# NSAI - ISO/IEC 27001:2022 Readiness Questionnaire

Disclaimer: This readiness questionnaire is intended as an aid to the implementing an Information Security Management System (ISMS) and a pathway to certification. Getting a "Likely High" score and level of readiness DOES NOT guarantee that your ISMS will be certified. Certification requires initial certification audits for new applicants or a transition audit for clients currently certified to I.S EN ISO/IEC 27001:2017 by qualified ISMS auditor who will evaluate your ISMS and its implementation against the requirements of the standard.

**Please see the NSAI website for information on "How Do I Get Certified?"**

## Introduction

This document has been designed to assess your company's readiness for an **ISO/IEC 27001:2022** Information Security Management System certification assessment. By completing this questionnaire your results will allow you to self-assess your organization and identify where you are in the process in relation to the main requirements of the standard.

The "**ISO IEC 27001 2022 clauses**" sheet presents the list of clauses of the standard.

The "**ISO IEC 27001 2022 controls**" sheet presents a list of the controls in support of clause 6.1.3 of the standard

The "**Clauses Questionnaire**" sheet presents a mapping of The clauses with questions designed to assess the readiness of organisations with regards to **ISO/IEC 27001:2022** certification

The "**Controls Questionnaire**" sheet presents a mapping of The controls supporting clause **6.1.3** with questions designed to assess the readiness of organisations with regards to **ISO/IEC 27001:2022** certification

The "**Results**" sheet presents the readiness score and level of the organisation, graphic visuals of the score per clause and control and general recommendations to improve the organisation's posture with regards to **ISO/IEC 27001:2022** certification

## How it works?

**1.** Answer the question in the question by selecting the options **"Yes"**, "**No**", "**N/A**" from the dropdown of each "**Answers**" cell in the "**Clauses Questionnaire**" and "**Controls Questionnaire**" sheets

**2.** The answers are as follows:
**Yes**: Requirement fulfilled
**No**: Requirement not fulfilled
**N/A**: Not required for the organisation's operations. Please provide a justification for each N/A answer in the rationale column.

**3.** Check the results and recommendations from the "**Results**" sheet

**The results are calculated based on the following formula**
**q=y/(v-z)×4**
Where; **q** = total of score in each domain; **y** = total of answer "**Yes**"; **v** = total of question (S1, S2, S3…); **z** = total of answer "**N/A**"; **4** = consists of 4 types **readiness level**;

**4.** For more information on the recommendations check out the detailed requirements under " **ISO IEC 27001 2022 clauses**" and "**ISO IEC 27001 2022 controls**" sheet.

## Definitions

Readiness level: Approximate maturity level with regards to the **ISO/IEC 27001:2022** controls/requirements. The readiness levels are:

'Not ready' = organisation meets less than 25% of the requirements,
'Likely Low' = organisation meets between 25% and 50% of the requirements,
'Likely Intermediate' = organisation meets between 50% and 75% of the requirements,
'Likely High' = organisation meets between 75% and 100% of the requirements.

**ISO/IEC 27001:2022** is available to purchase from NSAI store @
**ISO/IEC 27001:2022** Information security, cybersecurity and privacy protection — Information security management systems — Requirements

**Normative references and definitions** in relation to ISO/IEC 27001 also available
**I.S EN ISO/IEC 27000:2020**, Information technology - Security techniques - Information security management systems - Overview and vocabulary

| ISO/IEC 27001:2022 Clauses | |
|---|---|
| **4** | Context of the organization |
| **4.1** | Understanding the organization and its context |
| **4.2** | Understanding the needs and expectations of interested parties |
| **4.3** | Determining the scope of the information security management system |
| **4.4** | Information security management system |
| **5** | Leadership |
| **5.1** | Leadership and commitment |
| **5.2** | Policy |
| **5.3** | Organizational roles, responsibilities and authorities |
| **6** | Planning |
| **6.1** | Actions to address risks and opportunities |
| **6.1.1** | General |
| **6.1.2** | Information security risk assessment |
| **6.1.3** | Information security risk treatment |
| **6.2** | Information security objectives and planning to achieve them |
| **7** | Support |
| **7.1** | Resources |
| **7.2** | Competence |
| **7.3** | Awareness |
| **7.4** | Communication |
| **7.5** | Documented information |
| **7.5.1** | General |
| **7.5.2** | Creating and updating |
| **7.5.3** | Control of documented information |
| **8** | **Operation** |
| **8.1** | Operational planning and control |
| **8.2** | Information security risk assessment |
| **8.3** | Information security risk treatment |
| **9** | Performance evaluation |
| **9.1** | Monitoring, measurement, analysis and evaluation |
| **9.2** | Internal audit |
| **9.2.1** | General |
| **9.2.2** | Internal audit programme |
| **9.3** | Management review |
| **9.3.1** | General |
| **9.3.2** | Management review inputs |
| **9.3.3** | Management review results |
| **10** | Improvement |
| **10.1** | Continual improvement |
| **10.2** | Nonconformity and corrective action |

# ISO/IEC 27001:2022 controls used in context of Clause *6.1.3 Information security risk treatment*

| A.5 | Organizational controls | |
|---|---|---|
| A.5.1 | Policies for information security | Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur. |
| A.5.2 | Information security roles and responsibilities | Information security roles and responsibilities shall be defined and allocated according to the organization needs. |
| A.5.3 | Segregation of duties | Conflicting duties and conflicting areas of responsibility shall be segregated |
| A.5.4 | Management responsibilities | Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization |
| A.5.5 | Contact with authorities | The organization shall establish and maintain contact with relevant authorities |
| A.5.6 | Contact with special interest groups | The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations. |
| A.5.7 | Threat Intelligence | Information relating to information security threats shall be collected and analysed to produce threat intelligence. |
| A.5.8 | Information security in project management | Information security shall be integrated into project management |
| A.5.9 | Inventory of information and other associated assets | An inventory of information and other associated assets, including owners, shall be developed and maintained. |
| A.5.10 | Acceptable use of information and other associated assets | Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented. |
| A.5.11 | Return of assets | Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement. |
| A.5.12 | Classification of information | Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements |
| A.5.13 | Labelling of Information | An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. |
| A.5.14 | Information transfer | Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties |
| A.5.15 | Access control | Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements. |
| A.5.16 | Identity Management | The full life cycle of identities shall be managed. |
| A.5.17 | Authentication Information | Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information. |
| A.5.18 | Access rights | Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control. |
| A.5.19 | Information security in supplier relationships | Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services. |
| A.5.20 | Addressing information security within supplier agreements | Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship. |
| A.5.21 | Managing information security in the information and communication technology (ICT) supply chain | Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain. |
| A.5.22 | Monitoring, review and change management of supplier services | The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery. |
| A.5.23 | Information security for use of cloud services | Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements. |
| A.5.24 | Information security incident management planning and preparation | The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities. |
| A.5.25 | Assessment and decision on information security events | The organization shall assess information security events and decide if they are to be categorized as information security incidents. |
| A.5.26 | Response to Information security incidents | Information security incidents shall be responded to in accordance with the documented procedures |
| A.5.27 | Learning from information security incidents | Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls. |
| A.5.28 | Collection of evidence | The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events. |

| | | |
|---|---|---|
| A.5.29 | Information security during disruption | The organization shall plan how to maintain information security at an appropriate level during disruption. |
| A.5.30 | ICT readiness for business continuity | ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements. |
| A.5.31 | Legal, statutory, regulatory and contractual requirements | Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date |
| A.5.32 | Intellectual property rights | The organization shall implement appropriate procedures to protect intellectual property rights. |
| A.5.33 | Protection of records | Records shall be protected from loss, destruction, falsification, unau¬thorized access and unauthorized release. |
| A.5.34 | Privacy and protection of person¬al identifiable information (PII) | The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements. |
| A.5.35 | Independent review of information security | The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur. |
| A.5.36 | Compliance with policies, rules and standards for information security | Compliance with the organization's information security policy, top¬ic-specific policies, rules and standards shall be regularly reviewed. |
| A.5.37 | Documented operating procedures | Operating procedures for information processing facilities shall be documented and made available to personnel who need them. |
| **A.6** | **PEOPLE CONTROLS** | |
| A.6.1 | Screening | Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. |
| A.6.2 | Terms and conditions of employment | The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security. |
| A.6.3 | Information security awareness, education and training | Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function. |
| A.6.4 | Disciplinary process | A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation. |
| A.6.5 | Responsibilities after termination or change of employment | Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties. |
| A.6.6 | Confidentiality or non-disclosure agreements | Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties. |
| A.6.7 | Remote working | Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises. |
| A.6.8 | Information security event reporting | The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner. |
| **A.7** | **PHYSICAL CONTROLS** | |
| A.7.1 | Physical security parameters | Security perimeters shall be defined and used to protect areas that contain information and other associated assets. |
| A.7.2 | Physical entry | Secure areas shall be protected by appropriate entry controls and access points |
| A.7.3 | Securing offices, rooms and facilities | Physical security for offices, rooms and facilities shall be designed and implemented. |
| A.7.4 | Physical security monitoring | Premises shall be continuously monitored for unauthorized physical access. |
| A.7.5 | Protecting against physical and environmental threats | Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented. |
| A.7.6 | Working in secure areas | Security measures for working in secure areas shall be designed and implemented |
| A.7.7 | Clear desk and clear screen | Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced |
| A.7.8 | Equipment siting and protection | Equipment shall be sited securely and protected. |
| A.7.9 | Security of assets off-premises | Off-site assets shall be protected. |
| A.7.10 | Storage media | Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements. |
| A.7.11 | Supporting utilities | Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities. |

| | | |
|---|---|---|
| A.7.12 | Cabling security | Cables carrying power, data or supporting information services shall be protected from interception, interference or damage. |
| A.7.13 | Equipment maintenance | Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information. |
| A.7.14 | Secure disposal or re-use of equipment | Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. |
| **A.8** | **TECHNOLOGY CONTROLS** | |
| A.8.1 | User end point devices | Information stored on, processed by or accessible via user end point devices shall be protected. |
| A.8.2 | Privileged access rights | The allocation and use of privileged access rights shall be restricted and managed. |
| A.8.3 | Information access restriction | Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control. |
| A.8.4 | Access to source code | Read and write access to source code, development tools and software libraries shall be appropriately managed. |
| A.8.5 | Secure authentication | Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control. |
| A.8.6 | Capacity management | The use of resources shall be monitored and adjusted in line with current and expected capacity requirements. |
| A.8.7 | Protection against malware | Protection against malware shall be implemented and supported by appropriate user awareness. |
| A.8.8 | Management of technical vulnerabilities | Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken. |
| A.8.9 | Configuration management | Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed. |
| A.8.10 | Information deletion | Information stored in information systems, devices or in any other storage media shall be deleted when no longer required. |
| A.8.11 | Data masking | Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration |
| A.8.12 | Data leakage prevention | Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information. |
| A.8.13 | Information backup | Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup. |
| A.8.14 | Redundancy of information processing facilities | Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. |
| A.8.15 | Logging | Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed. |
| A.8.16 | Monitoring activities | Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents. |
| A.8.17 | Clock synchronization | The clocks of information processing systems used by the organization shall be synchronized to approved time sources. |
| A.8.18 | Use of privileged utility programs | The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled. |
| A.8.19 | Installation of software on operational systems | Procedures and measures shall be implemented to securely manage software installation on operational systems. |
| A.8.20 | Network security | Networks and network devices shall be secured, managed and controlled to protect information in systems and applications. |
| A.8.21 | Security of network services | Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored. |
| A.8.22 | Segregation of networks | Groups of information services, users and information systems shall be segregated in the organization's networks |
| A.8.23 | Web filtering | Access to external websites shall be managed to reduce exposure to malicious content |
| A.8.24 | Use of cryptography | Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented. |
| A.8.25 | Secure development life cycle | Rules for the secure development of software and systems shall be established and applied. |
| A.8.26 | Application security requirements | Information security requirements shall be identified, specified and approved when developing or acquiring applications. |
| A.8.27 | Secure system architecture and engineering principles | Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities. |
| A.8.28 | Secure coding | Secure coding principles shall be applied to software development. |
| A.8.29 | Security testing in development and acceptance | Security testing processes shall be defined and implemented in the development life cycle. |

| | | |
|---|---|---|
| A.8.30 | Outsourced development | The organization shall direct, monitor and review the activities related to outsourced system development. |
| A.8.31 | Seperation of development, test and production environments | Development, testing and production environments shall be separated and secured. |
| A.8.32 | Change management | Changes to information processing facilities and information systems shall be subject to change management procedures. |
| A.8.33 | Test information | Test information shall be appropriately selected, protected and managed. |
| A.8.34 | Protection of information systems during audit testing | Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management. |

| Clauses | NSAI Questionnaire | Answers | Rationale |
|---|---|---|---|
| **4 Context of the organization** | Have the internal and external issues that are relevant to the ISMS, and that impact on the achievement of its expected outcome, been determined? | | |
| | Has the organization determined the interested parties that are relevant to the ISMS? | | |
| | Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements? | | |
| | Have the boundaries and applicability of the ISMS been determined to establish its scope, taking into consideration the external and internal issues, the requirements of interested parties and the interfaces and dependencies with other organizations? | | |
| | Is the scope documented? | | |
| **5 Leadership** | Is the organization's leadership commitment to the ISMS demonstrated by:<br>• Establishing the information security policy and objectives, compatible with the strategic direction of the organization, and in promotion of continual improvement? | | |
| | • Ensuring the integration of the ISMS requirements into its business processes? | | |
| | • Ensuring resources are available for the ISMS, and directing and supporting individuals, including management, who contribute to its effectiveness? | | |
| | • Communicating the importance of effective information security and conformance to ISMS requirements? | | |
| | Is there an established information security policy that is appropriate, gives a framework for setting objectives, and demonstrates commitment to | | |
| | meeting requirements and for continual improvement? | | |
| | Is the policy documented and communicated to employees and relevant interested parties? | | |
| | Are the roles within the ISMS clearly defined and communicated? | | |
| | Are the responsibilities and authorities for conformance and reporting on ISMS performance assigned? | | |
| **6 Planning** | Have the internal and external issues, and the requirements of interested parties been considered to determine the risks and opportunities that need to be addressed to ensure that the ISMS achieves its outcome, that undesired effects are prevented or reduced, and that continual improvement is achieved? | | |
| | Have actions to address risks and opportunities been planned, and integrated into the ISMS processes, and are they evaluated for effectiveness? | | |
| | Has an information security risk assessment process that establishes the criteria for performing information security risk assessments, including risk acceptance criteria been defined? | | |
| | Is the information security risk assessment process repeatable and does it produce consistent, valid and comparable results? | | |
| | Does the information security risk assessment process identify risks associated with loss of confidentiality, integrity and availability for information within the scope of the ISMS, and are risk owners identified? | | |
| | Are information security risks analysed to assess the realistic likelihood and potential consequences that would result, if they were to occur, and have | | |
| | the levels of risk been determined? | | |
| | Are information security risks compared to the established risk criteria and prioritised? | | |
| | Is documented information about the information security risk assessment process available? | | |
| | Is there an information security risk treatment process to select appropriate risk treatment options for the results of the information security risk | | |
| | assessment, and are controls determined to implement the risk treatment option chosen? | | |
| | Have the controls determined, been compared with ISO/IEC 27001:2017 Annex A to verify that no necessary controls have been missed? | | |
| | Has a Statement of Applicability been produced to justify Annex A exclusions, and inclusions together with the control implementation status? | | |
| | Has an information security risk treatment plan been formulated and approved by risk owners, and have residual information security risks been | | |
| | authorised by risk owners? | | |
| | Is documented information about the information security risk treatment process available? | | |
| | Have measurable ISMS objectives and targets been established, documented and communicated throughout the organization? | | |
| | In setting its objectives, has the organization determined what needs to be done, when and by whom? | | |
| | Is everyone within the organization's control aware of the importance of the information security policy, their contribution to the effectiveness of the ISMS and the implications of not conforming? | | |

| | | | |
|---|---|---|---|
| **7 Support** | Has the organization determined the need for internal and external communications relevant to the ISMS, including what to communicate, when, with whom, and who by, and the processes by which this is achieved? | | |
| | Has the organization determined the documented information necessary for the effectiveness of the ISMS? | | |
| | Is the documented information in the appropriate format, and has it been identified, reviewed and approved for suitability? | | |
| | Is the documented information controlled such that it is available and adequately protected, distributed, stored, retained and under change control, including documents of external origin required by the organization for the ISMS? | | |
| **8 Operation** | Has a programme to ensure the ISMS achieves its outcomes, requirements and objectives been developed and implemented? | | |
| | Is documented evidence retained to demonstrate that processes have been carried out as planned? | | |
| | Are changes planned and controlled, and unintended changes reviewed to mitigate any adverse results? | | |
| | Have outsourced processes been determined and are they controlled? | | |
| | Are information security risk assessments performed at planned intervals or when significant changes occur, and is documented information retained? | | |
| | Has the information security risk treatment plan been implemented and documented information retained? | | |
| **9 Performance evaluation** | Is the information security performance and effectiveness of the ISMS evaluated? | | |
| | Has it been determined what needs to be monitored and measured, when, by whom, the methods to be used, and when the results will be evaluated? | | |
| | Is documented information retained as evidence of the results of monitoring and measurement? | | |
| | Are internal audits conducted periodically to check that the ISMS is effective and conforms to both ISO/IEC 27001:2022 and the organization's requirements? | | |
| | Are the audits conducted by an appropriate method and in line with an audit programme based on the results of risk assessments and previous audits? | | |
| | Are results of audits reported to management, and is documented information about the audit programme and audit results retained? | | |
| | Where non conformities are identified, are they subject to corrective action (see section 18)? | | |
| | Do top management undertake a review of the ISMS at planned intervals? | | |
| | Does the output from the ISMS management review identify changes and improvements? | | |
| | Are the results of the management review documented, acted upon and communicated to interested parties as appropriate? | | |
| **10 Improvement** | Have actions to control, correct and deal with the consequences of non-conformities been identified? | | |
| | Has the need for action been evaluated to eliminate the root cause of non-conformities to prevent reoccurrence? | | |
| | Have any actions identified been implemented and reviewed for effectiveness and given rise to improvements to the ISMS? | | |
| | Is documented information retained as evidence of the nature of non-conformities, actions taken and the results? | | |

| Controls | NSAI Questionnaire | Answers | Rationale |
|---|---|---|---|
| **A.5** Organizational controls | Are information security policies that provide management direction defined and regularly reviewed? | | |
| | Has a management framework been established to control the implementation and operation of security within the organization, including assignment of responsibilities and segregation of conflicting duties? | | |
| | Are appropriate contacts with authorities and special interest groups maintained? | | |
| | Have the processes for acquisition, use, management and exit from cloud services been defined and communicated to relevant interested parties and has a risk assessment been conducted on the cloud services provided by the cloud service provider? | | |
| | Has information relating to information security threats been collected, analysed, and shared among relevant interested parties and has the analysed information been integrated into your organization's technical preventive and detective controls? | | |
| | Is information security addressed in Projects? | | |
| | Is information classified and appropriately labelled, and have procedures for handling assets in accordance of their classification been defined? | | |
| | Based on the outcome of the business impact analysis and risk assessment involving ICT services, has ICT continuity strategies for business continuity during, before and after disruption been planned, implemented, maintained and tested? | | |
| | Is there an inventory of assets associated with information and information processing, have owners been assigned, and are rules for acceptable use of assets and return of assets defined? | | |
| | Has an access control policy been defined and reviewed, and is user access to the network controlled in line with the policy? | | |
| | Is there a formal user registration process assigning and revoking access and access rights to systems and services, and are access rights regularly reviewed, and removed upon termination of employment? | | |
| | Are privileged access rights restricted and controlled, and is secret authentication information controlled, and users made aware of the practices for use? | | |
| | Is access to information restricted in line with the access control policy, and is access controlled via a secure log-on procedure? | | |
| | Are there policies and agreements in place to protect information assets that are accessible to suppliers, and is the agreed level of information security and service delivery monitored and managed, including changes to provision of services? | | |
| | Is there a consistent approach to the management of security incidents and weaknesses, including assignment of responsibilities, reporting, assessment, response, analysis and collection of evidence? | | |
| | Have all legislative, statutory, regulatory and contractual requirements and the approach to meeting these requirements been defined for each information system and the organization, including but not limited to procedures for intellectual property rights, protection of records, privacy and protection of personal information and regulation of cryptographic controls? | | |
| | Is there an independent review of information security? | | |

| Controls | NSAI Questionnaire | Answers | Rationale |
|---|---|---|---|
| | Is there a procedure in place to protect intellectual property rights? | | |
| | Has appropriate technical and organizational measures been implemented to protect PII? | | |
| | Are information systems regularly reviewed for technical compliance with policies and standards? | | |
| | Do managers regularly review the compliance of information processing and procedures within their areas of responsibility? | | |
| | Are operating procedures documented and are changes to the organization, business processes and information systems controlled? | | |
| **A.6** People Controls | Are human resources subject to screening, and do they have terms and conditions of employment defining their information security responsibilities? | | |
| | Are employees required to adhere to the information security policies and procedures, provided with awareness, education and training, and is there a disciplinary process? | | |
| | Are the information security responsibilities and duties communicated and enforced for employees who terminate or change employment? | | |
| | Are security measures implemented for personnels working remotely? | | |
| | Is it standard practice for all parties involved to have signed, documented, and regularly reviewed confidentiality and non-disclosure agreements? | | |
| **A.7** Physical controls | Are there policies and controls to prevent unauthorised physical access and damage to information and information processing facilities? | | |
| | Are there policies and controls in place to prevent loss, damage, theft or compromise of assets and interruptions to operations? | | |
| | Before being disposed of or used again, has the device been checked to see if storage media is contained? | | |
| | Are physical premises constantly monitored by surveillance systems? | | |
| | Are clear desk and clear screen rules defined and appropriately enforced? | | |
| | Is there a consistent approach to the management of security incidents and weaknesses, including assignment of responsibilities, reporting, assessment, response, analysis and collection of evidence? | | |
| | Are information processing facilities implemented with redundancy to meet availability requirements? | | |
| | Is information about technical vulnerabilities obtained and appropriate measures taken to address risks? | | |
| | Has sensitive data that was previously stored on systems, devices, and services but is no longer required been securely deleted using the appropriate deletion method and has your organization verified your vendor's deletion process as acceptable? | | |
| | Have techniques for hiding sensitive data (PII), such as data masking, pseudonymization, or anonymization, been implemented in accordance with the organization's access control policy? | | |
| | Are utility programs that can be capable of overriding system and application controls restricted and tightly controlled? | | |

| Controls | NSAI Questionnaire | Answers | Rationale |
|---|---|---|---|
| **A.8** Technological controls | Are privileged access rights restricted and controlled, and is secret authentication information controlled, and users made aware of the practices for use? | | |
| | Are operating procedures documented and are changes to the organization, business processes and information systems managed? | | |
| | Have effective secure coding practices been applied before, during and after software development and is there a software security testing and monitoring process to identify security vulnerabilities? | | |
| | Is outsourced software development supervised and monitored? | | |
| | Are development, testing and production environments securely separated? | | |
| | Are there controls in place to log events and generate evidence? | | |
| | Are the clocks of information processing systems synchronized to approved time sources? | | |
| | Are networks managed, segregated when necessary, and controlled to protect information systems, and are network services subject to service agreements? | | |
| | Are information security requirements for information systems defined and is information passing over public networks and application service transactions protected? | | |
| | Are systems and rules for the development of software established and changes to systems within the development lifecycle formally controlled? | | |
| | Are procedures in place to securely manage software installation on operational systems? | | |
| | Are application security requirements identified and specified during development and acquisition? | | |
| | Are information, software and systems subject to back up and regular testing? | | |
| | Has the organisation utilized appropriate measures or tools to identify, classify, detect and prevent user actions or network transmissions that expose sensitive information? | | |
| | Have measures been taken to prevent employees from accessing unauthorized web resources, such as web filtering tools and staff training on how to use internet resources safely and appropriately? | | |
| | Is there a monitoring system in place that constantly monitors anomalous behaviour while also performing the appropriate actions to evaluate information security incidents on networks, systems and applications in real time? | | |
| | Is there protection against malware? | | |
| | Are test information appropriately selected, protected and managed? | | |
| | Have audit tests and other assurance activities involving assessment of operational systems been planned and agreed between the tester and appropriate management? | | |

| Your readiness score |
| --- |
| Not ready |

| Clauses readiness score |
| --- |
| Not ready |

| Controls readiness score |
| --- |
| Not ready |