ISO/IEC 27001:2022 Self-assessment questionnaire

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.

Context of the organization

- Have you determined the external and internal issues that are relevant to your organization's purpose that affects your ability to achieve the intended results of your Information Security Management System (ISMS)? ☐
- Have you determined the needs and expectations of interested parties that are relevant to the ISMS and do you review these on a regular basis? ☐
- Have you determined the scope of your ISMS and did this take into account the external and internal issues, interested parties, and any activities performed by other organizations? ☐
- Have the internal and external issues that may impact the ISMS been considered? ☐
- Have the risks and opportunities associated with these issues and requirements been considered? ☐
- Are you aware of the requirements of interested parties, including regulatory, statutory and those of your customers? ☐
- Have you determined which of the requirements of interested parties will be addressed through the information security management system? ☐
- Has continual improvement been considered? ☐
- Have the processes needed to establish, maintain, implement and establish the information security management systems and their interactions been determined and implemented? ☐

Leadership

- Are the information security policy and objectives that have been established compatible with the context and strategic direction of the organization? ☐
- Has the information security policy been communicated within the organization and to interested parties? ☐
- Does the policy include information security objectives or provides the framework for setting information security objectives ☐
- Are the roles within the ISMS clearly defined, annotated and communicated? ☐
- Do the roles carry the authority for ensuring conformance and reporting, as well as the responsibility? ☐
- Has a programme to ensure the ISMS achieves its outcomes, requirements and objectives been developed and put in place? ☐
- Have you communicated the importance of effective information security management and of conforming to the informartion security management system requirements? ☐

bsi.

Planning

Have the risks and opportunities identified in the interetsed parties and scope been addressed to ensure the ISMS can achieve its intended result(s) been established?

Has an information security risk assessment process been established to include risk acceptance criteria?

Has the information security risk assessment process been defined and developed to be repeatable and ensure consistent, valid and comparable results?

Does the risk assessment produce consistent, valid and comparable results?

Has the organization planned actions to address these risks and opportunities and determined how to integrate and implement them into the ISMS, and how to evaluatate the effectiveness of these actions??

Is the information security risk assessment process sufficient to identify risks associated with loss of confidentiality, integrity and availability for information within the scope of the ISMS?

Have risk owners been identified?

Are information security risks analyzed 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 prioritized?

Has information about the information security risk assessment process been documented?

Have appropriate risk treatment options been determined and implemented?

Have controls been determined to implement the risk treatment option chosen?

Have the controls determined, been compared with ISO/IEC 27001:2022 Annex A to verify that no necessary controls have been missed?

Is there a Statement of Applicability with revision history in accordance with ISO 27001:2022?

Does the Statement of Applicability include whether the necessary controls are implemented or not?

Does the Statement of Applicability include justification for the selection or exclusion of controls from Annex A?

Has an information security risk treatment plan been created?

- Have risk owners reviewed and approved the plan?
- Have residual information security risks been authorized by risk owners?
- Has it been documented?

Have measurable ISMS objectives 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?

Have you determined and documented how the objectives are to be monitored?

While planning for change in ISMS have you determined the need for changes to ISMS, and how the changes are to be carried out in a planned manner?

Support

Have you determined and provided the resources needed to establish, implement, maintain and continually improve the ISMS (including people, infrastructure and environment for the operation of processes)?

Have you determined the competence necessary for those performing ISMS roles? (e.g risk owners, internal auditors, etc.)

Is there evidence of competence for these roles?

Have you ensured that persons doing work under the organization's control are

i) aware of the ISMS policy

ii) how their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance.

iii) the implications of not conforming with the information security management system requirements. (e.g disciplinary actions)

Has the documented information required by the standard and necessary for the effective implementation and operation of the ISMS been established?

Has the organisation determined what internal and extermnal coiommunications may be relevant?

Is the documented information controlled in a way 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?

Operations

Have you implemented or are implementing the actions determined in Clause 6, by:
— establishing criteria for the processes;
— implementing control of the processes in accordance with the criteria?

Have documented evidence been kept to show that processes have been carried out as planned?

Is there a plan to determine the need for changes to the ISMS and managing their implementation?

When changes are planned, are they carried out in a controlled way and actions taken to mitigate any adverse effects?

For the externally provided processes, are they appropriately controlled and implemented?

Are information security risk assessments carried out at planned intervals or when significant changes occur, and is documented information retained?

Has the organization planned actions to address risks and opportunities and integrated them into the system processes?

Is there a process to retain documented information on the results of the information security risk assessment?

Is there a process to obtain approval for risk treatment and residual risk from the risk owners?

Performance evaluation

Have you determined what needs to be monitored and measured, when, by whom, the methods to be used, and when the results will be evaluated?

Are the results of monitoring and measurement documented?

Can the auditors selected to conduct internal audits demonstrate objectivity and impartiality during the process?

Has the organization established a program for internal audits to check that the ISMS is effective and conforms to the requirements of ISO/IEC 27001 and the organization's own requirements?

Are results of these audits reported to management, documented and retained?

Where nonconformities are identified, has the organization established appropriate processes for managing nonconformities and the related corrective actions?

Do top management undertake regular and periodic reviews of the ISMS?

Does the input to management review include changes in external and internal issues and changes in the need for interested parties?

Have the feedback on information security performance been considered as an input to the management review?

Does the output from the ISMS management review identify changes and improvements?

Is documented information available to evidence the results of the management review?

Improvement

Have actions to control, correct and deal with the consequences of nonconformities been identified? ☐

Has the need for action been evaluated to eliminate the root cause of nonconformities and to prevent reoccurrence? ☐

Have any actions identified been implemented and reviewed for effectiveness and given rise to improvements to the ISMS? ☐

Is documented information kept as evidence of the nature of non-conformities, actions taken and the results? ☐