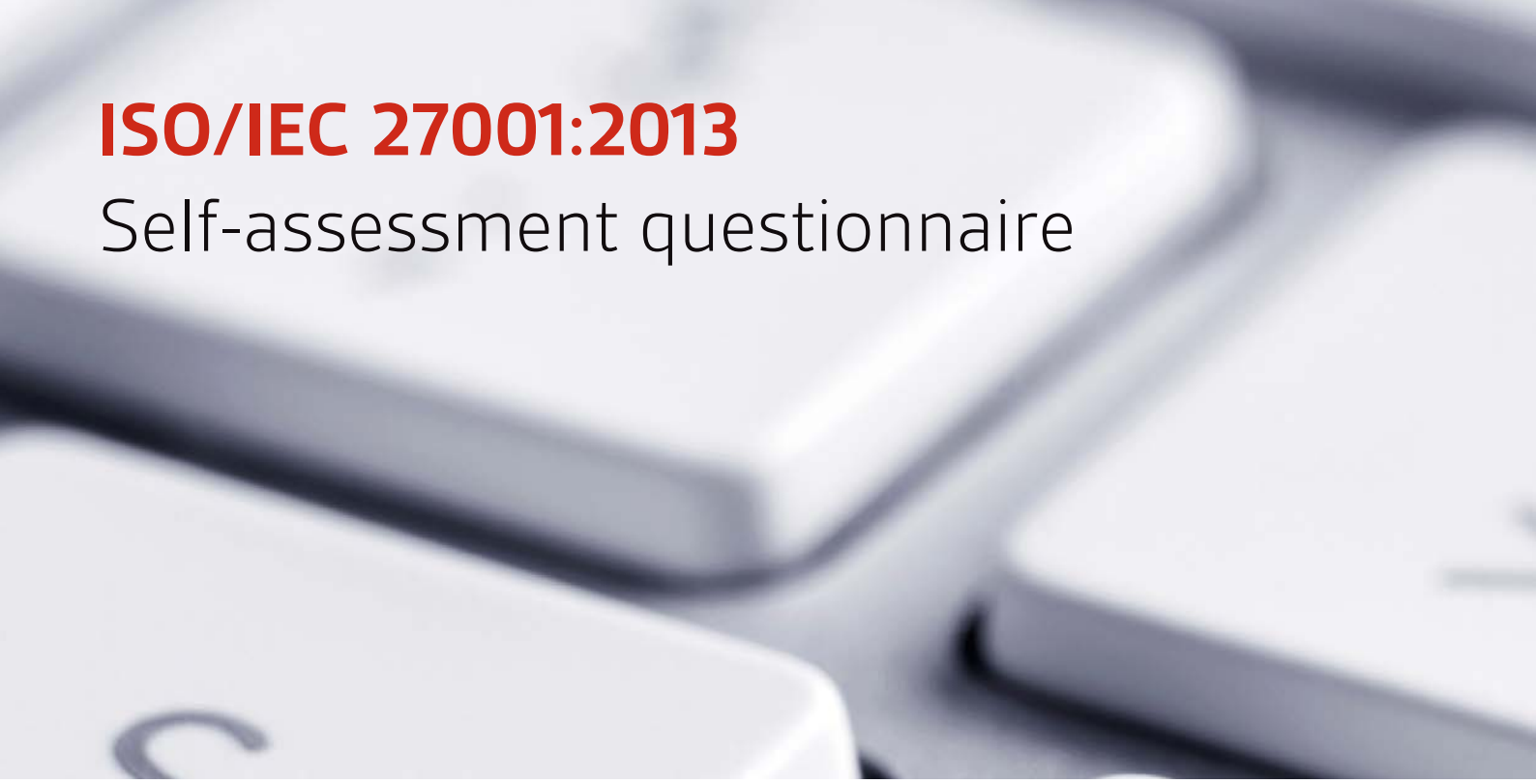

ISO/IEC 27001:2013

Self-assessment questionnaire

How ready are you?

This document has been designed to assess your company's readiness for an ISO/IEC 27001:2013 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)?
- Do you have a way of reviewing and monitoring changes to these issues on a regular basis?
- 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?
- Are you aware of the requirements of interested parties, including regulatory, statutory and those of your customers?
- Have the risks and opportunities associated with these issues and requirements been considered?
- Has continual improvement been considered?

Leadership

- Has top management taken responsibility for the effectiveness of the ISMS and have they communicated the importance of an effective ISMS?
- Have the policy and objectives for the ISMS, which are compatible with the context and strategic direction of the organization, been established and communicated?
- 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?

Continued >>

Leadership – *continued*

Has a programme to ensure the ISMS achieves its outcomes, requirements and objectives been developed and put in place?

Planning

Have the risks and opportunities that need to be 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 developed to be repeatable?

Does it produce consistent, valid and comparable results?

Has the organization planned actions to address these risks and opportunities and integrated them?

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 and is available?

Does the information security risk treatment process allow for appropriate options?

Have controls been 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 left out?

Have you produced a Statement of Applicability to justify Annex A exclusions and inclusions, together with the control implementation status?

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?

Planning – *continued*

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

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?

Support

Has the organization determined and provided the resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS (including people, infrastructure and environment for the operation of processes)?

Do you have a defined and documented process for determining competence for ISMS roles?

- Is that process and the competence of those in those roles documented?

Has the organization determined the knowledge necessary for those performing ISMS roles?

Has the organization ensured that those persons who can affect the performance and effectiveness of the ISMS are competent on the basis of appropriate education, training, or experience or taken action to ensure that those persons can gain the necessary competence?

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

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?

Operation

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

Is there a plan for the determining 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?

If you have outsourced processes, are they appropriately controlled?

Continued >>

Operation – *continued*

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 integrate them into the system processes?

Have these actions been documented?

Performance evaluation

Do you have criteria for the evaluation, selection, monitoring of performance and re-evaluation of your external providers?

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?

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?

Has the organization established a program for internal audits of the ISMS?

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 output from the ISMS management review identify changes and improvements?

Performance eveluation – *continued*

Are the results of the management review documented, acted upon and communicated to interested parties as appropriate?

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

Do top management carry out regular and periodic reviews 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?

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 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?