

## ISO/IEC 27001:2022Self-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	Leadership	
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	Are the information security policy and objectives that have been established compatible with the context and strategic direction of the organization?	
Management System (ISMS)?	Has the information security policy been communicated within the organization and to	
Have you determined the needs and expectations of interested parties that are relevant to the ISMS	interested parties?	
and do you review these on a regular basis?	Does the policy include information security objectives or provides the framework for setting information security objectives	
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?	Are the roles within the ISMS clearly defined, annotated and communicated?	
Have the internal and external issues that may impact the ISMS been considered?	Do the roles carry the authority for ensuring conformance and reporting, as well as the responsibility?	
Have the risks and opportunities associated with these issues and requirements been considered?	Has a programme to ensure the ISMS achieves its outcomes, requirements and objectives been developed and put in place?	
Are you aware of the requirements of interested parties, including regulatory, statutory and		
those of your customers?	Have you communicated the importance of effective information security management and of conforming to the informartion security	
Have you determined which of the requirements of interested parties will be addressed through the information security management system?	management system requirements?	
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?		



Have the risks and opportunities identified in the interested 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 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?  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 reviewed and approved the plan?  Have risk owners?  Have residual information security risks been authorized by risk owners?  Have measurable ISMS objectives been established, documented?  In setting its objectives, has the organization determined what needs to be done, when and by whom?  In setting its objectives, has the organization 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 information security risks compared to the established risk criteria and prioritized?  Are information about the information security risk assessment process been determined?  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 processe	Planning		
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 reviewed and approved the plan?  Have residual information security risks been authorized by risk owners?  Have measurable ISMS objectives been established, documented?  Have measurable ISMS objectives been established, documented and communicated throughout the organization?  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	interetsed parties and scope been addressed to ensure the ISMS can achieve its intended result(s)	justification for the selection or exclusion of	
the plan?  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 about the information security risk compared to the established risk criteria and prioritized?  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.)  Have you determined the competence for these roles?  Have you determined the competence of competenc	process been established to include risk		
Have residual information security risks been authorized by risk owners?      Has the been documented?  Has the been documented?  Has the been documented?  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?  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?  Have appropriate risk treatment options been determined and implemented?  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	acceptance criteria?	·	
<ul> <li>Has it been documented?</li> <li>Have measurable ISMS objectives been established, documented and communicated throughout the organization?</li> <li>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??</li> <li>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?</li> <li>Have risk owners been identified?</li> <li>Have 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?</li> <li>Are information security risks compared to the established risk criteria and prioritized?</li> <li>Has information about the information security risk assessment process been documented?</li> <li>Has information about the information security risk assessment process been documented?</li> <li>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)?</li> <li>Have you determined the competence necessary for those performing ISMS roles? (e.g risk owners, internal auditors, etc.)</li> <li>Have you determined the competence necessary for those performing ISMS roles? (e.g risk owners, internal auditors, etc.)</li> <li>Have controls been determined to implement the risk treatment option chosen?</li> <li>Have you ensured that persons doing work under</li> </ul>	process been defined and developed to be repeatable and ensure consistent, valid and		
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 about the information security risk assessment process been documented?  Has information about the information security risk assessment process been documented?  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.)  Have controls been determined to implement the risk treatment option chosen?  Have you ensured that persons doing work under	·	Has it been documented?	
In setting its objectives, has the organization plantage attoints?  In setting its objectives, has the organization 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?  In setting its objectives, has the organization determined what needs to be done, when and by whom?  In setting its objectives, has the organization 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		established, documented and communicated	
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?  Are information about the information security risk assessment process been documented?  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	Has the organization planned actions to address these risks and opportunities and determined how	throughout the organization?	
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?  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.)  Have controls been determined to implement the risk treatment option chosen?  Have you ensured that persons doing work under	to integrate and implement them into the ISMS, and how to evaluatate the effectiveness	determined what needs to be done, when and	
determined the need for changes to ISMS, and how the changes are to be carried out in a planned manner?  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?  Are information security risks compared to the established risk criteria and prioritized?  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 appropriate risk treatment options been determined and implemented?  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	process sufficient to identify risks associated with loss of confidentiality, integrity and availability for		
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?  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 appropriate risk treatment options been determined and implemented?  Have controls been determined to implement the risk treatment option chosen?  Is there evidence of competence for these roles?  Have you ensured that persons doing work under	information within the scope of the ISMS?		
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 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.)  Have controls been determined to implement the risk treatment option chosen?  Have you ensured that persons doing work under	Have risk owners been identified?	and how the changes are to be carried out	
Are information security risks compared to the established risk criteria and prioritized?  Has information about the information security risk assessment process been documented?  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.)  Have controls been determined to implement the risk treatment option chosen?  Have you ensured that persons doing work under	the realistic likelihood and potential consequences that would result, if they were to occur, and have	Support	
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?  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			
Has information about the information security risk assessment process been documented?  Have you determined the competence necessary for those performing ISMS roles? (e.g risk owners, internal auditors, etc.)  Have controls been determined to implement the risk treatment option chosen?  Is there evidence of competence for these roles?  Have you ensured that persons doing work under		continually improve the ISMS (including people, infrastructure and environment for the operation	
Have appropriate risk treatment options been determined and implemented?  Have controls been determined to implement the risk treatment option chosen?  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			
Have controls been determined to implement the risk treatment option chosen?  Have you ensured that persons doing work under	Have appropriate risk treatment options been	for those performing ISMS roles? (e.g risk owners,	
Have you lensured that persons doing work under	Have controls been determined to implement the	Is there evidence of competence for these roles?	
the organization's control are	risk treatment option chosen?	Have you ensured that persons doing work under the organization's control are	
Have the controls determined, been compared with ISO/IEC 27001:2022 Annex A to verify that  i) aware of the ISMS policy		_	
no necessary controls have been missed?  ii) how their contribution to the effectiveness of the information security management system, including the benefits of improved information		the information security management system,	
history in accordance with ISO 27001:2022?		security performance.	
Does the Statement of Applicability include whether the necessary controls are implemented  iii) the implications of not conforming with the information security management system requirements. (e.g disciplinary actions)	Does the Statement of Applicability include	the information security management system	



or not?

Has the documented information required by	Performance evaluation	
the standard and necessary for the effective implementation and operation of the ISMS been established?	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?	
Has the organisation determined what internal and extermnal coiommunications may be relevant?	Are the results of monitoring and measurement documented?	
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?	Can the auditors selected to conduct internal audits demonstrate objectivity and impartiality during the process?	
Operations	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?	
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?	Are results of these audits reported to management, documented and retained?	
Have documented evidence been kept to show that processes have been carried out as planned?	Where nonconformities are identified, has the organization established appropriate processes for managing nonconformities and the related corrective actions?	
Is there a plan to determine the need for changes to the ISMS and managing their implementation?	Do top management undertake regular and periodic reviews of the ISMS?	
When changes are planned, are they carried out in a controlled way and actions taken to mitigate any adverse effects?	Does the input to management review include changes in external and internal issues and changes in the need for interested parties?	
For the externally provided processes, are they appropriately controlled and implemented?	Have the feedback on information security performance been considered as an input to the management review?	
Are information security risk assessments carried out at planned intervals or when significant changes occur, and is documented information retained?	Does the output from the ISMS management review identify changes and improvements?	
Has the organization planned actions to address risks and opportunities and integrated them into the system processes?	Is documented information available to evidence the results of the management review?	
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?		



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?	

Improvement