

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
4 Context of the organization	.		
<p>4.1 The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its BCMS. These issues shall be taken into account when establishing, implementing and maintaining the organization's BCMS.</p>	<p>The organization shall identify and document the following:</p> <ul style="list-style-type: none"> a) the organization's activities, functions, services, products, partnerships, supply chains, relationships with interested parties, and the potential impact related to a disruptive incident; b) links between the business continuity policy and the organization's objectives and other policies, including its overall risk management strategy; and c) the organization's risk appetite. <p>In establishing the context, the organization shall</p> <ul style="list-style-type: none"> 1) articulate its objectives, including those concerned with business continuity, 2) define the external and internal factors that create the uncertainty that gives rise to risk, 3) set risk criteria taking into account the risk appetite, and 4) define the purpose of the BCMS. 	<p>Documented information required</p>	

ISO 22301:2012 Assessment Checklist

Type:		Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)		Compliance
4.2 Understanding the needs and expectations of interested parties				
4.2.1 General	When establishing its BCMS, the organization shall determine a) the interested parties that are relevant to the BCMS, and b) the requirements of these interested parties (i.e. their needs and expectations whether stated, generally implied or obligatory).			

ISO 22301:2012 Assessment Checklist

Type:		Assessors:		Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance		
4.2.2 Legal and regulatory requirements	<p>The organization shall establish, implement and maintain a procedure(s) to identify, have access to, and assess the applicable legal and regulatory requirements to which the organization subscribes related to the continuity of its operations, products and services, as well as the interests of relevant interested parties.</p> <p>The organization shall ensure that these applicable legal, regulatory and other requirements to which the organization subscribes are taken into account in establishing, implementing and maintaining its BCMS.</p> <p>The organization shall document this information and keep it up-to-date. New or variations to legal, regulatory and other requirements shall be communicated to affected employees and other interested parties</p>	<p>Documented information required</p>			
4.3 Determining the scope of the business continuity management system					

ISO 22301:2012 Assessment Checklist

Type:		Assessors:		Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance		
4.3.1 General	<p>The organization shall determine the boundaries and applicability of the BCMS to establish its scope.</p> <p>When determining this scope, the organization shall consider</p> <ul style="list-style-type: none"> — the external and internal issues referred to in 4.1, and — the requirements referred to in 4.2. <p>The scope shall be available as documented information.</p>	Documented information required			

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
4.3.2 Scope of the BCMS	<p>The organization shall</p> <ul style="list-style-type: none"> a) establish the parts of the organization to be included in the BCMS, b) establish BCMS requirements, considering the organization's mission, goals, internal and external obligations (including those related to interested parties), and legal and regulatory responsibilities, c) identify products and services and all related activities within the scope of the BCMS, d) take into account interested parties' needs and interests, such as customers, investors, shareholders, the supply chain, public and/or community input and needs, expectations and interests (as appropriate), and e) define the scope of the BCMS in terms of and appropriate to the size, nature and complexity of the organization. <p>When defining the scope, the organization shall document and explain exclusions; any such exclusions shall not affect the organization's ability and responsibility to provide continuity of business and operations that meet the BCMS requirements, as determined by business impact analysis or risk assessment and applicable legal or regulatory requirements.</p>	<p>Document and explain exclusions</p>	

ISO 22301:2012 Assessment Checklist

Type:		Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)		Compliance
4.4 Business continuity management system				
	The organization shall establish, implement, maintain and continually improve a BCMS, including the processes needed and their interactions, in accordance with the requirements of this International Standard.			
5 Leadership				
5.1 Leadership and commitment	Persons in top management and other relevant management roles throughout the organization shall demonstrate leadership with respect to the BCMS. EXAMPLE This leadership and commitment can be shown by motivating and empowering persons to contribute to the effectiveness of the BCMS.			

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
5.2 Management commitment	<p>Top management shall demonstrate leadership and commitment with respect to the BCMS by</p> <ul style="list-style-type: none"> — ensuring that policies and objectives are established for the business continuity management system and are compatible with the strategic direction of the organization, — ensuring the integration of the business continuity management system requirements into the organization’s business processes, — ensuring that the resources needed for the business continuity management system are available, — communicating the importance of effective business continuity management and conforming to the BCMS requirements, — ensuring that the BCMS achieves its intended outcome(s), — directing and supporting persons to contribute to the effectiveness of the BCMS, — promoting continual improvement, and — supporting other relevant management roles to demonstrate their leadership and commitment as it applies to their areas of responsibility 		

ISO 22301:2012 Assessment Checklist

Type:		Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)		Compliance
5.3 Policy	<p>Top management shall establish a business continuity policy that</p> <ul style="list-style-type: none"> a) is appropriate to the purpose of the organization, b) provides a framework for setting business continuity objectives, c) includes a commitment to satisfy applicable requirements, d) includes a commitment to continual improvement of the BCMS. <p>The BCMS policy shall</p> <ul style="list-style-type: none"> — be available as documented information, — be communicated within the organization, — be available to interested parties, as appropriate, — be reviewed for continuing suitability at defined intervals and when significant changes occur <p>The organization shall retain documented information on the business continuity policy.</p>	Documented information required		
5.4 Organizational roles, responsibilities and authorities	<p>Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.</p> <p>Top management shall assign the responsibility and authority for</p> <ul style="list-style-type: none"> a) ensuring that the management system conforms to the requirements of this International Standard, and b) reporting on the performance of the BCMS to top management. 			

ISO 22301:2012 Assessment Checklist

Type:		Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)		Compliance
6 Planning				
6.1 Actions to address risks and opportunities	<p>When planning for the BCMS, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to</p> <ul style="list-style-type: none"> — ensure the management system can achieve its intended outcome(s), — prevent, or reduce, undesired effects, — achieve continual improvement. <p>The organization shall plan</p> <ul style="list-style-type: none"> a) actions to address these risks and opportunities, b) how to <ul style="list-style-type: none"> 1) integrate and implement the actions into its BCMS processes (see 8.1), 2) evaluate the effectiveness of these actions (see 9.1). 			

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
6.2 Business continuity objectives and plans to achieve them	<p>Top management shall ensure that business continuity objectives are established and communicated for relevant functions and levels within the organization.</p> <p>The business continuity objectives shall</p> <ul style="list-style-type: none"> a) be consistent with the business continuity policy, b) take account of the minimum level of products and services that is acceptable to the organization to achieve its objectives, c) be measurable, d) take into account applicable requirements, and e) be monitored and updated as appropriate. <p>The organization shall retain documented information on the business continuity objectives.</p> <p>To achieve its business continuity objectives, the organization shall determine</p> <ul style="list-style-type: none"> — who will be responsible, — what will be done, — what resources will be required, — when it will be completed, and — how the results will be evaluated. 	Documented information required	
7 Support			
7.1 Resources	The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the BCMS.		

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
7.2 Competence	<p>The organization shall</p> <ul style="list-style-type: none"> a) determine the necessary competence of person(s) doing work under its control that affects its performance, b) ensure that these persons are competent on the basis of appropriate education, training, and experience, c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken, and d) retain appropriate documented information as evidence of competence. <p>NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the reassignment of current employed persons; or the hiring or contracting of competent persons.</p>	Documented information required	
7.3 Awareness	<p>Persons doing work under the organization's control shall be aware of</p> <ul style="list-style-type: none"> a) the business continuity policy, b) their contribution to the effectiveness of the BCMS, including the benefits of improved business continuity management performance, c) the implications of not conforming with the BCMS requirements, and d) their own role during disruptive incidents. 		

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
7.4 Communication	<p>The organization shall determine the need for internal and external communications relevant to the BCMS including</p> <ul style="list-style-type: none"> a) on what it will communicate, b) when to communicate, c) with whom to communicate. <p>The organization shall establish, implement, and maintain procedure(s) for</p> <ul style="list-style-type: none"> — internal communication amongst interested parties and employees within the organization, — external communication with customers, partner entities, local community, and other interested parties, including the media, — receiving, documenting, and responding to communication from interested parties, — adapting and integrating a national or regional threat advisory system, or equivalent, into planning and operational use, if appropriate, — ensuring availability of the means of communication during a disruptive incident, — facilitating structured communication with appropriate authorities and ensuring the interoperability of multiple responding organizations and personnel, where appropriate, and — operating and testing of communications capabilities intended for use during disruption of normal communications. <p>NOTE Further requirements for communication in response to an incident are specified in 8.4.3.</p>	<p>Documented information required</p>	

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
7.5 Documented information			
7.5.1 General	<p>The organization's BCMS shall include</p> <ul style="list-style-type: none"> — documented information required by this International Standard, and — documented information determined by the organization as being necessary for the effectiveness of the BCMS. <p>NOTE The extent of documented information for a BCMS can differ from one organization to another due to</p> <ul style="list-style-type: none"> — the size of organization and its type of activities, processes, products and services, — the complexity of processes and their interactions, and — the competence of persons. 	<p>The following is a summary of the Documented information requirements. Examples should be given in the relevant sections of this checklist.</p> <ul style="list-style-type: none"> 4.1 Understanding of the organization and its context 4.2.2 Legal and regulatory requirements 4.3 Scope of the BCMS 5.3 Policy 6.2 Business continuity objectives 7.2 Competence 7.4 Communication 7.5 Documented information 8.1 Operational planning and control 8.2 Business impact analysis and risk assessment 8.4 Establish and implement business continuity procedures 9.1 Monitoring, measurement, analysis and evaluation 9.2 Internal audit 9.3 Management review 10.1 Nonconformity and corrective action 	

ISO 22301:2012 Assessment Checklist

Type:		Assessors:		Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance		
7.5.2 Creating and updating	When creating and updating documented information, the organization shall ensure appropriate a) identification and description (e.g. a title, date, author or reference number), b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic), and review and approval for suitability and adequacy.	Documented information required			

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
<p>7.5.3 Control of documented information</p>	<p>Documented information required by the BCMS and by this International Standard shall be controlled to ensure</p> <p>a) it is available and suitable for use, where and when it is needed,</p> <p>b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).</p> <p>For the control of documented information, the organization shall address the following activities, as applicable</p> <ul style="list-style-type: none"> — distribution, access, retrieval and use, — storage and preservation, including preservation of legibility, — control of changes (e.g. version control), — retention and disposition, — retrieval and use, — preservation of legibility (i.e. clear enough to read), and — prevention of the unintended use of obsolete information. <p>Documented information of external origin determined by the organization to be necessary for the planning and operation of the BCMS shall be identified, as appropriate, and controlled.</p> <p>When establishing control of documented information, the organization shall ensure that there is adequate protection for the documented information (e.g. protection against compromise, unauthorized modification or deletion).</p>	<p>Documented information required</p>	

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
	NOTE Access implies a decision regarding the permission to view the documented information, or the permission and authority to view and change the documented information, etc.		
8 Operation			
8.1 Operational planning and control	<p>The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in 6.1, by</p> <ul style="list-style-type: none"> a) establishing criteria for the processes, b) implementing control of the processes in accordance with the criteria, and c) keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned. <p>The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.</p> <p>The organization shall ensure that outsourced processes are controlled.</p>	Documented information required	

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
<p>8.2 Business impact analysis and risk assessment</p> <p>8.2.1 General</p>	<p>The organization shall establish, implement and maintain a formal and documented process for business impact analysis and risk assessment that</p> <ul style="list-style-type: none"> a) establishes the context of the assessment, defines criteria and evaluates the potential impact of a disruptive incident, b) takes into account legal and other requirements to which the organization subscribes, c) includes systematic analysis, prioritization of risk treatments, and their related costs, d) defines the required output from the business impact analysis and risk assessment, and e) specifies the requirements for this information to be kept up-to-date and confidential. <p>NOTE There are various methodologies for business impact analysis and risk assessment which will determine the order in which these will be conducted.</p>	<p>Documented information required</p>	

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
8.3 Business continuity strategy			
8.3.1 Determination and selection	<p>Determination and selection of strategy shall be based on the outputs from the business impact analysis and risk assessment.</p> <p>The organization shall determine an appropriate business continuity strategy for</p> <ul style="list-style-type: none"> a) protecting prioritized activities, b) stabilizing, continuing, resuming and recovering prioritized activities and their dependencies and supporting resources, and c) mitigating, responding to and managing impacts. <p>The determination of strategy shall include approving prioritized time frames for the resumption of activities.</p> <p>The organization shall conduct evaluations of the business continuity capabilities of suppliers.</p>		

ISO 22301:2012 Assessment Checklist

Type:		Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)		Compliance
8.3.2 Establishing resource requirements	<p>The organization shall determine the resource requirements to implement the selected strategies. The types of resources considered shall include but not be limited to</p> <ul style="list-style-type: none"> a) people, b) information and data, c) buildings, work environment and associated utilities, d) facilities, equipment and consumables, e) information and communication technology (ICT) systems, f) transportation, g) finance, and h) partners and suppliers. 			
8.3.3 Protection and mitigation	<p>For identified risks requiring treatment, the organization shall consider proactive measures that</p> <ul style="list-style-type: none"> a) reduce the likelihood of disruption, b) shorten the period of disruption, and c) limit the impact of disruption on the organization's key products and services. <p>The organization shall choose and implement appropriate risk treatments in accordance with its risk appetite.</p>			

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
8.4 Establish and implement business continuity procedures			
8.4.1 General	<p>The organization shall establish, implement, and maintain business continuity procedures to manage a disruptive incident and continue its activities based on recovery objectives identified in the business impact analysis.</p> <p>The organization shall document procedures (including necessary arrangements) to ensure continuity of activities and management of a disruptive incident.</p> <p>The procedures shall</p> <ul style="list-style-type: none"> a) establish an appropriate internal and external communications protocol, b) be specific regarding the immediate steps that are to be taken during a disruption, c) be flexible to respond to unanticipated threats and changing internal and external conditions, d) focus on the impact of events that could potentially disrupt operations, e) be developed based on stated assumptions and an analysis of interdependencies, and f) be effective in minimizing consequences through implementation of appropriate mitigation strategies 	Documented information required	

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
8.4.2 Incident response structure	<p>The organization shall establish, document, and implement procedures and a management structure to respond to a disruptive incident using personnel with the necessary responsibility, authority and competence to manage an incident.</p> <p>The response structure shall</p> <ul style="list-style-type: none"> a) identify impact thresholds that justify initiation of formal response, b) assess the nature and extent of a disruptive incident and its potential impact, c) activate an appropriate business continuity response, d) have processes, and procedures for the activation, operation, coordination, and communication of the response, e) have resources available to support the processes and procedures to manage a disruptive incident in order to minimize impact, and f) communicate with interested parties and authorities, as well as the media. <p>The organization shall decide, using life safety as the first priority and in consultation with relevant interested parties, whether to communicate externally about its significant risks and impacts and document its decision. If the decision is to communicate then the organization shall establish and implement procedures for this external communication, alerts and warnings including the media as appropriate.</p>	<p>Documented information required</p>	

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
8.4.3 Warning and communication	<p>The organization shall establish, implement and maintain procedures for</p> <ul style="list-style-type: none"> a) detecting an incident, b) regular monitoring of an incident, c) internal communication within the organization and receiving, documenting and responding to communication from interested parties, d) receiving, documenting and responding to any national or regional risk advisory system or equivalent, e) assuring availability of the means of communication during a disruptive incident, f) facilitating structured communication with emergency responders, g) recording of vital information about the incident, actions taken and decisions made, and the following shall <p>also be considered and implemented where applicable:</p> <ul style="list-style-type: none"> — alerting interested parties potentially impacted by an actual or impending disruptive incident; — assuring the interoperability of multiple responding organizations and personnel; — operation of a communications facility. <p>The communication and warning procedures shall be regularly exercised.</p>	<p>Documented information required</p>	

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance

8.4.4 Business continuity plans	<p>The organization shall establish documented procedures for responding to a disruptive incident and how it will continue or recover its activities within a predetermined timeframe. Such procedures shall address the requirements of those who will use them.</p> <p>The business continuity plans shall collectively contain</p> <ul style="list-style-type: none"> a) defined roles and responsibilities for people and teams having authority during and following an incident, b) a process for activating the response, c) details to manage the immediate consequences of a disruptive incident giving due regard to <ul style="list-style-type: none"> 1) the welfare of individuals, 2) strategic, tactical and operational options for responding to the disruption, and 3) prevention of further loss or unavailability of prioritized activities; d) details on how and under what circumstances the organization will communicate with employees and their relatives, key interested parties and emergency contacts, e) how the organization will continue or recover its prioritized activities within predetermined timeframes, f) details of the organization's media response following an incident, including <ul style="list-style-type: none"> 1) a communications strategy, 2) preferred interface with the media, 	<p>Documented information required</p>	
--	---	--	--

ISO 22301:2012 Assessment Checklist

Type:		Assessors:		Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)		Compliance	
	3) guideline or template for drafting a statement for the media, and 4) appropriate spokespeople; g) a process for standing down once the incident is over. Each plan shall define — purpose and scope, — objectives, — activation criteria and procedures, — implementation procedures, — roles, responsibilities, and authorities, — communication requirements and procedures, — internal and external interdependencies and interactions, — resource requirements, and — information flow and documentation processes.				
8.4.5 Recovery	The organization shall have documented procedures to restore and return business activities from the temporary measures adopted to support normal business requirements after an incident.	Documented information required			

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
8.5 Exercising and testing			
	<p>The organization shall exercise and test its business continuity procedures to ensure that they are consistent with its business continuity objectives.</p> <p>The organization shall conduct exercises and tests that</p> <ul style="list-style-type: none"> a) are consistent with the scope and objectives of the BCMS, b) are based on appropriate scenarios that are well planned with clearly defined aims and objectives, c) taken together over time validate the whole of its business continuity arrangements, involving relevant interested parties, d) minimize the risk of disruption of operations, e) produce formalized post-exercise reports that contain outcomes, recommendations and actions to implement improvements, f) are reviewed within the context of promoting continual improvement, and g) are conducted at planned intervals and when there are significant changes within the organization or to the environment in which it operates. 		

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
9 Performance evaluation			
9.1 Monitoring, measurement, analysis and evaluation			

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
9.1.1 General	<p>The organization shall determine</p> <ul style="list-style-type: none"> a) what needs to be monitored and measured, b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results, c) when the monitoring and measuring shall be performed, and d) when the results from monitoring and measurement shall be analysed and evaluated. <p>The organization shall retain appropriate documented information as evidence of the results.</p> <p>The organization shall evaluate the BCMS performance and the effectiveness of the BCMS.</p> <p>Additionally, the organization shall</p> <ul style="list-style-type: none"> — take action when necessary to address adverse trends or results before a nonconformity occurs, and — retain relevant documented information as evidence of the results. <p>The procedures for monitoring performance shall provide for</p> <ul style="list-style-type: none"> — the setting of performance metrics appropriate to the needs of the organization, — monitoring the extent to which the organization's business continuity policy, objectives and targets are met, — performance of the processes, procedures and functions that protect its prioritized activities, — monitoring compliance with this International Standard and the business continuity objectives, 	<p>Documented information required</p>	

ISO 22301:2012 Assessment Checklist

Type:		Assessors:		Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance		
	<ul style="list-style-type: none"> — monitoring historical evidence of deficient BCMS' performance, and — recording data and results of monitoring and measurement to facilitate subsequent corrective actions. <p>NOTE Deficient performance could include non-conformity, near misses, false alarms, and actual incidents.</p>				

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
9.1.2 Evaluation of business continuity procedures	<p>a) The organization shall conduct evaluations of its business continuity procedures and capabilities in order to ensure their continuing suitability, adequacy and effectiveness;</p> <p>b) These evaluations shall be undertaken through periodic reviews, exercising, testing, post-incident reporting and performance evaluations. Significant changes arising shall be reflected in the procedure(s) in a timely manner;</p> <p>c) The organization shall periodically evaluate compliance with applicable legal and regulatory requirements, industry best practices, and conformance with its own business continuity policy and objectives; and</p> <p>d) The organization shall conduct evaluations at planned intervals and when significant changes occur.</p> <p>When a disruptive incident occurs and results in the activation of its business continuity procedures, the organization shall undertake a post-incident review and record the results.</p>		

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
9.2 Internal audit	<p>The organization shall conduct internal audits at planned intervals to provide information on whether the business continuity management system</p> <p>a) conforms to</p> <p>1) the organization's own requirements for its BCMS,</p> <p>2) the requirements of this International Standard, and</p> <p>b) is effectively implemented and maintained.</p> <p>The organization shall</p> <ul style="list-style-type: none"> — plan, establish, implement and maintain (an) audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits, — define the audit criteria and scope for each audit, — select auditors and conduct audits to ensure objectivity and the impartiality of the audit process, — ensure that the results of the audits are reported to relevant management, and — retain documented information as evidence of the implementation of the audit programme and the audit results. 	<p>Documented information required</p>	

ISO 22301:2012 Assessment Checklist

Type:		Assessors:		Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance		
	<p>The audit programme, including any schedule, shall be based on the results of risk assessments of the organization's activities, and the results of previous audits. The audit procedures shall cover the scope, frequency, methodologies and competencies, as well as the responsibilities and requirements for conducting audits and reporting results.</p> <p>The management responsible for the area being audited shall ensure that any necessary corrections and corrective actions are taken without undue delay to eliminate detected nonconformities and their causes.</p> <p>Follow-up activities shall include the verification of the actions taken and the reporting of verification results.</p>				

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
9.3 Management review	<p>Top management shall review the organization's BCMS, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.</p> <p>The management review shall include consideration of</p> <ul style="list-style-type: none"> a) the status of actions from previous management reviews, b) changes in external and internal issues that are relevant to the business continuity management system, c) information on the business continuity performance, including trends in <ul style="list-style-type: none"> 1) nonconformities and corrective actions, 2) monitoring and measurement evaluation results, and 3) audit results, d) opportunities for continual improvement. <p>Management reviews shall consider the performance of the organization, including</p> <ul style="list-style-type: none"> — follow-up actions from previous management reviews, — the need for changes to the BCMS, including the policy and objectives, — opportunities for improvement, — results of BCMS audits and reviews, including those of key suppliers and partners where appropriate,. 	<p>Documented information required</p>	

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
	<ul style="list-style-type: none"> — techniques, products or procedures, which could be used in the organization to improve the BCMS' performance and effectiveness, — status of corrective actions, — results of exercising and testing, — risks or issues not adequately addressed in any previous risk assessment, — any changes that could affect the BCMS, whether internal or external to the scope of the BCMS, — adequacy of policy, — recommendations for improvement, — lessons learned and actions arising from disruptive incidents, and — emerging good practice and guidance. <p>The outputs of the management review shall include decisions related to continual improvement opportunities and the possible need for changes to the BCMS, and include the following:</p> <ul style="list-style-type: none"> a) variations to the scope of the BCMS; b) improvement of the effectiveness of the BCMS; c) update of the risk assessment, business impact analysis, business continuity plans and related procedures; d) modification of procedures and controls to respond to internal or external events that may impact on the BCMS, including changes to <ul style="list-style-type: none"> 1) business and operational requirements, 		

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
	2) risk reduction and security requirements, 3) operational conditions and processes, 4) legal and regulatory requirements, 5) contractual obligations, 6) levels of risk and/or criteria for accepting risks, 7) resource needs, 8) funding and budget requirements; and e) how the effectiveness of controls are measured. The organization shall retain documented information as evidence of the results of management reviews. The organization shall — communicate the results of management review to relevant interested parties, and — take appropriate action relating to those results.		

ISO 22301:2012 Assessment Checklist

Type:	Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)	Compliance
10 Improvement			
10.1 Nonconformity and corrective action	When nonconformity occurs, the organization shall <ol style="list-style-type: none"> a) identify the nonconformity, b) react to the nonconformity, and, as applicable, <ol style="list-style-type: none"> 1) take action to control and correct it, and 2) deal with the consequences. c) evaluate the need for action to eliminate the causes of the nonconformity, in order that it does not recur or occur elsewhere, by <ol style="list-style-type: none"> 1) reviewing the nonconformity, 2) determining the causes of the nonconformity, and 3) determining if similar nonconformities exist, or could potentially occur, 4) evaluating the need for corrective action to ensure that nonconformities do not recur or occur elsewhere, 5) determining and implementing corrective action needed, 	Documented information required	

ISO 22301:2012 Assessment Checklist

Type:		Assessors:	Date (s)	
Clause	Requirement	Evidence Sighted (Identify documents or records, e.g. show title, date, author or reference number)		Compliance
	<p>6) reviewing the effectiveness of any corrective action taken and</p> <p>7) making changes to the BCMS, if necessary.</p> <p>d) implement any action needed,</p> <p>e) review the effectiveness of any corrective action taken,</p> <p>f) make changes to the business continuity management system, if necessary.</p> <p>Corrective actions shall be appropriate to the effects of the nonconformities encountered.</p> <p>The organization shall retain documented information as evidence of</p> <ul style="list-style-type: none"> — the nature of the nonconformities and any subsequent actions taken, and — the results of any corrective action. 			
10.2 Continual improvement	<p>The organization shall continually improve the suitability, adequacy or effectiveness of the BCMS.</p> <p>NOTE The organization can use the processes of the BCMS such as leadership, planning and performance evaluation, to achieve improvement.</p>			