EXIN Business Continuity Management

FOUNDATION

Certified by EXIN

Sample Exam

Edition 201607

Content

Introduction

This is the sample exam EXIN Business Continuity Management Foundation (BCMF.EN). The Rules and Regulations for EXIN's examinations apply to this exam.

This exam consists of 40 multiple-choice questions. Each multiple-choice question has a number of possible answers, of which only one is the correct answer.

The maximum number of points that can be obtained for this exam is 40. Each correct answer is worth one point. If you obtain 26 points or more you will pass.

The time allowed for this exam is 60 minutes.

Good luck!

Sample Exam

1 of 40
How should the level of risk for an organization be determined?

A. Combining consequence and likelihood of events
B. Combining importance and acceptance of events
C. Combining acceptable and tolerable events
D. Combining profitability and analysis of events

2 of 40
Business continuity is the capability of an organization to react to disruptions.

What should the Business Continuity Management System (BCMS) be?

A. A part of the organization's IT Management system
B. A part of the organization’s overall management system
C. Always managed by an external service provider
D. Separate from the organization’s overall management system

3 of 40
A Business Continuity Plan helps organizations to operate at what level?

A. 100% of original capabilities
B. Main activities
C. Best effort levels of capabilities
D. Undetermined levels of capabilities

4 of 40
Of which process should Business Continuity programs be a part?

A. Incident Management process
B. Compliance process
C. Governance process
D. Problem Management process

5 of 40
What should the scope of the BCMS be to understand the needs and expectations of interested parties?

A. At least the main business processes
B. Only services including the IT department
C. All of the organization's profitable services

6 of 40
What are the two levels of BCMS objectives?

A. Legal and Regulatory
B. Operational and Tactical
C. Strategic and Tactical
D. Tactical and Operational

7 of 40
When determining the scope of the BCMS, what is true?

A. The scope only relates to the internal needs of the organization.
B. The scope should always cover the whole organization.
C. The scope should document and explain any exclusions.
D. The scope should never be changed.

8 of 40
Top management shall establish a business continuity policy that is appropriate and provides a framework for setting business continuity objectives.

How often should BCM policies be reviewed?

A. Annually
B. Monthly
C. Quarterly
D. Regularly

9 of 40
Top management should demonstrate its commitment to the BCMS.

What should BCMS Leadership ensure?

A. Requirements are integrated in the organization's business processes.
B. Information technology suppliers' contracts support IT needs.
C. Incidents that affect service availability are addressed immediately.

10 of 40
How should the top management demonstrate its commitment to the BCMS?

A. appoint a business continuity manager
B. conduct effective management reviews of the BCMS
C. ensure that BCM objectives are aligned to the strategic goals of the business
D. hire external expertise regarding BCM

11 of 40
Policies are mandated by an organization that will always be performed according to a preset design plan, and supporting all business functions within an organization.

What is the definition of a BCMS policy?

A. A statement by management of what the organization should do.
B. Information required to be controlled and maintained by an organization, defined by its top management.
C. Intentions and direction of an organization as formally expressed by its top management.
D. Ongoing management and governance process document, set by top management.

12 of 40
BCMS should be demonstrated.

What are BCMS Leaders responsible for?

A. Ensuring policies and objectives are established.
B. Implementing of BCMS technology for continuity.
C. Monitoring how BCMS documents are reviewed.

13 of 40
A BCMS policy statement is a good place to set out the objectives and adherence to the policy will ensure compliance. What should the BCMS policy contain?

A. Compatibility with the strategic direction of the organization
B. Definition of key performance indicators to monitor during a disaster
C. Critical success factors for improvement of objectives

14 of 40
Executive leadership is essential at every stage of the BCMS project.

What are the responsibilities of top management in establishing a BCMS?

A. Compatibility with the strategic direction of the organization
B. Invocation for activating response to incidents
C. Objectives with detailed aspects
D. Power of execution

15 of 40
Risk Appetite is a method to help guide an organization's approach to risk and risk management.

What does the term risk appetite refer to?

A. Amount and type of risk to test, validate, or change
B. Amount and type of risk to accept, tolerate or pursue
C. Amount and type of risk to remove, refer or investigate
D. Amount and type of risk to identify, analyze or evaluate

16 of 40
The overall process regarding risk assessment is identification, analysis and evaluation.

What is mandatory?

A. A document called Risk Assessment Report
B. Risk assessment sheets or information collected through risk assessment tool
C. Risk assessment policy document

17 of 40
Regarding business continuity awareness and training, what document is mandatory to determine competence and effectiveness of performance?

A. A Training Plan
B. A business continuity strategy
C. A document called Awareness raising plan
D. A risk assessment policy

18 of 40
The organization should nominate incident response personnel with the necessary responsibility, authority and competence to manage an incident.

How may Incident response personnel be assigned to the different teams?

A. Based on demonstrated competence
B. Based on management skills and experience
C. Based on their role in the organization

19 of 40
Different training types may be appropriate for specific roles.

What type of training subject is appropriate for people involved in setting up and managing the BCMS?

A. Communication skills
B. Delivering presentations at conferences and seminars
C. Incident assessment skills

20 of 40
The organization should establish, implement and maintain procedures for warning and communication.

What procedure needs to be established for Warning and Incident communication for BCM?

A. Procedure for detecting, analysis, responding and correcting
B. Procedure for interpreting, escalating, maintaining and improving
C. Procedure for organizing, prioritizing, approving and implementing
D. Procedure for detecting, monitoring, sharing and recording information

21 of 40
What is one of the five BCM elements within operations?

A. Establish and implement business continuity procedures
B. External audit to evaluate business continuity procedures
C. Management review to evaluate continuity suitability

22 of 40
The organization should determine, plan, implement and control those operational activities needed to fulfill its business continuity policy and objectives.

What process is recommended for controlling those activities?

A. Application Management
B. Project Management
C. Incident Management
D. Service Level Management

23 of 40
Which recognized management method should an organization adopt to ensure that the establishment of the BCMS is effectively managed?

A. Business Continuity Management
B. Business Impact Analysis
C. Project Management
D. Risk Management

24 of 40
Management has overall responsibility for the creation, funding, review, and maintenance of an effective business continuity management system.

What is one of the key management good practices for managing an effective business continuity capability?

A. An incident management capability is enabled and provides an effective response.
B. Conduct regular management reviews.
C. Regular exercising ensures that staff are trained to respond effectively to an incident or disruption.
D. Staff receive adequate support and communications in the event of a disruption.

25 of 40
What is **not** one of the outcomes indicative of an effective Business Continuity program?

A. The impact of a disruption on the organization's key services is limited.
B. The likelihood of a disruption is reduced.
C. The period of disruption is shortened.
D. The organization´s supply chain is secured.

26 of 40
The organization should establish a formal evaluation process for determining continuity and recovery priorities and objectives.

What is one of the purposes of the Business Impact Analysis (BIA)?

A. to determine the business continuity strategy
B. to determine minimal acceptable outage
C. to identify risks

27 of 40
What is a type of impact over time related to the business that may be addressed in the BIA?

A. damage to reputation
B. damage to the facility of a third party
C. disruption of the critical business processes only

28 of 40
What is one of the options an organization has to consider when developing the BIA methodology?

A. Ceasing or changing a business activity if viable alternatives are available.
B. Establishing alternate processes or creating redundancy/spare capacity in processes.
C. Time scales for assessment
D. Transferring a business activity to a third party.

29 of 40
Business impact analysis gives an idea about the timing of the recovery and the timing of the backup.

How is the timing of the backup determined?

A. Via Maximum Acceptable Outage (MAO)
B. Via Recovery Time Objective (RTO)
C. Via Recovery Point Objective (RPO)
D. Via Single Point Of Failure (SPOF)

30 of 40
What is an element that should be included in the BIA in the context of ISO 31000 (a standard for Risk Assessment)?

A. Assessment of recovery priorities
B. Identification of dependencies between activities
C. Identification of treatments

31 of 40
When assessing potential impacts over time of disruptions during the business impact analysis, which ones should the organization consider?

A. Internal and external sources
B. Related to its business aims and objectives and its interested parties
C. The organization's key products services
D. The organization's reputation

32 of 40
When identifying risks of disruptive incidents, how are single points of failure (SPOF), inadequacies in fire protection, electrical resilience, staffing levels, IT security and IT resilience considered?

A. Impacts
B. Risks
C. Threats
D. Vulnerabilities

33 of 40
An organization should provide appropriate procedures to respond to unanticipated threats and changing internal and external conditions and ensure that its activities continue based on their identified recovery objectives in the BIA.

How should those business continuity procedures be perceived?

A. Flexible
B. Proactive
C. Smart
D. Strict

34 of 40
An organization should put in place procedures that will enable it to prepare for, mitigate and respond effectively to disruptive incidents.

How could all aspects of incident response be handled in smaller organizations?

A. A tiered approach to incident response may be used.
B. It may be handled by one team or an individual but the response should never be the responsibility of a single individual.
C. Special arrangements may be required for ensuring the effectiveness of communication with interested parties.
D. The warning and communication system should be regularly exercised.

35 of 40
The organization shall exercise and test its business continuity procedures to ensure that they are consistent with its business continuity objectives.

Who should make decisions about the method, scope, objectives and timing regarding exercising and testing a Business Continuity Plan?

A. Process owners
B. The IT manager
C. Top management

36 of 40
All business continuity plans should be concise and accessible to those with responsibilities defined within them. There may be several business continuity plans which collectively meet the needs of the business.

What should every plan contain?

A. The response procedure containing details of actions and tasks that need to be performed by management.
B. The response procedure to address issues at all levels - strategic, tactical or operational options.
C. The response procedure should include management of welfare issues where appropriate.
D. The response procedure should include who has the authority, and what is the method of activating and deactivating plans.

37 of 40
The organization exercises and tests its business continuity procedures to ensure that they are consistent with its business continuity objectives.

Which method can be used for exercising and testing the Business continuity plan?

A. Activate Incident response plans and Recovery plans verbally
B. Desk check
C. E-learning
D. Report incidents via a help desk application

38 of 40
The organization determines the performance that needs to be monitored, measured and evaluated.

What is a crucial prerequisite for measurement?

A. Business Continuity policy
B. Business Continuity objectives
C. Provide training to achieve the desired level of knowledge and skills
D. Setting the scope of your BCMS

39 of 40
The organization should conduct internal audits at planned intervals to discover nonconformities. What is a requirement for the internal audit program of the BCMS?

A. It should always cover the full scope of the BCMS.
B. It should be based on the full scope of the BCMS.
C. It should include all staff.

40 of 40
The organization should identify nonconformities, take action to control, contain and correct them, deal with the consequences and evaluate the need for action.

What should be the basis for determining the priority of corrective actions?

A. Results of the Incident log
B. Results of an Internal audit
C. Results of the Management review
D. Results of the risk assessment and impact analysis

Answer Key

1/40

How should the level of risk for an organization be determined?

A. Combining consequence and likelihood of events
B. Combining importance and acceptance of events
C. Combining acceptable and tolerable events
D. Combining profitability and analysis of events

A. Correct. Determining the level of risk directly, or through consequences and likelihood. Once you identify the risks, you need to know how high they are – for example, you can use the scale of 1 to 5, where 1 would be very low, 2 low, 3 medium, etc.; alternatively, you can choose to assess consequences and likelihood – e.g., using the same scale of 1 to 5, the likelihood of fire is low (2); however, the consequences would be very high (5) – in such approach the level of risk would be a calculated result of consequences and likelihood (see below "Method of risk calculation"). Again, assessing risk directly is quicker, but assessing consequences and likelihood will give a more precise result and it will be compliant with the information security risk assessment if you choose to do it afterwards. *Becoming Resilient, chapter 6.2 and ISO 22301, clauses 8.2.1 and 8.2.3*

B. Incorrect. This is not a risk determination method.
C. Incorrect. This is not a risk determination method.
D. Incorrect. This is not a risk determination method.

2/40
Business continuity is the capability of an organization to react to disruptions.

What should the Business Continuity Management System (BCMS) be?

A. A part of the organization's IT Management system
B. A part of the organization’s overall management system
C. Always managed by an external service provider
D. Separate from the organization’s overall management system

A. Incorrect. The Business Continuity Management System (BCMS) is part of the overall company activities that focuses not only on implementing, but also maintaining and improving business continuity. Just as companies have, e.g., financial management with various rules and responsibilities, business continuity has certain policies, procedures, processes, etc. that are part of the BCMS.
B. Correct. The Business Continuity Management System (BCMS) is part of the overall company activities that focuses not only on implementing, but also maintaining and improving business continuity. Just as companies have, e.g., financial management with various rules and responsibilities, business continuity has certain policies, procedures, processes, etc. that are part of the BCMS. *Becoming Resilient, chapter 2.2 Terminology*
C. Incorrect. The Business Continuity Management System (BCMS) is part of the overall company activities that focuses not only on implementing, but also maintaining and improving business continuity. Just as companies have, e.g., financial management with various rules and responsibilities, business continuity has certain policies, procedures, processes, etc. that are part of the BCMS.
D. Incorrect. The Business Continuity Management System (BCMS) is part of the overall company activities that focuses not only on implementing, but also maintaining and improving business continuity. Just as companies have, e.g., financial management with various rules and responsibilities, business continuity has certain policies, procedures, processes, etc. that are part of the BCMS.

3/40

A Business Continuity Plan helps organizations to operate at what level?

A. 100% of original capabilities
B. Main activities
C. Best effort levels of capabilities
D. Undetermined levels of capabilities

A. Incorrect. The Business continuity plan (BCP) is a document (or, more often, a set of documents) that describes how to respond to an incident, and how to continue an organization's main activities within the Recovery Time Objective. You could also consider BCPs as checklists on what you need to do if your activities are disrupted.
B. Correct. The Business continuity plan (BCP) is a document (or, more often, a set of documents) that describes how to respond to an incident, and how to continue an organization's main activities within the Recovery Time Objective. You could also consider BCPs as checklists on what you need to do if your activities are disrupted. *Becoming resilient, chapter 2.2 Terminology and 6.9: Business continuity plan (clause 8.4)*
C. Incorrect. The Business continuity plan (BCP) is a document (or, more often, a set of documents) that describes how to respond to an incident, and how to continue an organization's main activities within the Recovery Time Objective. You could also consider BCPs as checklists on what you need to do if your activities are disrupted.
D. Incorrect. The Business continuity plan (BCP) is a document (or, more often, a set of documents) that describes how to respond to an incident, and how to continue an organization's main activities within the Recovery Time Objective. You could also consider BCPs as checklists on what you need to do if your activities are disrupted.

4/40

Of which process should Business Continuity programs be a part?

A. Incident Management process
B. Compliance process
C. Governance process
D. Problem Management process

A. Incorrect. Ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.
B. Incorrect. Ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.
C. Correct. Ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management. *ISO22301, clause 3.7*
D. Incorrect. Ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.

5/40
What should the scope of the BCMS be to understand the needs and expectations of interested parties?

A. At least the main business processes
B. Only services including the IT department
C. All of the organization's profitable services

A. Correct. A BCMS scope must cover your whole company (or at least your main business processes), *Becoming Resilient, chapter 5.4, ISO 22301 clause 4.3*
B. Incorrect. If your scope only includes the IT department, you still depend on the inputs from the business part of your organization which means you will have to perform business impact analysis (see section 6.6) for your business departments also. So, in reality, you didn't save as much as you perhaps intended. *Becoming Resilient, chapter 5.4*
C. Incorrect. Your scope document should include not only physical locations that are part of the scope, but also products and services you are delivering, activities and processes, and requirements that are relevant for setting the scope. Becoming Resilient, chapter 5.4

6/40
What are the two levels of BCMS objectives?

A. Legal and Regulatory
B. Operational and Tactical
C. Strategic and Tactical
D. Tactical and Operational

A. Incorrect. Options Documentation. There are at least two levels for which you need to set objectives: Strategic objectives and Tactical objectives
B. Incorrect. Options Documentation. There are at least two levels for which you need to set objectives: Strategic objectives and Tactical objectives
C. Correct. Options Documentation. There are at least two levels for which you need to set objectives: Strategic objectives – for your whole Business Continuity Management System, and Tactical objectives – Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), Minimum Business Continuity Objectives (MBCOs), and exercising and testing objectives. *Becoming Resilient, chapter 5.6, ISO 22301 clause 6.2*
D. Incorrect. Options Documentation. There are at least two levels for which you need to set objectives: Strategic objectives and Tactical objectives

7/40

When determining the scope of the BCMS, what is true?

A. The scope only relates to the internal needs of the organization.
B. The scope should always cover the whole organization.
C. The scope should document and explain any exclusions.
D. The scope should never be changed.

A. Incorrect. Where part of an organization is excluded from the scope of its BCMS, the organization should document and explain the exclusion.
B. Incorrect. Where part of an organization is excluded from the scope of its BCMS, the organization should document and explain the exclusion.
C. Correct. Where part of an organization is excluded from the scope of its BCMS, the organization should document and explain the exclusion. *Becoming Resilient, appendix B and ISO 22301, clause 4.3.2.*
D. Incorrect. Where part of an organization is excluded from the scope of its BCMS, the organization should document and explain the exclusion.

8/40

Top management shall establish a business continuity policy that is appropriate and provides a framework for setting business continuity objectives.

How often should BCM policies be reviewed?

A. Annually
B. Monthly
C. Quarterly
D. Regularly

A. Incorrect. The policy must be regularly reviewed – an owner of a policy should be defined, and this person is responsible for keeping the policy up to date.
B. Incorrect. The policy must be regularly reviewed – an owner of a policy should be defined, and this person is responsible for keeping the policy up to date.
C. Incorrect. The policy must be regularly reviewed – an owner of a policy should be defined, and this person is responsible for keeping the policy up to date.
D. Correct. The policy must be regularly reviewed – an owner of a policy should be defined, and this person is responsible for keeping the policy up to date. *Becoming Resilient, chapter 5.5 and ISO 22301, clause 5.3*

9/40
Top management should demonstrate its commitment to the BCMS.

What should BCMS Leadership ensure?

A. Requirements are integrated in the organization's business processes.
B. Information technology suppliers' contracts support IT needs.
C. Incidents that affect service availability are addressed immediately.

A. Correct. Ensuring the integration of the business continuity management system requirements into the organization's business processes. *ISO 22301, clause 5.2*
B. Incorrect. This is part of the Business Impact Analysis. *Becoming Resilient, chapter 6.5 and ISO 22301, clause 8.2.2*
C. Incorrect. This is part of the incident response process. *Becoming Resilient, chapter 6.11 and ISO 22301, clause 8.4.2*

10/40
How should the top management demonstrate its commitment to the BCMS?

A. appoint a business continuity manager
B. conduct effective management reviews of the BCMS
C. ensure that BCM objectives are aligned to the strategic goals of the business
D. hire external expertise regarding BCM

A. Incorrect. Whilst this may be a useful and necessary step, it is not key in showing top management commitment.
B. Incorrect. Whilst this is an important role for top management, it is not specifically one that demonstrates commitment.
C. Correct. ISO 22301 requires the management to ensure that BCMS is compatible with the strategic direction of the organization. *Becoming Resilient, chapter 5.5 and* Top management shall demonstrate leadership and commitment with respect to the BCMS by ensuring that policies and objectives are established for the business continuity management system and are compatible with the strategic direction of the organization, *ISO 22301, clause 5.2*
D. Incorrect. The organization may invite any external resources that may be involved in a response – such as Fire, Police, Public Health and third party vendors – to review with management relevant parts of its business continuity procedures. *ISO 22313, clause 7.4*

11/40
Policies are mandated by an organization that will always be performed according to a preset design plan, and supporting all business functions within an organization.

What is the definition of a BCMS policy?

A. A statement by management of what the organization should do.
B. Information required to be controlled and maintained by an organization, defined by its top management.
C. Intentions and direction of an organization as formally expressed by its top management.
D. Ongoing management and governance process document, set by top management.

A. Incorrect. This is not the definition of a policy
B. Incorrect. This is the definition of documented information.
C. Correct. The main purpose of the policy is that the top management defines what it wants to achieve with business continuity. *Becoming Resilient, chapter 5.5 and ISO 22301, clause 3.38*
D. Incorrect. This is the definition of a Business Continuity Program.

12/40
BCMS should be demonstrated.

What are BCMS Leaders responsible for?

A. Ensuring policies and objectives are established.
B. Implementing of BCMS technology for continuity.
C. Monitoring how BCMS documents are reviewed.

A. Correct. Ensuring that policies and objectives are established for the business continuity management system and are compatible with the strategic direction of the organization. *Becoming Resilient, chapter 5.5 and ISO 22301, clause 5.2*
B. Incorrect. Implementing technology is a responsibility of technology staff and not a responsibility of the management.
C. Incorrect. This is addressed in ISO 22301, clause 7.5.2 – create and update documented information.

13/40
A BCMS policy statement is a good place to set out the objectives and adherence to the policy will ensure compliance. What should the BCMS policy contain?

A. Compatibility with the strategic direction of the organization
B. Definition of key performance indicators to monitor during a disaster
C. Critical success factors for improvement of objectives

A. Correct. Basically, the Business continuity policy should actually serve as a main link between your top management and your business continuity activities, especially because ISO 22301 requires the management to ensure that "BCMS is compatible with the strategic direction of the organization" (clause 5.2). The policy is probably the best way to do this. *Becoming Resilient, chapter 5.5*
B. Incorrect. This is part of ISO 22301 clause 9.1.1 Monitoring, measurement, analysis and evaluation
C. Incorrect. This is part of ISO 22301 clause 9.1.1 Monitoring, measurement, analysis and evaluation

14/40
Executive leadership is essential at every stage of the BCMS project.

What are the responsibilities of top management in establishing a BCMS?

A. Compatibility with the strategic direction of the organization
B. Invocation for activating response to incidents
C. Objectives with detailed aspects
D. Power of execution

A. Correct. Basically, the Business continuity policy should actually serve as a main link between your top management and your business continuity activities, especially because ISO 22301 requires the management to ensure that "BCMS is compatible with the strategic direction of the organization" (clause 5.2). The policy is probably the best way to do this. *Becoming Resilient, chapter 5.5*
B. Incorrect. Invocation is a process for activating the organization's response to a disruptive incident and within each documented procedure, its activation criteria and procedures. *ISO 22301, clause 3.23*
C. Incorrect. Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). *ISO 22301, clause 3.32*
D. Incorrect. ISO 22301 requires the management to ensure that "BCMS is compatible with the strategic direction of the organization" (clause 5.2).

15/40
Risk Appetite is a method to help guide an organization's approach to risk and risk management.

What does the term risk appetite refer to?

A. Amount and type of risk to test, validate, or change
B. Amount and type of risk to accept, tolerate or pursue
C. Amount and type of risk to remove, refer or investigate
D. Amount and type of risk to identify, analyze or evaluate

A. Incorrect. Amount and type of risk that an organization is willing to pursue or retain. *ISO 22301, clause 3.49.*
B. Correct. Amount and type of risk that an organization is willing to pursue or retain. *ISO 22301, clause 3.49.*
C. Incorrect. Amount and type of risk that an organization is willing to pursue or retain. *ISO 22301, clause 3.49.*
D. Incorrect. Amount and type of risk that an organization is willing to pursue or retain. *ISO 22301, clause 3.49.*

16/40
The overall process regarding risk assessment is identification, analysis and evaluation.

What is mandatory?

A. A document called Risk Assessment Report
B. Risk assessment sheets or information collected through risk assessment tool
C. Risk assessment policy document

A. Incorrect. A document called Risk assessment report may be produced; sometimes it is called Risk assessment and risk treatment report if it also includes the results from risk treatment. If you have already done a risk assessment according to ISO 27001 project, use those documents. *Becoming Resilient, chapter 6.3*
B. Correct. Documentation Tip (mandatory) Risk assessment sheets or information collected through risk assessment tool. *Becoming Resilient, chapter 6.3*
C. Incorrect. This document does not exist in ISO 22301.

17/40
Regarding business continuity awareness and training, what document is mandatory to determine competence and effectiveness of performance?

A. A Training Plan
B. A business continuity strategy
C. A document called Awareness raising plan
D. A risk assessment policy

A. Correct. Personnel records (mandatory, for each employee individually), or a document called Training plan – this plan can be merged together with the awareness document, so then you can call it Training and Awareness Plan. *Becoming Resilient, chapter 5.7 and ISO 22301, clauses 7.2 and 7.3*
B. Incorrect. This is not mandatory for the awareness and training process.
C. Incorrect. This is not mandatory for the awareness and training process.
D. Incorrect. This is not mandatory for the awareness and training process.

18/40
The organization should nominate incident response personnel with the necessary responsibility, authority and competence to manage an incident.

How may Incident response personnel be assigned to the different teams?

A. Based on demonstrated competence
B. Based on management skills and experience
C. Based on their role in the organization

A. Correct. Personnel may be assigned to teams according to their demonstrated competence of dealing with different aspects of incident response, e.g., Incident management/strategic management; Communications; Safety and welfare; Salvage and security; Resuming activities; Recovery of ICT. All personnel who are in these groups should have clearly defined responsibilities and authorities that apply before, during and after an incident. *ISO 22313, clause 7.1.3*
B. Incorrect. Personnel may be assigned to teams according to their demonstrated competence of dealing with different aspects of incident response, e.g., Incident management/ strategic management; Communications; Safety and welfare; Salvage and security; Resuming activities; Recovery of ICT. All personnel who are in these groups should have clearly defined responsibilities and authorities that apply before, during and after an incident. *ISO 22313, clause 7.1.3*
C. Incorrect. Personnel may be assigned to teams according to their demonstrated competence of dealing with different aspects of incident response, e.g., Incident management/ strategic management; Communications; Safety and welfare; Salvage and security; Resuming activities; Recovery of ICT. All personnel who are in these groups should have clearly defined responsibilities and authorities that apply before, during and after an incident. *ISO 22313, clause 7.1.3*

19/40
Different training types may be appropriate for specific roles.

What type of training subject is appropriate for people involved in setting up and managing the BCMS?

A. Communication skills
B. Delivering presentations at conferences and seminars
C. Incident assessment skills

A. Correct. The type of training appropriate for setting up and managing the BCMS is Communication skills. *ISO 22313, clause 7.2 a) 4)*
B. Incorrect. This is part of demonstrating the awareness of BCM trends. *ISO 22313, clause 7.2 Competence*
C. Incorrect. This is appropriate for specific roles in incident response and business recovery.

20/40
The organization should establish, implement and maintain procedures for warning and communication.

What procedure needs to be established for Warning and Incident communication for BCM?

A. Procedure for detecting, analysis, responding and correcting
B. Procedure for interpreting, escalating, maintaining and improving
C. Procedure for organizing, prioritizing, approving and implementing
D. Procedure for detecting, monitoring, sharing and recording information

A. Incorrect. Procedures are detecting an incident; regular monitoring of an incident; internal communication within the organization and receiving, documenting and responding to communication from interested parties; recording of vital information about the incident, actions taken and decisions made. *ISO 22313, clause 8.4.3.*
B. Incorrect. Procedures are detecting an incident; regular monitoring of an incident; internal communication within the organization and receiving, documenting and responding to communication from interested parties; recording of vital information about the incident, actions taken and decisions made. *ISO 22313, clause 8.4.3*.
C. Incorrect. Procedures are detecting an incident; regular monitoring of an incident; internal communication within the organization and receiving, documenting and responding to communication from interested parties; recording of vital information about the incident, actions taken and decisions made. *ISO 22313 clause 8.4.3.*
D. Correct. Detecting an incident and alerting response personnel; continuing monitoring of an incident; internal communication between the various levels and functions within the organization; external communications with interested parties; recording of vital information about the incident, actions taken and decisions made.. *ISO 22313, clause 8.4.3.1*

21/40

What is one of the five BCM elements within operations?

A. Establish and implement business continuity procedures
B. External audit to evaluate business continuity procedures
C. Management review to evaluate continuity suitability

A. Correct. *Becoming Resilient, appendix C – PDCA-cycle and ISO 22313, clause 8.1.1* d) *and clause 8.3*
B. Incorrect. An External audit is not one of the five BCM elements.
C. Incorrect. A Management review is not one of the five BCM elements.

22/40

The organization should determine, plan, implement and control those operational activities needed to fulfill its business continuity policy and objectives.

What process is recommended for controlling those activities?

A. Application Management
B. Project Management
C. Incident Management
D. Service Level Management

A. Incorrect. Application management is the process of managing the operation, maintenance, versioning and upgrading of an application throughout its lifecycle.
B. Correct. The organization should use an appropriate project or program methodology to ensure that business continuity is well managed from the outset. *Becoming Resilient, chapter 4.2*
C. Incorrect. Incident management is a term describing the activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence.
D. Incorrect. Service Level Management is the process that forms the link between the organization and its customers and suppliers. It handles the monitoring and management of the quality of service of the organization's key performance indicators.

23/40
Which recognized management method should an organization adopt to ensure that the establishment of the BCMS is effectively managed?

A. Business Continuity Management
B. Business Impact Analysis
C. Project Management
D. Risk Management

A. Incorrect. Business Continuity Management (BCM) is a management process that identifies risk, threats and vulnerabilities that could impact an entity's continued operations and provides a framework for building organizational resilience and the capability for an effective response.
B. Incorrect. Business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency.
C. Correct. The organization may adopt a recognized project management method to ensure that the BCM program is effectively managed. *Becoming Resilient, chapter 4.2 and ISO 22313, clause 8.1.2*
D. Incorrect. Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Risk management's objective is to assure uncertainty does not deflect the endeavor from the business goals.

24/40
Management has overall responsibility for the creation, funding, review, and maintenance of an effective business continuity management system.

What is one of the key management good practices for managing an effective business continuity capability?

A. An incident management capability is enabled and provides an effective response.
B. Conduct regular management reviews.
C. Regular exercising ensures that staff are trained to respond effectively to an incident or disruption.
D. Staff receive adequate support and communications in the event of a disruption.

A. Incorrect. That is one of the outcomes indicative of an effective business continuity program. *ISO 22313, clause 8.1.5*
B. Correct. Managing an effective BCMS includes regular review of all aspects of the BCMS by management. *Becoming Resilient, chapter 7.6 and ISO 22301, clause 9.3*
C. Incorrect. That is one of the outcomes indicative of an effective business continuity program. *ISO 22313, clause 8.1.5*
D. Incorrect. That is one of the outcomes indicative of an effective business continuity program. *ISO 22313, clause 8.1.5*

25/40

What is **not** one of the outcomes indicative of an effective Business Continuity program?

A. The impact of a disruption on the organization's key services is limited.
B. The likelihood of a disruption is reduced.
C. The period of disruption is shortened.
D. The organization´s supply chain is secured.

A. Incorrect. The BIA and risk assessment should enable the organization to identify measures that limit the impact of a disruption on the organization's key services. *Becoming Resilient, chapter 6.4*
B. Incorrect. The BIA and risk assessment should enable the organization to identify measures that reduce the likelihood of a disruption. *Becoming Resilient, chapter 6.4*
C. Incorrect. The BIA and risk assessment should enable the organization to identify measures that shorten the period of disruption. *Becoming Resilient, chapter 6.4*
D. Correct. Outcomes indicative of an effective Business Continuity program do not necessarily include that the organization´s supply chain is secured. *ISO 22313, clause 8.1.5*

26/40

The organization should establish a formal evaluation process for determining continuity and recovery priorities and objectives.

What is one of the purposes of the Business Impact Analysis (BIA)?

A. to determine the business continuity strategy
B. to determine minimal acceptable outage
C. to identify risks

A. Correct. The BIA together with the Risk assessment form the main input into developing the business continuity strategy. *Becoming resilient, chapter 6.5 and ISO 22313, clauses 8.2.1 and 8.2.2*
B. Incorrect. This is to determine the maximum acceptable outage (MAO). *Becoming resilient, chapter 6.5 and ISO 22313, clause 8.2.2*
C. Incorrect. This is part of a Risk assessment.

27/40

What is a type of impact over time related to the business that may be addressed in the BIA?

A. damage to reputation
B. damage to the facility of a third party
C. disruption of the critical business processes only

A. Correct. A question to ask in the BIA questionnaire is "How will the disruption influence the loss of reputation?" *Becoming Resilient, chapter 6.6 (Impact assessment and figure 9) and ISO 22313, clause 8.2.2*
B. Incorrect. This is not an issue because this is the responsibility of the third party itself.
C. Incorrect. All processes included in the scope of BCMS are investigated when performing a BIA. *ISO 22313, clause 8.2.2 a)*

28/40

What is one of the options an organization has to consider when developing the BIA methodology?

A. Ceasing or changing a business activity if viable alternatives are available.
B. Establishing alternate processes or creating redundancy/spare capacity in processes.
C. Time scales for assessment
D. Transferring a business activity to a third party.

A. Incorrect. The organization should determine appropriate strategy options in their business continuity strategy for protecting prioritized activities after the BIA. These may be targeted at ceasing or changing the activity if viable alternatives are available.
B. Incorrect. The organization should determine appropriate strategy options in their business continuity strategy for stabilizing, continuing, resuming and recovering prioritized activities and their dependencies and supporting resources after the BIA. Continuity options may include alternate processes and spare capacity.
C. Correct. The point of business impact analysis is to assess the impact of a disruption of an activity throughout time – therefore, you need to find appropriate time scales for assessment. *Becoming Resilient, chapter 6.5 and ISO 22301, clause 8.2.2*
D. Incorrect. The organization should determine appropriate strategy options in their business continuity strategy for protecting prioritized activities after the BIA. These may be targeted at transferring the activity to a third party (though the responsibility remains with the organization).

29/40

Business impact analysis gives an idea about the timing of the recovery and the timing of the backup.

How is the timing of the backup determined?

A. Via Maximum Acceptable Outage (MAO)
B. Via Recovery Time Objective (RTO)
C. Via Recovery Point Objective (RPO)
D. Via Single Point Of Failure (SPOF)

A. Incorrect. Determining the Maximum Acceptable Outage (MAO) for each activity (BS 25999-2 called this Maximum tolerable period of disruption (MTPD)) is the first step of determining the timing of recovery.
B. Incorrect. Determine the Recovery Time Objective (RTO) for each activity is the second step of determining the timing of recovery.
C. Correct. The timing of the backup is determined via Recovery Point Objective (RPO), or Maximum Data Loss as ISO 22301 calls it – this is basically the maximum amount of data that can be lost for a particular database or application or a particular type of data, and you have to set the frequency of your backup accordingly. *Becoming Resilient, chapter 6.5*
D. Incorrect. A single point of failure is a characteristic of an activity that depends on a single resource that is not replaceable, and the failure of such resource can cause a disruption of the whole activity.

30/40
What is an element that should be included in the BIA in the context of ISO 31000 (a standard for Risk Assessment)?

A. Assessment of recovery priorities
B. Identification of dependencies between activities
C. Identification of treatments

A. Incorrect. This is part of the BIA and the Business Continuity Strategy.
B. Incorrect. This is part of the BIA.
C. Correct. Decide on which risks need treatment. *Becoming resilient, chapter 6.2 and ISO 22313, clause 8.2.3*

31/40
When assessing potential impacts over time of disruptions during the business impact analysis, which ones should the organization consider?

A. Internal and external sources
B. Related to its business aims and objectives and its interested parties
C. The organization's key products services
D. The organization's reputation

A. Incorrect. The purpose of the BIA is to obtain an understanding of the organization's key products services and the activities that deliver them.
B. Correct. When assessing impacts, the organization should primarily consider those relating to its business aims and objectives and its interested parties. *ISO 22313, clause 8.2.2*
C. Incorrect. The purpose of the BIA is to identify these.
D. Incorrect. For some organization's this might be the primary driver, but this is not true of all organizations everywhere.

32/40
When identifying risks of disruptive incidents, how are single points of failure (SPOF), inadequacies in fire protection, electrical resilience, staffing levels, IT security and IT resilience considered?

A. Impacts
B. Risks
C. Threats
D. Vulnerabilities

A. Incorrect. Impact is an evaluated consequence of a particular effect due to the cause, such as a threat.
B. Incorrect. Risk is the effect of uncertainty on objectives. *ISO 22301, clause 3.48*
C. Incorrect. Specific threats may be described as events or actions which could, at some point, cause an impact to the resources, e.g. threats such as fire, flood, power failure, staff loss, staff absenteeism, computer viruses and hardware failure.
D. Correct. Vulnerabilities might occur as weaknesses within the resources and may, at some point be exploited by the threats, e.g., single points of failure, inadequacies in fire protection, electrical resilience, staffing levels, IT security and IT resilience. *Becoming Resilient, chapter 6.2 and ISO 22313, clause 8.2.3*

33/40
An organization should provide appropriate procedures to respond to unanticipated threats and changing internal and external conditions and ensure that its activities continue based on their identified recovery objectives in the BIA.

How should those business continuity procedures be perceived?

A. Flexible
B. Proactive
C. Smart
D. Strict

A. Correct. The business continuity procedures shall "be flexible to respond to unanticipated threats". *ISO 22301, clause 8.4.1*
B. Incorrect. The business continuity procedures shall "be flexible to respond to unanticipated threats". *ISO 22301, clause 8.4.1*
C. Incorrect. The business continuity procedures shall "be flexible to respond to unanticipated threats". *ISO 22301, clause 8.4.1*
D. Incorrect. The business continuity procedures shall "be flexible to respond to unanticipated threats". *ISO 22301, clause 8.4.1*

34/40
An organization should put in place procedures that will enable it to prepare for, mitigate and respond effectively to disruptive incidents.

How could all aspects of incident response be handled in smaller organizations?

A. A tiered approach to incident response may be used.
B. It may be handled by one team or an individual but the response should never be the responsibility of a single individual.
C. Special arrangements may be required for ensuring the effectiveness of communication with interested parties.
D. The warning and communication system should be regularly exercised.

A. Incorrect. Larger or complex organizations may use a tiered approach to incident response and may establish different teams to focus on incident response, incident management, communications, welfare, business continuity and business recovery issues. *ISO 22313, clause 8.4.2*
B. Correct. In smaller organizations all aspects of incident response may be handled by one team but should never be the responsibility of a single individual. *ISO 22313, clause 8.4.2*
C. Incorrect. This is part of the implementation and maintenance of procedures for warning and communication for all types of organizations. *ISO 22313, clause 8.4.3*
D. Incorrect. This is part of the implementation and maintenance of procedures for warning and communication for all types of organizations. *ISO 22313, clause 8.4.3*

35/40
The organization shall exercise and test its business continuity procedures to ensure that they are consistent with its business continuity objectives.

Who should make decisions about the method, scope, objectives and timing regarding exercising and testing a Business Continuity Plan?

A. Process owners
B. The IT manager
C. Top management

A. Incorrect. The IT manager, process owners and department heads should be consulted before a decision can be made by Top management.
B. Incorrect. The IT manager, process owners and department heads should be consulted before a decision can be made by Top management.
C. Correct. Since exercising and testing are extremely important, and might influence daily operations, the decisions about the method, scope, objectives and timing should be made by the top management. *Becoming resilient, chapter 7.1 and ISO 22301 clause 8.5*

36/40
All business continuity plans should be concise and accessible to those with responsibilities defined within them. There may be several business continuity plans which collectively meet the needs of the business.

What should every plan contain?

A. The response procedure containing details of actions and tasks that need to be performed by management.
B. The response procedure to address issues at all levels - strategic, tactical or operational options.
C. The response procedure should include management of welfare issues where appropriate.
D. The response procedure should include who has the authority, and what is the method of activating and deactivating plans.

A. Incorrect. This is not required in every plan.
B. Incorrect. This is not required in every plan.
C. Incorrect. This is not part of every plan.
D. Correct. Collectively, all business continuity procedures should contain the Invocation and standing down elements, where each response procedure should as appropriate identify meeting locations with alternatives. *Becoming Resilient, figure 15*

37/40
The organization exercises and tests its business continuity procedures to ensure that they are consistent with its business continuity objectives.

Which method can be used for exercising and testing the Business continuity plan?

A. Activate Incident response plans and Recovery plans verbally
B. Desk check
C. E-learning
D. Report incidents via a help desk application

A. Incorrect. That is a best practice method in crisis management. *Becoming Resilient, chapter 6.10*
B. Correct. Desk check – checking the plans by means of auditing, validation and verification techniques; conducted with plan author and moderator. *Becoming Resilient, chapter 7.1 and ISO 22301, clause 8.5.*
C. Incorrect. E-Learning can be a method for raising awareness of Business Continuity and train the employees.
D. Incorrect. A helpdesk application is one of the methods for reporting an incident.

38/40
The organization determines the performance that needs to be monitored, measured and evaluated.

What is a crucial prerequisite for measurement?

A. Business Continuity policy
B. Business Continuity objectives
C. Provide training to achieve the desired level of knowledge and skills
D. Setting the scope of your BCMS

A. Incorrect. The main purpose of the Business continuity policy is that top management defines what it wants to achieve regarding business continuity.
B. Correct. A crucial prerequisite for measurement are business continuity objectives – the key idea is to measure what is achieved compared to these objectives. *Becoming Resilient, chapter 7.4 and ISO 22031, clause 9.1.1.*
C. Incorrect. This is a method which is used for achieving competence in business continuity.
D. Incorrect. The scope of your BCMS relates to which areas are within the scope and which are outside the scope of the BCMS.

39/40
The organization should conduct internal audits at planned intervals to discover nonconformities. What is a requirement for the internal audit program of the BCMS?

A. It should always cover the full scope of the BCMS.
B. It should be based on the full scope of the BCMS.
C. It should include all staff.

A. Incorrect. This is not a requirement.
B. Correct. *Becoming Resilient, chapter 7.5 and ISO 22313 clause 9.2*;
C. Incorrect. This is not a requirement.

40/40
The organization should identify nonconformities, take action to control, contain and correct them, deal with the consequences and evaluate the need for action.

What should be the basis for determining the priority of corrective actions?

A. Results of the Incident log
B. Results of an Internal audit
C. Results of the Management review
D. Results of the risk assessment and impact analysis

A. Incorrect. The purpose of such list is to understand better what is going on, and to be able to understand the relationship between seemingly unrelated incidents. Such incident log should contain a shorter version of the information listed in a Post-incident review form/report.
B. Incorrect. Internal audits can enable you to discover problems (i.e., nonconformities) that would otherwise stay hidden and would therefore harm your business.
C. Incorrect. Management review is where the standard asks your top management to participate actively in decisions that have a major impact on your BCMS.
D. Correct. The priority of corrective actions should be determined based on the results of the risk assessment and impact analysis. *ISO 22313, clause 10.1 Nonconformity and corrective action*

Evaluation

The table below shows the correct answers to the questions in this sample exam.

Question	Answer	Question	Answer
1	A	21	A
2	B	22	B
3	B	23	C
4	C	24	B
5	A	25	D
6	C	26	A
7	C	27	A
8	D	28	C
9	A	29	C
10	C	30	C
11	C	31	B
12	A	32	D
13	A	33	A
14	A	34	B
15	B	35	C
16	B	36	D
17	A	37	B
18	A	38	B
19	A	39	B
20	D	40	D

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER