ISO 27001:2022

Information Security, Cybersecurity, and Privacy Protection

kiwa | Compass Assurance Services

Self Assessment Checklist

Context

The Organisation

□ Have we determined internal and external issues that will impact on our information security management system?

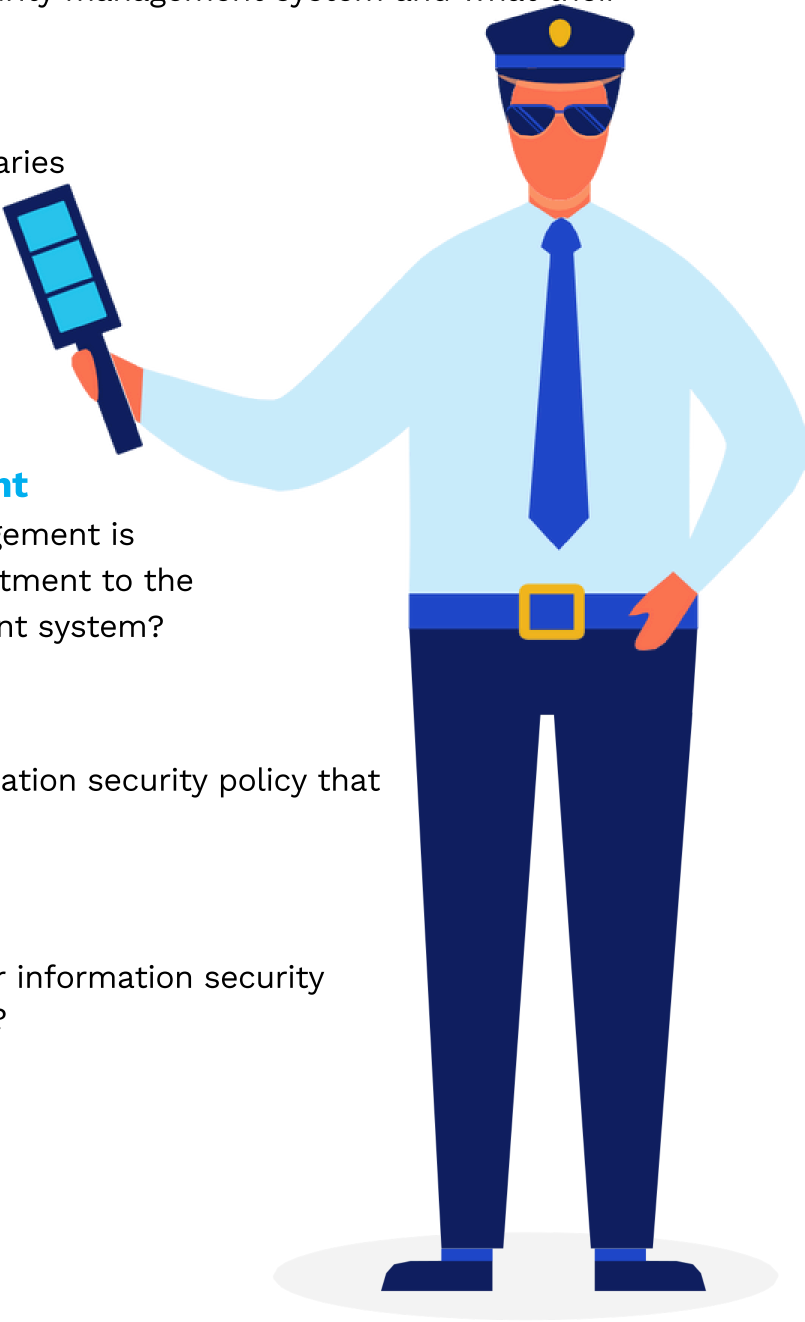
□ Have we determined which stakeholder requirements are addressed through the information security management system?

Interested Parties

□ Have we determined what internal and external interested parties are relevant to the information security management system and what their requirements are?

Scope

□ Have we determined the boundaries of the information security management system and documented the scope?



Leadership

Leadership and Commitment

□ Can we demonstrate top management is providing leadership and commitment to the information security management system?

Information Security Policy

□ Have we documented an information security policy that is communicated and available?

Roles and Responsibilities

□ Are roles and responsibilities for information security communicated and understood?

Planning

Risks and Opportunities

□ Have we determined the information security risks and opportunities related to our organisation?

□ Have we implemented a documented information security risk assessment process?

Statement of Applicability

□ Have we documented a risk treatment plan and Statement of Applicability with regard to controls?

Information Security Objectives

□ Have we established information security objectives?

□ Are our information security objectives available as documented information

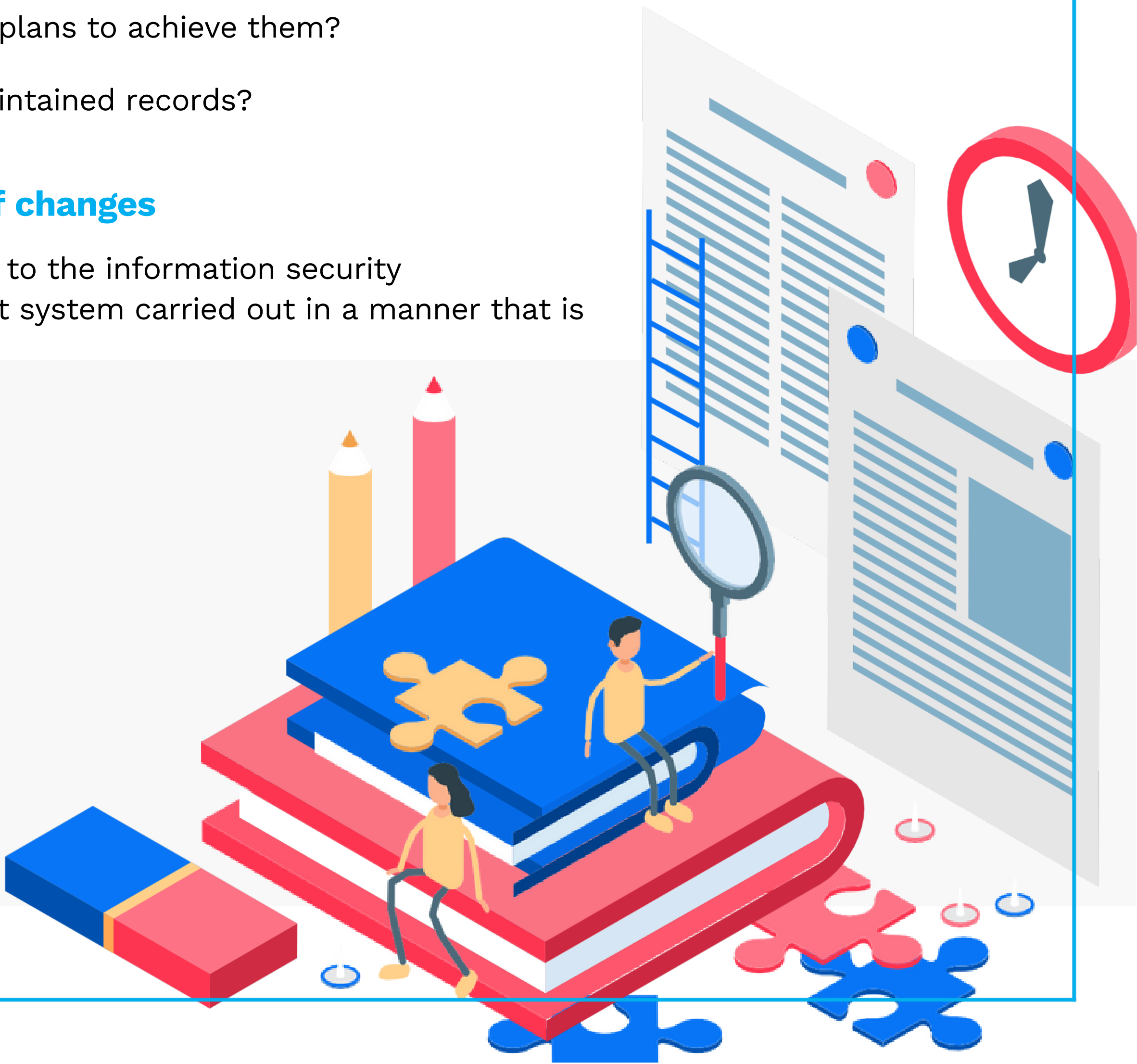
□ Do we monitor, measure, and communicate them?

□ Do we have plans to achieve them?

□ Have we maintained records?

Planning of changes

□ Are changes to the information security management system carried out in a manner that is planned?



Support

Resources

□ Have we determined and ensured necessary resources are in place for the information security management system?

Competence

□ Do we ensure competence of personnel?

□ Do we maintain records?

Awareness

□ Have we ensured that personnel are aware of our policy, relevant objectives, and their responsibilities?

Communication

□ Have we determined processes for internal and external communication relevant to information security?

Control of Documents

□ Do we ensure documents and records are controlled?

Operations

Operational Planning and Control

□ Have we established and maintained procedures to meet the requirements of the information security management system?

□ Have we established criteria for processes, and do we maintain control of the processes in accordance with these criteria?

Risk Assessment

□ Do we assess risk at planned intervals and when significant changes occur, and do we maintain records?

Risk Treatment

□ Have we implemented risk treatment plans, and do we maintain records?

Performance Evaluation

Monitoring & Measurement

□ Do we monitor things such as processes, operational controls, access, usage, change?

□ Do we measure things such as KPIs, performance against targets?

□ Do we analyse this information and maintain records?

Internal Audit

□ Do we plan and conduct internal audits to ensure the information security system conforms to requirements and is implemented effectively?

□ Do we maintain records?

Management Review

□ Does our top management review our information security management system at planned intervals?

□ Do we maintain records?

□ Do we include decisions relating to continual improvement and any need for changes in the documented results of the management reviews?

Improvement

Continual Improvement

□ Do we continually improve the information security management system?

Nonconformity and Corrective Action

□ Do we take control of, correct and deal with the consequences of nonconformities raised?

□ Do we review and determine the root cause of the nonconformity?

□ Do we review the effectiveness of corrective action taken and use this knowledge to make changes or improvements to the information security management system?

□ Do we maintain records?

ANNEX A

5 Organisational Controls

5.1 Policies for information security	A set of information security policies relevant to interested parties
5.2 Information security roles and responsibilities	Defining and allocating roles and responsibilities within the information security management system as appropriate and in accordance with organisational needs
5.3 Segregation of duties	Conflicting duties and areas of responsibility are handled separately from each other
5.4 Management responsibilities	Management ensures all personnel are applying information security in accordance with the established policies and procedures of the organisation
5.5 Contact with authorities	Contact with relevant authorities is established and maintained by the organisation
5.6 Contact with special interest groups	Contact with special interest groups, specialist security forums and/or professional associations is established and maintained by the organisation
5.7 Threat intelligence	The organisation collects and analyses information relating to information security threats
5.8 Information security in project management	Information security is integrated into management of projects
5.9 Inventory of information and other associated assets	Development and maintenance of an inventory of information and other associated assets, including owners
5.10 Acceptable use of information and other associated assets	Defined, documented, and implemented rules for the acceptable use and procedures for handling information and other associated assets
5.11 Return of assets	Assets belonging to the organisation in the possession of personnel and other interested parties are returned to the organisation upon change to or termination of their employment, contract, or agreement
5.12 Classification of information	Information is classified based on confidentiality, integrity, availability, and relevant interested party requirements
5.13 Labelling of information	A set of defined, documented, and implemented procedures for labeling of information aligned with the information classification scheme
5.14 Information transfer	Defined and implemented rules, procedures, or agreements for all types of transfer facilities within the organisation as well as between the organisation and other parties
5.15 Access control	Defined and documented rules to control physical and logical access to information

5.16 Identity management	Management of identities for their full life cycle
5.17 Authentication information	Allocation and management of authentication information, such as usernames and passwords, is controlled by a management process that includes advising personnel on appropriate handling of authentication information
5.18 Access rights	Provisioning, reviewing, and monitoring of access rights to information and other assets in accordance with the relevant policy and rules for access control
5.19 Information security in supplier relationships	Defined and implemented processes and procedures for managing information security risks associated with the use of supplier products or services
5.20 Addressing information security within supplier agreements	Establishing and agreeing upon information security requirements in supplier relationships
5.21 Managing information security in the information and communication technology (ICT) supply chain	Defined and implemented processes and procedures to manage information security risks associated with ICT products and services supply chain
5.22 Monitoring, review and change management of supplier services	Regular monitoring, review, and evaluation of changes in supplier information security practice
5.23 Information security for use of cloud services	Establishing processes for the acquisition, use, management, and exit from cloud services in accordance with the organisational information security requirements
5.24 Information security incident management planning and preparation	Defined, implemented, and communicated processes as well as roles and responsibilities for management of an information security incident
5.25 Assessment and decision on information security events	Assessing information security events to determine if they are to be categorised as information security incidents
5.26 Response to information security incidents	Documented and implemented procedures on appropriate response to information security incidents
5.27 Learning from information security incidents	Strengthening and improving controls based on knowledge gained from information security incidents
5.28 Collection of evidence	Establishing and implementing procedures for identification, collection, acquisition, and preservation of evidence relating to information security events
5.29 Information security during disruption	Developing a plan to maintain information security at an appropriate level during disruption
5.30 ICT readiness for business continuity	Implementing processes so the organisation can continue operations as usual in case of a disruption that affects ICT

5.32 Intellectual property rights	Identifying, documenting and keeping up to date with legal, statutory, regulatory and contractual requirements relevant to information security
5.32 Intellectual property rights	Implementing appropriate procedures to protect intellectual property rights
5.33 Protection of records	Storing records such that they are protected from loss, destruction, falsification, unauthorised access, and unauthorised release
5.34 Privacy and protection of personal identifiable information (PII)	Identifying and meeting relevant requirements regarding preservation of privacy and protection of PII
5.35 Independent review of information security	Independent reviews at planned intervals, or when significant changes occur, of the organisational approach to managing information security and its implementation including people, processes, and technologies
5.36 Compliance with policies, rules, and standards for information security	Regularly reviewing organisational compliance with its information security policy and topic-specific policies, rules, and standards
5.37 Documented operating procedures	Documented procedures for information processing facilities
6 People Controls	
6.1 Screening	Conducting background checks on all candidates prior to joining the organisation as well as on an ongoing basis
6.2 Terms and conditions of employment	Documenting both personnel and organisational responsibilities for information security in employment contractual agreements
6.3 Information security awareness, education, and training	Regularly providing personnel of the organisation and other relevant interested parties appropriate information security awareness, education, and training as well as updates of the organisation's information security policy, topic-specific policies, and procedures as appropriate to their job
6.4 Disciplinary process	Formalising and communicating a process to take actions against personnel and other relevant interested parties who violate information security policies
6.5 Responsibilities after termination or change of employment	Defining, enforcing, and communicating to relevant personnel and interested parties the responsibilities and duties that remain after termination or change of employment
6.6 Confidentiality or non-disclosure agreements	Documenting and regularly reviewing confidentiality or non-disclosure agreements signed by personnel and other relevant parties as per organisational needs

6.7 Remote working	Implementing security measures when personnel are working remotely such that information accessed, processed, or stored outside the organisation’s premises is protected
6.8 Information security event reporting	Providing a method by which personnel can report observed or suspected information security events through appropriate channels and in a timely manner
7 Physical Controls	
7.1 Physical security perimeters	Defining security perimeters to protect areas that contain information and other associated assets
7.2 Physical entry	Protecting secure areas with appropriate entry controls and access points
7.3 Securing offices, rooms, and facilities	Designing and implementing physical security for offices, rooms, and facilities
7.4 Physical security monitoring	Continuous monitoring of premises for unauthorised physical access
7.5 Protecting against physical and environmental threats	Designing and implementing infrastructure to protect against physical and environmental threats such as natural disasters
7.6 Working in secure areas	Designing and implementing security measures for working in secure areas
7.7 Clear desk and clear screen	Defining and enforcing clear desk rules for papers and removable storage, as well as clear screen rules for information processing facilities
7.8 Equipment siting and protection	Securely siting and protecting equipment
7.9 Security of assets off-premises	Protecting assets that are stored off-site
7.10 Storage media	Managing storage media through their life cycle of acquisition, use, transportation, and disposal in accordance with the organisation’s classification scheme and handling requirements
7.11 Supporting utilities	Protecting information processing facilities from power failures and other disruptions
7.12 Cabling security	Protecting cables carrying power, data, or supporting information services from interception, interference, or damage
7.13 Equipment maintenance	Maintaining equipment correctly to ensure the availability, integrity, and confidentiality of information
7.14 Secure disposal or re-use of equipment	Verifying items of equipment containing storage media to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use

8 Technological Controls	
8.1 User end point devices	Protecting information stored on, processed by, or accessible via user end point devices
8.2 Privileged access rights	Restricting and managing the use or privileged access rights
8.3 Information access restriction	Restricting access to information and other associated assets in accordance with the organisation's access control policy
8.4 Access to source code	Managing read and write access to source code, development tools and software libraries
8.5 Secure authentication	Implementing secure authentication technologies and procedures based on access restrictions and the organisation's access control policy
8.6 Capacity management	Monitoring and adjusting the use of resources in line with current and expected capacity requirements
8.7 Protection against malware	Implementing malware protection supported by user awareness
8.8 Management of technical vulnerabilities	Obtaining information about technical vulnerabilities, evaluating the organisation's exposure to such vulnerabilities, and taking appropriate measures
8.9 Configuration management	Establishing, documenting, implementing, monitoring, and reviewing configurations including security configurations of hardware, software, services, and networks
8.10 Information deletion	Deleting information stored in information systems, devices, or other storage media when the information is no longer required
8.11 Data masking	Masking data as appropriate and in accordance with the organisation's access control policy and other relevant legislation
8.12 Data leakage prevention	Applying measures to systems, networks, and any other devices that process, store, or transmit sensitive data to prevent leakage of data
8.13 Information backup	Maintaining backup copies of information, software, and systems
8.14 Redundancy of information processing facilities	Implementing sufficient redundancy in information processing systems to meet availability requirements
8.15 Logging	Producing, storing, protecting, and analysing logs that record activities, exceptions, faults, and other relevant events
8.16 Monitoring activities	Monitoring networks, systems, and applications for unusual behaviour and taking appropriate actions to evaluate potential for information security events

8.17 Clock synchronisation	Synchronising clocks of information processing systems to approve time sources
8.18 Use of privileged utility programs	Restricting the use of utility programs that can override system and application controls
8.19 Installation of software on operational systems	Implementing procedures to securely manage installation of software on operational systems
8.20 Networks security	Securing, managing, and controlling networks and network devices to protect information in systems and applications
8.21 Security of network services	Implementing and monitoring security mechanisms, service levels, and service requirements of network services
8.22 Segregation of networks	Segregating groups of information services, users, and information systems in the organisation’s networks
8.23 Web filtering	Managing access to external websites to reduce exposure to malicious content
8.24 Use of cryptography	Defining and implementing rules for effective use of cryptography, including cryptographic key management
8.25 Secure development life cycle	Establishing and applying rules for the secure development of software and systems
8.26 Application security requirements	Managing access to external websites to reduce exposure to malicious content
8.27 Secure system architecture and engineering principles	Establishing, documenting, maintaining, and applying principles for engineering secure systems to all information system development activities
8.28 Secure coding	Applying secure coding principles to software development
8.29 Security testing in development and acceptance	Defining and implementing processes for security testing within the development life cycle
8.30 Outsourced development	Monitoring and reviewing development activities that have been outsourced
8.31 Separation of development, test, and production environments	Secure, separate environments for development, testing, and production
8.32 Change management	Procedures implemented to manage changes to information processing facilities and information systems
8.33 Test information	Appropriate selection, protection, and management of information used for testing
8.34 Protection of information systems during audit testing	Planning and appropriately managing audit tests and other assurance activities of operational systems

So What Now?

Contact us for a quick quote to get a better idea of costs and timings. Visit our website:

www.cas.com.au