ISO/IEC 27001:2013
Information Security
Management System

Self-assessment questionnaire

How ready are you for ISO/IEC 27001:2013?

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

---

1. The organization and its context

Have the internal and external issues that are relevant to the ISMS, and that impact on the achievement of its expected outcome, been determined? ☐

2. Needs and expectations of interested parties

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? ☐

3. Scope of the ISMS

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 of the ISMS documented? ☐

Continue >>

bsi.

...making excellence a habit.™

4. Leadership and management commitment

Is the organization's leadership commitment to the ISMS demonstrated by:

- Establishing the information security policy and objectives, in consideration of 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?

5. Information security policy

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?

6. Roles and responsibilities

Are the roles within the ISMS clearly defined and communicated?

Are the responsibilities and authorities for conformance and reporting on ISMS performance assigned?

7. Risks and opportunities of ISMS implementation

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?

8. Information security risk assessment

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?

9. Information security risk treatment

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 27001:2013 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?

10. Information security objectives and planning to achieve them

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?

11. ISMS resources and competence

Is the ISMS adequately resourced?

Is there a process defined and documented for determining competence for ISMS roles?

Are those undertaking ISMS roles competent, and is this competence documented appropriately?

12. Awareness and communication

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?

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?

13. Documented information

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?

Continue >>

14. Operational planning and control

- 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?

15. Monitoring, measurement and 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?

16. Internal audit

- Are internal audits conducted periodically to check that the ISMS is effective and conforms to both ISO/IEC 27001:2013 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)?

17. Management review

- Do top management undertake a periodic review of the ISMS?
- 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?

18. Corrective action and continual 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?

19. Security controls – as applicable, based on the results of your information security risk assessment

- 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?
- Is information security addressed in Projects?
- Is there a mobile device policy and teleworking policy in place?
- 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?
- 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?
- Is information classified and appropriately labelled, and have procedures for handling assets in accordance of their classification been defined?
- Are there procedures for the removal, disposal and transit of media containing information?
- 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 password management systems interactive and do they enforce a quality password?
- Is the use of utility programs and access to program source code restricted?
- Is there a policy for the use of cryptography and key management?
- 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?
- Are operating procedures documented and are changes to the organization, business processes and information systems controlled?
- Are resources monitored and projections made of future capacity requirements?

Continue >>

Is there separation of development, testing and operational environments?

Is there protection against malware?

Are information, software and systems subject to back up and regular testing?

Are there controls in place to log events and generate evidence?

Is the implementation of software on operational systems controlled, and are there rules governing the installation of software by users?

Is information about technical vulnerabilities obtained and appropriate measures taken to address risks?

Are networks managed, segregated when necessary, and controlled to protect information systems, and are network services subject to service agreements?

Are there policies and agreements to maintain the security of information transferred within or outside of the organization?

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 business critical applications reviewed and tested after changes to operating system platforms and are there restrictions to changes to software packages?

Have secure engineering principles been established and are they maintained and implemented, including secure development environments, security testing, the use of test data and system acceptance testing?

Is outsourced software development supervised and monitored?

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?

Is information security continuity embedded within the business continuity management system, including determination of requirements in adverse situations, procedures and controls, and verification of effectiveness?

Are information processing facilities implemented with redundancy to meet availability requirements?

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?

Do managers regularly review the compliance of information processing and procedures within their areas of responsibility?

Are information systems regularly reviewed for technical compliance with policies and standards?

For BSI to complete the analysis on your behalf, please click the submit button below or email a saved copy of your completed questionnaire to:
sales.nl@bsigroup.com

Save Submit

+31 20 346 0780
sales.nl@bsigroup.com
bsigroup.com