target	Network controls, security of network controls, segregation in networks.
Example controls	Manage and control networks to protect the ISMS, with appropriate security, support contracts, or service level agreements if in-house. Segregate networks if necessary.
9.2	**Information transfer**
Objective	To maintain the security of information transferred within an organisation and with any external entity.
Target	Information transfer policies and procedures, electronic messaging, confidentiality or non-disclosure agreements.
Example controls	Document and adopt suitable protocols for external information transfer of all types, and protect sensitive information in electronic messaging. Use confidentiality agreements, where necessary.
10	**System acquisition, development and maintenance**
10.1	**Security requirements of information systems**
Objective	To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.
Target	Information security requirements analysis and specification, securing application services on public networks, protecting application services transactions.
Example controls	Consider and include information security requirements (including wider transmission and access security requirements) for any system upgrades or changes.
10.2	**Security in development and support processes**
Objective	To ensure that information security is designed and implemented within the development lifecycle of information systems.
Target	Secure development policy, system change control procedures, technical review of applications after operating platform changes, restrictions on changes to software packages, secure system engineering principles, secure development environment, outsourced development, system security testing, system acceptance testing.
Example controls	Document formal controls for creation and changes to software and hardware, test before deployment to prevent business disruption. Coordinate and minimise change where possible. Utilise structured systems approaches and UAT protocols.

10.3	**Test data**
Objective	Protection of test data. Test data shall be selected.
Target	Protection of test data.
Example controls	Carefully select and control test data.
11	**Supplier security**
11.1	**Information security in supplier relationships**
Objective	To ensure protection of the organisation's assets that is accessible by suppliers.
Target	Information security policy for supplier relationships, addressing security within supplier agreements, information and communication technology supply chain.
Example controls	Identify and document all information security requirements associated with external suppliers or users (eg procedures to access, process, store and communicate data, or provision of components & software).
11.2	**Supplier service delivery management**
Objective	To maintain an agreed level of information security and service delivery in line with supplier agreements.
Target	Monitor and review of supplier services, managing changes to supplier services.
Example controls	Monitor, review and audit suppliers, and manage changes carefully based on risk.
12	**Information security incident management**
12.1	**Management of information security incidents and improvements**
Objective	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.
Target	Responsibilities and procedures, reporting information security events, reporting information security weaknesses, assessment of and decision on information security events, response to information security incidents, learning from information security incidents, collection of evidence.
Example controls	Document responsibilities and procedures to ensure effective responses to security incidents, including rapid reporting of observed or suspected issues or weaknesses. Classify events, and respond accordingly, including capturing evidence. Analyse and learn from events and patterns to prevent recurrence.
13	**Information security aspects of business continuity management**
13.1	**Information security continuity**
Objective	Information security continuity shall be embedded in the organisation's business continuity management systems.
Target	Planning information security continuity, implementing information security continuity, verify, review and evaluate information security continuity.
Example controls	Identify the organisations information access needs in emergency situations, and take steps to ensure the required level of access during and after incidents. Test arrangements to check they are effective and suitable.
13.2	**Redundancies**
Objective	To ensure availability of information processing facilities.
Target	Availability of information processing facilities.
Example controls	Ensure sufficient system redundancy and backup to meet business needs.
14	**Compliance**
14.1	**Compliance with legal and contractual requirements**
Objective	To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.
Target	Identification of applicable legislation and contractual requirements, intellectual

	property rights, protection of records, privacy and protection of personally identifiable information, regulation of cryptographic controls.
Example controls	Identify, document and update legal, regulatory, contractual and organisational requirements for information security (including IPR and software licences etc.). Implement procedures and controls to maintain compliance. Protect records from damage, falsification, loss and unauthorised access or release. Protect personal information and privacy in line with legislative and other requirements. Use cryptographic protection as required.
14.2	**Information security reviews**
Objective	To ensure that information security is implemented and operated in accordance with the organisational policies and procedures.
Target	Independent review of information security, compliance with security policies and standards, technical compliance review.
Example controls	Independently review the organisation's information security periodically or when significant changes occur. Managers should routinely monitor and enforce compliance, and technical compliance checks should be carried out.