

ISO 22301 BCMS - Certified Lead Auditor

GAQM ISO-BCMS-22301

Version Demo

Total Demo Questions: 12

Total Premium Questions: 125

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

PASSQUEEN.COM

support@passqueen.com

QUESTION NO: 1

Which two (2) elements should be included in business continuity procedures for responding to a disruptive incident? (Choose two)

- A. Procedures for communicating with relevant interested parties
- B. Procedures for activating business continuity solutions
- C. Procedures for setting annual sales targets
- D. Procedures for approving personal leave

ANSWER: A B

Explanation:

Procedures for communicating with relevant interested parties and **procedures for activating business continuity solutions** are correct. Effective response procedures need to define how relevant information will be communicated to personnel and other interested parties, including customers, suppliers, authorities, and emergency responders where applicable. They must also enable the organization to activate the continuity strategies and solutions selected to maintain or recover prioritized activities.

Response procedures commonly include assessment, escalation, decision-making, roles, responsibilities, communications, and recovery actions. They should be available to those responsible for using them and be maintained as organizational conditions change. ISO 22301 requires organizations to establish, implement, and maintain procedures for managing disruptive incidents. See [ISO 22301:2019—Business continuity management systems](#).

QUESTION NO: 2

Policy documents are developed in accordance to the framework of objectives.

- A. True
- B. False

ANSWER: B

Explanation:

False is correct because the relationship described is reversed. In an ISO 22301 business continuity management system, top management establishes the business continuity policy first. The policy expresses the organization's commitment to business continuity, is appropriate to the organization's purpose, and provides the framework for setting business continuity objectives. Objectives are then established at relevant functions and levels in a manner consistent with that policy. They should be measurable where practicable, monitored, communicated, updated as appropriate, and supported by planning that identifies actions, resources, responsibilities, completion dates, and evaluation methods.

Therefore, objectives are developed within the direction and framework established by the policy; the policy is not developed according to a pre-existing framework of objectives. This hierarchy ensures that detailed, measurable business continuity targets support the organization's overall strategic intent and commitments. ISO's overview of ISO 22301 describes the standard as a framework for establishing, implementing, maintaining, and continually improving a BCMS: [ISO 22301:2019—Security and resilience](#). Further guidance on management-system policy and objectives is available from [ISO management system standards](#).

QUESTION NO: 3

The probability of a threat or risk to occur is defined as _____

- A. Likelihood
- B. Risk appetite
- C. Control
- D. Impact

ANSWER: A

Explanation:

Likelihood is the correct term for the probability or chance that a threat, event, or risk scenario will occur. In risk assessment, likelihood is evaluated alongside the potential consequence or impact of the event. This combination enables an organization to determine the level of risk and prioritize treatment, controls, monitoring, and business-continuity planning appropriately. Likelihood may be expressed qualitatively, such as rare, unlikely, possible, likely, or almost certain, or quantitatively as an estimated frequency or probability over a specified period. The selected scale should be defined consistently within the organization's risk-assessment methodology so that assessments are repeatable and can support informed decisions. ISO 22301 requires organizations to identify risks that could affect the intended results of the business continuity management system and to plan actions to address them. A sound understanding of likelihood helps auditors assess whether risk identification and evaluation are sufficiently systematic and whether planned BCMS actions are proportionate to the organization's exposure. ISO's risk-management guidance describes risk as the effect of uncertainty on objectives and supports evaluating the characteristics of risk to guide decision-making. See [ISO 31000 risk management](#) and [ISO 22301:2019—Business continuity management systems](#).

QUESTION NO: 4

Support lays out the foundation of planning and managing the BCMS.

- A. True
- B. False

ANSWER: A

Explanation:

True is correct. In ISO 22301, the support requirements provide the enabling foundation that allows a business continuity management system to be planned, implemented, operated, maintained, and improved in a controlled way. Clause 7 addresses the resources the organization must provide, the competence of people performing BCMS-related work, awareness of the business continuity policy and individual contributions, internal and external communications, and the control of documented information. These elements make planning practical and repeatable: plans require capable people, sufficient resources, clear communication channels, and controlled, accessible information.

Support is therefore not merely administrative activity. It establishes the organizational capability needed to manage continuity objectives and to ensure that BCMS processes can be consistently applied and evidenced. For example, documented information supports the availability of approved continuity procedures, while competence and awareness help personnel carry out assigned continuity responsibilities effectively. This aligns with ISO 22301's management-system approach, in which support processes underpin the effective operation and ongoing management of business continuity arrangements. See the [ISO 22301:2019 standard overview](#) and ISO's [business continuity guidance page](#).

QUESTION NO: 5

Which two (2) practices support effective control of documented information within a BCMS? (Choose two)

- A. Ensuring that current versions are available where needed
- B. Protecting documented information from unintended alteration or loss
- C. Allowing uncontrolled changes to incident procedures

D. Using obsolete contact lists as the primary response record

ANSWER: A B

Explanation:

Ensuring that current versions are available where needed and protecting documented information from unintended alteration or loss are correct. Business continuity procedures, contact lists, recovery instructions, and response plans must be accessible to authorized users when they are needed, including during disruption. They must also be protected so that obsolete, corrupted, or unauthorized versions do not undermine response activities.

Documented information control includes appropriate identification, format, review, approval, distribution, access, retrieval, storage, preservation, retention, and disposition. Retaining every superseded document without control, or allowing any employee to change response procedures without authorization, would increase the risk of using incorrect information during an incident. See [ISO 22301:2019](#).

QUESTION NO: 6

Which Resources are involved in Business Continuity to continue critical operations at an acceptable level? (Choose four)

- A. Premises
- B. Information
- C. Technology
- D. Supplies
- E. Data
- F. Knowledge

ANSWER: A B C D

Explanation:

Premises, Information, Technology, and Supplies are essential resource categories that must be considered when planning to sustain critical operations at an acceptable level during disruption. Premises includes the physical locations and facilities from which activities are delivered, including the need for alternate work locations where necessary. Information covers the documented and operational information required to perform, coordinate, and recover priority activities. Technology includes the systems, communications capabilities, equipment, and supporting infrastructure needed to deliver products and services. Supplies includes the materials, consumables, and other inputs on which time-critical activities depend.

ISO 22301 requires an organization to determine and provide the resources needed to establish, implement, maintain, and continually improve its business continuity management system. Business impact analysis and continuity strategies should therefore identify dependencies on facilities, information, technology, and supplies, then establish arrangements that enable those dependencies to remain available or be recovered within required time frames. This supports the standard's objective of ensuring that prioritized products and services can continue through disruptive incidents. See the [ISO 22301:2019 standard overview](#) and the [NIST contingency-planning guidance](#) for continuity-planning context.

QUESTION NO: 7

Which type of review can often used as a secondary method to support other forms of information collection methods?

- A. Documentary review
- B. Visionary review
- C. Personal review
- D. Private review

ANSWER: A

Explanation:

Documentary review is correct because reviewing documented information is commonly used to substantiate, clarify, and corroborate evidence collected through other audit activities, such as interviews, observation, and sampling. In a business continuity management system audit, relevant documents can include the BCMS scope, business impact analysis outputs, risk assessments, continuity strategies, plans, exercise records, incident reports, internal-audit results, and management-review records. Examining these materials enables an auditor to confirm that stated practices are supported by objective evidence and that required processes have been established, implemented, and maintained.

Document review can take place before an audit to prepare the audit team and identify areas requiring attention, as well as during the audit to validate information obtained from personnel and observed operations. This supporting role is especially useful because BCMS effectiveness depends not only on documented arrangements but also on their practical operation and testing. ISO 19011 describes audit evidence as verifiable information and recognizes the review of documented information as an important evidence-gathering activity. ISO 22301 establishes the requirements for a BCMS and provides the context for reviewing the organization's continuity documentation and records. See [ISO 19011:2018 guidance for auditing management systems](#) and [ISO 22301:2019 Security and resilience — Business continuity management systems](#).

QUESTION NO: 8

Which two (2) actions are appropriate when a disruptive incident occurs and business continuity procedures are activated? (Choose two)

- A. Assessing the nature and potential impact of the incident
- B. Communicating with relevant interested parties
- C. Delaying all decisions until normal operations resume
- D. Discarding incident records before review

ANSWER: A B

Explanation:

Assessing the nature and potential impact of the incident and **communicating with relevant interested parties** are correct. Effective response arrangements require the organization to assess the situation, determine whether activation and escalation are necessary, make timely decisions, and coordinate actions to manage the incident. Communications should be appropriate to the incident and directed to relevant personnel, customers, suppliers, authorities, emergency services, or other interested parties.

Business continuity procedures should also support the activation of continuity solutions, allocation of required resources, monitoring of the situation, and recording of decisions and actions. Waiting until all effects are known before making any communication, or allowing staff to use uncontrolled public statements, may delay coordinated response and increase adverse consequences. See [ISO 22301:2019—Business continuity management systems](#) and [ISO business continuity management](#).

QUESTION NO: 9

Corporate Services and Information Technology are the functions that provide a range of physical and technological infrastructure services to all other functions.

- A. True
- B. False

ANSWER: A

Explanation:

“True” is correct. Corporate Services and Information Technology are commonly treated as enabling or support functions because they supply the shared capabilities on which operational and customer-facing functions depend. Corporate Services typically coordinates physical infrastructure and workplace-related resources, such as facilities, utilities, site access, security arrangements, and administrative services. Information Technology provides technological infrastructure, including networks, business applications, end-user devices, data platforms, communications tools, identity services, and technical support.

In a business continuity management system, these functions must be considered carefully because disruption to their services can affect multiple processes simultaneously. ISO 22301 requires organizations to understand activities, resources, dependencies, and disruption impacts when establishing continuity arrangements. Shared physical and technology services are therefore important dependencies to identify through business impact analysis and risk assessment. Continuity strategies should establish how the organization will maintain or restore the required facilities and IT capabilities within agreed timeframes, allowing dependent functions to continue delivering prioritized products and services. This aligns with the ISO overview of [ISO 22301:2019](#) and the business-continuity guidance published by the [UK National Cyber Security Centre](#).

QUESTION NO: 10

Which four factors are considered when designing questionnaires for the BIA?

- A. Concise information
- B. Layout
- C. Types of question
- D. Level of detail
- E. Image and Pictures
- F. Virtualization

ANSWER: A B C D

Explanation:

A business impact analysis (BIA) questionnaire must be designed so that process owners can provide information that is usable, consistent, and sufficiently reliable for determining disruption impacts and recovery priorities. **Concise information** is essential because questions should be direct and understandable, helping respondents supply focused answers without unnecessary effort. The **layout** should make the questionnaire easy to navigate and complete, supporting clear grouping of related topics and reducing the likelihood of missed responses. Selecting appropriate **types of question**, such as structured, scaled, and open questions where needed, enables both comparable impact data and necessary contextual detail. The required **level of detail** must also be carefully set: it needs to capture critical activities, dependencies, impacts, and time-based recovery needs while remaining practical for business representatives to complete accurately. Together, these design factors improve response quality and support a defensible analysis of continuity requirements. ISO 22301 requires the organization to determine the impact of disruption over time and establish priorities and requirements for continuity; a well-designed BIA questionnaire is a common means of collecting this evidence. See [ISO 22301:2019 overview](#) and the [Business Continuity Institute Good Practice Guidelines](#).

QUESTION NO: 11

The actions of the media and press have a profound impact on the long-term performance, or in some cases.

- A. True
- B. False

ANSWER: A

Explanation:

True is correct. During a disruptive incident, media and press coverage can materially affect an organization's reputation, stakeholder confidence, customer retention, and ability to recover commercially. News reporting may shape how customers, regulators, investors, suppliers, employees, and the public perceive both the incident itself and the organization's competence, transparency, and empathy in responding to it. Consequently, business continuity arrangements should account for external communications, including clear responsibilities, approved communication channels, timely escalation, coordinated public statements, and monitoring of public information.

ISO 22301 treats communication as an essential element of a business continuity management system. The organization must determine relevant internal and external communications, including what will be communicated, when, by whom, and through which processes. In a crisis, effective media engagement supports the continuity objective by protecting confidence and helping the organization maintain critical relationships while response and recovery activities proceed. This makes media and press actions capable of having a profound influence on long-term organizational performance and, in severe circumstances, organizational viability. See [ISO 22301:2019—Business continuity management systems](#) and [ISO Online Browsing Platform: ISO 22301](#).

QUESTION NO: 12

Which two (2) activities are expected when the organization establishes business continuity strategies and solutions? (Choose two)

- A. Identifying options for continuity strategies
- B. Determining resources required for selected solutions
- C. Deferring all recovery decisions until disruption occurs
- D. Eliminating the need for business impact analysis

ANSWER: A B

Explanation:

Identifying options for continuity strategies and **determining the resources required to implement selected solutions** are correct. After business impact analysis and risk assessment, the organization needs to identify and select strategies that enable prioritized activities to be maintained or recovered within established requirements. The selected solutions must be supported by realistic resources, including people, facilities, technology, information, equipment, finance, and external services.

Strategies should be evaluated for their ability to meet continuity requirements and should be practicable in the organization's operating context. The organization should not select a solution solely because it has the lowest initial cost, nor should it wait for an incident before determining required recovery resources. See [ISO 22301:2019](#) and [ISO business continuity management overview](#).