hicomply

ISO 27001 Checklist: A Step-by-Step Guide

hicomply

Contents

1. 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 organisation determined the interested groups that are relevant to the ISMS?
- [ ] Have the requirements of these interested groups been identified, including legal, regulatory and contractual requirements?

3. ISMS scope

- [ ] Have the boundaries and applicability of the ISMS been established to ascertain its scope, in line with both internal external issues, the needs of interested groups and the interfaces and dependencies with other businesses or organisations?
- [ ] Is the scope of the ISMS documented?

4. Leadership and management commitment

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

- [ ] Establishing the information security policy and objectives, in consideration of the strategic direction of the organisation, and in promotion of continuous improvement?
- [ ] Ensuring resources are available for the ISMS, and directing and aiding the individuals, including management, who support its effectiveness?
- [ ] Establishing the importance of effective information security and conformance to ISMS requirements?

5. Information security policy

- [ ] Is there an established information security policy that is relevant, gives a framework for setting objectives, and proves commitment to meeting information security requirements and for ongoing improvement?
- [ ] Is the policy documented and communicated to employees and relevant groups?

6. Roles and responsibilities

- [ ] Are the roles within the ISMS clearly specified and circulated within the organisation?
- [ ] Are the responsibilities and authorities for compliance and reporting on ISMS performance assigned?

7. Risks and opportunities of ISMS implementation

- [ ] Have the internal and external issues, and the needs of interested groups been considered to ascertain the risks and opportunities that need to be addressed to ensure that the ISMS achieves its outcome, that unwanted effects are stopped or reduced, and that continuous 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 undertaking information security risk assessments, including risk acceptance criteria, been established?
- [ ] Does the information security risk assessment procedure determine risks associated with loss of confidentiality, integrity and availability for information within the scope of the ISMS, and are risk owners established?

(cont.)

8. Information security risk assessment (cont.)

- [ ] Are risks to information security analysed to assess the practical likelihood and possible consequences that would result, should they occur, and have the levels of risk been established?
- [ ] Are risks to information security correlated to the established risk criteria and prioritised as necessary?
- [ ] Is information about the information security risk assessment process available in a documented format?

9. Information security risk treatment

- [ ] Is there an information security risk treatment process in place to select relevant risk treatment options for the results of the information security risk assessment, and are controls established to implement the risk treatment option chosen?
- [ ] Have the established controls been compared with ISO/IEC 27001:2013 Annex A to verify that no essential controls have been missed?
- [ ] Has an information security risk treatment plan been formulated and approved by risk owners, and have residual information security risks been permitted by risk owners?
- [ ] Is information about the information security risk treatment process available in a documented format?

10. Information security objectives and planning to achieve them

- [ ] Have measurable ISMS objectives and targets been ascertained, documented and disclosed throughout the organisation?
- [ ] In setting its objectives, has the organisation established what needs to be done, when and by whom?

11. ISMS resources and competence

- [ ] Is the ISMS adequately resourced?
- [ ] Is there a defined and documented procedure for determining competence for ISMS roles?
- [ ] Are those undertaking ISMS roles competent, and is this capability correctly documented?

12. Awareness and communication

- [ ] Is everyone within the organisation's control aware of the significance of the information security policy, their role in the success of the ISMS and the ramifications of not conforming?
- [ ] Has the organisation established the need for internal and external communications relevant to the ISMS, including what to disclose, when, with whom, and who by, and the procedures by which this is achieved?

13. Documented information

- [ ] Has the organisation established the documented information necessary for the effectiveness of the ISMS?
- [ ] Is the documented information in the correct format, and has it been identified, reviewed and approved for suitability?
- [ ] Is the documented information controlled in such a way that it is available and appropriately secured, distributed, stored, retained and under change control, including documents of external origin required by the organisation for the ISMS?

14. Operational planning and control

- [ ] Has a programme to ensure the organisation's ISMS delivers its outcomes, requirements and objectives been created and implemented?
- [ ] Is documented evidence retained to illustrate that processes have been carried out as planned?

(cont.)

14. Operational planning and control (cont.)

- [ ] Are changes planned and controlled, and unplanned changes reviewed to alleviate any adverse results?
- [ ] Have outsourced procedures been established and are they controlled?
- [ ] Are information security risk assessments undertaken at regularly 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 appraised?
- [ ] Is documented information retained as evidence of the results of observation and measurement?

16. Internal audit

- [ ] Are internal audits undertaken regularly to check that the ISMS is successful and conforms to both ISO/IEC 27001:2013 and the organisation's requirements?
- [ ] Are the audits undertaken by an appropriate method and in line with an audit programme based on the results of risk assessments and any previous audits?
- [ ] Are the results of audits reported to management, and is documented information about the audit programme and audit results retained?
- [ ] Where non-conformities are detected, are they subject to corrective action (as in section 18)?

17. Management review

- [ ] Does senior management undertake a regular review of the ISMS?
- [ ] Does the output from the ISMS management review establish necessary changes and improvements?
- [ ] Are the results of the management review documented, acted upon and disclosed to interested groups as appropriate?

18. Corrective action and continual improvement

- [ ] Have actions to govern, amend and deal with the ramifications of non-conformities been identified?
- [ ] Has the need for action been calculated to eliminate the root cause of non-conformities in order to prevent recurrence?
- [ ] Have any actions identified been implemented and analysed for effectiveness and led to improvements to the ISMS?
- [ ] Have any actions identified been implemented and analysed for effectiveness and led to improvements to the ISMS?
- [ ] Is documented information retained as evidence of the nature of non-conformities, actions taken and the results?
- [ ] Is there a split between 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 installation of software on operational systems controlled, and are there rules controlling the installation of software by users?
- [ ] Is information about technical vulnerabilities collected and appropriate measures taken to address risks?

(cont.)

18. Corrective action and continual improvement (cont.)

- [ ] 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 preserve the security of information conveyed internally or external to the organisation?
- [ ] Are information security requirements for information systems outlined and is information passing over public networks and application service transactions safeguarded?
- [ ] 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 examined after changes to operating system platforms and are there restrictions to changes to software packages?
- [ ] Have secure engineering principles been implemented, including secure development environments, security testing, the use of test data and system acceptance testing?
- [ ] Is any outsourced software development managed and monitored?

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

- [ ] Are information security policies that provide management direction outlined and regularly reviewed?
- [ ] Has a management framework been created to control the implementation and management of security within the organisation, including assignment of responsibilities and segregation of conflicting duties?
- [ ] Are appropriate contacts with authorities and special interest groups retained?
- [ ] Is information security addressed in projects?

(cont.)

Security controls (cont.)

- [ ] Is there a mobile device policy and teleworking policy in place?
- [ ] Is the human resources department subject to screening, and does it have terms and conditions of employment defining staff's information security responsibilities?
- [ ] Are employees obligated 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 disclosed and enforced for employees who terminate or change employment?
- [ ] Is there an inventory of assets associated with information and information processing, have asset 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 created and reviewed, and is user access to the network managed 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 require the use of a quality password?
- [ ] Is the use of utility programmes and access to programme source code restricted?

(cont.)

Security controls (cont.)

- [ ] 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 organisation, business processes and information systems controlled?
- [ ] Are resources monitored and projections made of future capacity requirements?
- [ ] 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 organisation, 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?

(cont.)

Security controls (cont.)

- [ ] 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?

You've completed your ISO 27001 checklist!

To learn more about how you can automate the process to ISO 27001 certification and take the stress out of building your organisation's ISMS, get in touch with team Hicomply - or explore the options below:

Book a demo

Read the Hicomply blog

Visit the ISO 27001 hub