

Neueste CBCP-002 Pass Guide & neue Prüfung CBCP-002 braindumps & 100% Erfolgsquote



Laden Sie die neuesten ZertFragen CBCP-002 PDF-Versionen von Prüfungsfragen kostenlos von Google Drive herunter:
https://drive.google.com/open?id=1aBKv2VbW-r9XKmO7XigRIz_32dI2vcAR

Wir suchen die Methode des Erfolgs, aber nicht die Ausrede des Misserfolgs. Um zu garantieren, dass die Prüfungsunterlagen der GAQM CBCP-002 für Sie am verlässlichsten ist, haben die IT-Profis von ZertFragen seit Jahren die Prüfungsaufgaben der GAQM CBCP-002 sorgfältig analysiert und die ausführliche Erklärungen geordnet. Die Zertifizierung der GAQM CBCP-002 ist der überzeugende Beweis für Ihre IT-Fähigkeit und wird in Ihrem Berufsleben eine große Rolle spielen.

Nach erfolgreichem Abschluss der CBCP-002 Prüfung erhalten Kandidaten das Zertifikat Certified Business Continuity Professional (CBCP). Diese Zertifizierung ist weltweit anerkannt und zeigt, dass die Person über das Wissen und die Fähigkeiten verfügt, um effektive Business Continuity-Pläne zu entwickeln und umzusetzen. Es ist ein wertvolles Zeugnis für Fachleute, die in Branchen arbeiten, die eine robuste Business Continuity-Management erfordern.

>> CBCP-002 Zertifizierung <<

Die seit kurzem aktuellsten Certified Business Continuity Professional (CBCP) Prüfungsunterlagen, 100% Garantie für Ihren Erfolg in der GAQM CBCP-002 Prüfungen!

Die echten und originalen Prüfungsfragen und Antworten zu CBCP-002 (Certified Business Continuity Professional (CBCP)) bei ZertFragen wurden verfasst von unseren GAQM-Experten mit den Informationen von CBCP-002 (Certified Business Continuity Professional (CBCP)) aus dem Testcenter wie PROMETRIC oder VUE.

GAQM Certified Business Continuity Professional (CBCP) CBCP-002 Prüfungsfragen mit Lösungen (Q28-Q33):

28. Frage

Which of the following should NOT be released in a publicly released BCP?

- A. Process flows
- **B. All of the above**
- C. Contact lists
- D. BIA results

Antwort: B

Begründung:

Explanation

A publicly released BCP is a version of a business continuity plan that is intended for external audiences, such as customers, suppliers, partners, regulators, media, or the public. It should not contain sensitive or confidential information that may compromise the security or privacy of the organization or its stakeholders.

Therefore, it should not include process flows that detail how each function or process is performed; contact lists that reveal personal or organizational information; BIA results that show criticality ratings or recovery time objectives; or any other information that may expose vulnerabilities or risks. Verified References:

<https://www.ready.gov/business-continuity-plan><https://drii.org/resources/professionalpractices/EN>

29. Frage

Which of the following are three components of business continuity plan? (Choose three)

- A. Problem management
- B. Business recovery
- C. Disaster recovery
- D. Incident management
- E. Emergency response

Antwort: B,C,E

Begründung:

A Business Continuity Plan (BCP) is designed to ensure an organization can maintain or resume critical functions during and after a disruption. According to Business Continuity Professional standards, such as those from DRI International and ISO 22301, the BCP typically encompasses three core components that address different phases of response and recovery:

* A. Emergency response: This component focuses on the immediate actions taken during a disruption (e.g., evacuation, safety measures, and initial coordination). It is a foundational part of the BCP, ensuring personnel and asset safety as a prerequisite to continuity and recovery efforts.

* B. Incident management: While incident management (handling and resolving incidents) is critical in broader crisis management frameworks, it is often considered a distinct process under an Incident Response Plan (IRP) rather than a core BCP component. It overlaps with BCP but is not universally listed as one of the three primary elements.

* C. Problem management: This is an IT service management process (e.g., under ITIL) focused on identifying and resolving the root causes of incidents. It is not a standard component of a BCP, which prioritizes continuity and recovery over long-term problem resolution.

* D. Business recovery: This involves restoring critical business functions and processes after a disruption, ensuring the organization can resume normal operations. It is a central pillar of the BCP, addressing recovery time objectives (RTOs) and operational continuity.

* E. Disaster recovery: This focuses on recovering IT systems, data, and infrastructure following a disaster. Often integrated into the BCP, it ensures technological continuity, making it a key component alongside business recovery and emergency response.

The verified answer is A. Emergency response, D. Business recovery, E. Disaster recovery, as these three components collectively cover the lifecycle of a BCP—immediate response, business function restoration, and IT recovery—per established standards. While incident management is related, it is typically supplementary rather than a core BCP element when narrowed to three components.

References:

* DRI International Professional Practices for Business Continuity Management (2023), Section 6:

Business Continuity Plan Development - Identifies emergency response, business recovery, and disaster recovery as key BCP components.

* ISO 22301:2019, Clause 8.4 - Outlines planning for response (emergency), continuity (business recovery), and IT recovery (disaster recovery) as integral to BCP.

30. Frage

Which of the following four are action approach crisis and post-crisis management? (Choose four R's)

- A. Readiness
- B. Reduction
- C. Risk Feed
- D. Recovery
- E. Rustic
- F. Response

Antwort: A,B,D,F

Begründung:

The four R's are action approaches for crisis and post-crisis management. They are:

- * Reduction: This approach aims to prevent or mitigate the occurrence or impact of a crisis by identifying and addressing the root causes, vulnerabilities, and risks.
- * Readiness: This approach aims to prepare for a potential crisis by developing plans, policies, procedures, systems, teams, and resources that can enable a timely and effective response.
- * Response: This approach aims to manage a crisis by activating the plans, policies, procedures, systems, teams, and resources that can contain, control, and resolve the situation.
- * Recovery: This approach aims to restore normal operations after a crisis by implementing actions that can repair damages, restore functions and processes, resume services and products, recover losses, and learn lessons. Verified References: <https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-business-continuity.html> <https://phoenixnap.com/blog/what-is-business-continuity-management>

31. Frage

Individual accountability for the management of the risk should be clearly established.

- A. True
- B. False

Antwort: A

Begründung:

Explanation

Individual accountability for the management of the risk should be clearly established. This is true because accountability is one of the key principles of business continuity management. Accountability means that each person involved in the business continuity management program has a clear understanding of their roles and responsibilities, as well as the authority and resources to perform them. Accountability also means that each person is held responsible for their actions and outcomes, and that they report on their performance and progress regularly. Verified References:

<https://www.iso.org/publication/PUB100442.html> <https://phoenixnap.com/blog/what-is-business-continuity-management>

32. Frage

Which of the following can threats be considered? (Choose three)

- A. Operational failure
- B. Supply chain failure
- C. Technology failure
- D. Fire
- E. Water

Antwort: C,D,E

Begründung:

Threats can be considered any events or situations that can cause harm or disruption to an organization's functions or processes. Threats can be natural, human-made, or technological in origin. Some examples of threats are water (such as floods, leaks, or spills), technology failure (such as system crashes, cyberattacks, or power outages), and fire (such as arson, accidents, or explosions).

Verified References: <https://www.iso.org/publication/PUB100442.html>

<https://phoenixnap.com/blog/what-is-business-continuity-management>

33. Frage

.....

In dieser dynamischen Welt lohnt sich, etwas für berufliche Weiterentwicklung zu tun. Angesichts des Fachkräftemangels in vielen Branchen haben Sie mit einer GAQM CBCP-002 (Certified Business Continuity Professional (CBCP)) Zertifizierung mehr Kontrolle über Ihren eigenen Werdegang und damit bessere Aufstiegschancen.

CBCP-002 Online Prüfung: https://www.zertfragen.com/CBCP-002_pruefung.html

- BONUS!!!** Laden Sie die vollständige Version der ZertFragen CBCP-002 Prüfungsfragen kostenlos herunter:
https://drive.google.com/open?id=1aBKv2VbW-r9XKM07XigRlZ_32d12vcAR

BONUS!!! Laden Sie die vollständige Version der ZertFragen CBCP-002 Prüfungsfragen kostenlos herunter:
https://drive.google.com/open?id=1aBKv2VbW-r9XKM07XigRlZ_32d12vcAR