ISO 22301
Self-assessment questionnaire

How ready are you?

This document has been designed to assess your company's readiness for an ISO 22301 Business Continuity 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 Business Continuity Management System (BCMS)?

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 BCMS and do you review these on a regular basis?

Have you determined the scope of your BCMS and did this take into account the external and internal issues, interested parties, and any activities performed by other organizations?

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 BCMS and have they communicated the importance of an effective BCMS?

Have the policy and objectives for the BCMS, which are compatible with the context and strategic direction of the organization, been established and communicated?

Do the roles carry the authority for ensuring conformance and reporting, as well as the responsibility?

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

Continued >>

Planning

Have the risks and opportunities that need to be addressed to ensure the BCMS can achieve its intended result(s) been established?

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

Have measureable business continuity (BC) objectives been established, documented and communicated throughout the organization with a plan to achieve them?

Support

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

- Is this process consistent with the personnel in the defined BCMS roles?

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

Has the organization ensured that those persons who can affect the performance and effectiveness of the BCMS 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 BCMS?

Operation

Have you devised and implemented a programme to ensure the BCMS achieves its outcomes?

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

Is there a plan for the determining the need for changes to the BCMS 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?

Operation – *continued*

Is there a formal and documented process for understanding the organization through a Business Impact Analysis (BIA)?

Is there a formal process for determining comtinuity objectives based on understanding the impact of disruptive incidents?

Does the BIA enable prioritization of time frames for resuming each activity (Recovery Time Objectives) and have minimum levels for resuming activities that have been identified?

Have these actions been documented?

Is the BC strategy based on the outputs of the BIA and risk assessment?

Does the BC strategy protect prioritized activities and provide appropriate continuity and recovery of them, their dependencies and resources?

Does the BC strategy provide for mitigating, responding to and managing impacts?

Have prioritized time frames been set for the resumption of all activities?

Have the BC capabilities of suppliers been evaluated and mitigated?

Have the resource requirements for the selected strategy options been determined, including people, information and data, infrastructure, facilities, consumables, IT, transport, finance and partner/ supplier services?

Have measures to reduce the likelihood, duration or impact of a disruption for identified risks been considered and implemented, and are these in accordance with the organization's risk appetite?

Have documented BC procedures been put in place to manage a disruptive incident, and have continuity activities based on recovery onjectives been identifed in the BIA?

Have internal and external communication protocols been established as part of these procedures?

Is there an Incident Response Structure (IRS) which details the management structure and trained personnel in place to respond to a disruptive incident?

Does the IRS and associated procedures include thresholds, assessment, activation, resource provision and communication?

Do the people in your IRS have the necessary competencies to perform their duties and are records kept to demonstrate this?

Is there a procedure for detecting and monitoring incidents which included recording vital information, actions taken and decisions made?

Continued >>

Operation – *continued*

Is there a procedure for managing internal and external communications during a disruptive incident?

Is there a procedure for receiving and responding to warnings from outside agencies and emergency responders?

Is there a procedure for issuing alerts and warnings and is this communication regularly exercised and records kept of the results?

Are there documented plans/procedures for restoring business operations after an incident, do they reflect the needs of those who will use them and contain all the essential information they need?

Do the plans define roles and responsibilities and a process for activating the response?

Do the plans consider the management of the immediate consequences of a disruption, in particular the welfare of individuals, options for response and further loss prevention?

Do the plans detail how to communicate with interested parties, including the media during the disruption and how to prioritize activities?

Do the plans include a procedure for standing down the response and returning to normal business?

Have the business continuity procedures been tested, at planned intervals and with appropriate scenarios to ensure they are consistent with your BC objectives?

Have formal post-exercise reports been produced for the tests and outcomes reviewed to ensure they lead to improvement?

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?

Are internal audits conducted periodically to check that the BCMS is effective and conforms to both ISO 22301:2014 and the organization's requirements?

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

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

Performance evaluation – *continued*

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 BCMS?

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

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?

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 BCMS?

Is documented information kept as evidence of the nature of nonconformities, actions taken and the results?

Find out more

Call: +6 03 9212 9638 (Kuala Lumpur)
+6 07 276 3506 (Johor Bahru)
+6 04 227 9651 (Penang)
+6 082 232 003 (Kuching)
Email: info.malaysia@bsigroup.com
Visit: bsigroup.com.my

BSI/UK/852/SC/0516/EN/BLD