1. **Which disaster recovery plan test involves functional representatives meeting to review the plan in detail?**



* + Parallel test
  + Checklist test
  + Simulation test
  + Structured walk-through test

1. **What assesses potential loss that could be caused by a disaster?**



* + The Business Impact Analysis (BIA)
  + The Business Assessment (BA)
  + The Risk Assessment (RA)
  + The Business Continuity Plan (BCP)

1. **A Business Impact Analysis (BIA) does NOT:**



* + Estimate the financial and operational impact of a disruption.
  + Determine critical and necessary business functions and their resource dependencies.
  + Identify critical computer applications and the associated outage tolerance.
  + Recommend the appropriate recovery solution.

1. **What is NOT one of the drawbacks of hot sites?**



* + The hot sites are available immediately or within maximum tolerable downtime (MTD)
  + Full redundancy in hardware, software, communication lines and applications is very expensive
  + They are administratively resource intensive, as transaction redundacy controls need to be implemented to keep data up-to-date
  + Need Security controls, as it usually contain mirrored copies of live production data

1. **Who should direct short-term recovery actions immediately following a disaster?**



* + Chief Operating Officer.
  + Chief Information Officer.
  + Disaster Recovery Manager.
  + Chief Executive Officer.

1. **Which one of the following is NOT one of the outcomes of a vulnerability analysis?**



* + Formal approval of BCP scope and initiation document
  + Qualitative loss assessment
  + Quantative loss assessment
  + Defining critical support areas

1. **What is the MOST critical piece to disaster recovery and continuity planning?**



* + Staff training
  + Security policy
  + Availability of backup information processing facilities
  + Management support

1. **A Business Continuity Plan should be tested:**



* + At least once every two years.
  + At least once a year.
  + At least twice a year.
  + Once a month.

1. **Qualitative loss resulting from the business interruption does NOT usually include:**



* + Loss of competitive advantage or market share
  + Loss of market leadership
  + Loss of revenue
  + Loss of public confidence and credibility

1. **What is the LEAST expensive alternative providing processing facilities in case a disaster should strike?**



* + Cold site
  + Reciprocal agreement
  + Hot site
  + Warm site

1. **Which does NOT necessarily have to be a part of the BCP committee?**



* + Legal Department
  + IT Department
  + Business Units
  + Human Resources

1. **What assesses potential loss that could be caused by a disaster?**



* + The Business Impact Analysis (BIA)
  + The Business Assessment (BA)
  + The Risk Assessment (RA)
  + The Business Continuity Plan (BCP)

1. **Which of the following alternative business recovery strategies would be LEAST reliable in a large database and on-line communications network environment where the critical business continuity period is 7 days ?**



* + Reciprocal agreement
  + Hot site
  + Redundant or Alternate Site
  + Warm site

1. **The MAIN advantage of using hot sites is:**



* + Costs associated with this solution are relatively low.
  + Hot sites do not require that equipment and systems software be compatible with the primary installation being backed up.
  + Hot sites can be made ready for operation within a short period of time.
  + Hot sites can be used for an extended amount of time.

1. **Which primary element of BCP includes carrying out vulnerability analysis?**



* + Scope and Plan Initiation
  + Plan Approval and Implementation
  + Business Continuity Plan Development
  + Business Impact Assessment

1. **Which of the following could lead to the conclusion that the disaster recovery plan may NOT be operational within the timeframe the business needs to recover?**



* + Critical recovery priority levels are not defined
  + Offsite backups are located away from the alternate site.
  + The alternate site is a warm site.
  + The alternate site is located 70 miles away from the primary site

1. **Which of the following steps is NOT one of the eight detailed steps of a Business Impact Assessment (BIA):**



* + Calculating the risk for each different business function.
  + Creating data gathering techniques.
  + Identifying critical business functions.
  + Notifying senior management of the start of the assessment.

1. **Which of the following computer recovery sites is only partially equipped with processing equipment?**



* + cold site.
  + warm site.
  + rolling hot site.
  + hot site.

1. **Of the reasons why a Disaster Recovery plan gets outdated, which of the following is not true?**



* + Large plans can take a lot of work to maintain
  + Personnel turnover
  + Continous auditing makes a Disaster Recovery plan irrelevant
  + Infrastructure and environment changes

1. **Which of the following focuses on sustaining an organization's *business functions* during and after a disruption?**



* + Disaster recovery plan
  + Business recovery plan
  + Continuity of operations plan
  + Business continuity plan

1. Question: 1518 | Difficulty: 5/5 | Relevancy: 3/3

**Which of the following statements is the most important assumption behind the warm site concept?**

* + The warm site is partially configured with selected network equipments and peripheral devices.
  + Heat, ventilation and air conditioning are installed at the warm site.
  + **›The main equipment can be obtained quickly for emergency installation at a warm site.**
  + The choice of a warm site is less expensive than that of a hot site.

Sorry - you had a wrong answer. Please review details below.

|  |  |
| --- | --- |
| Details | Submit a comment on [this question](http://www.freepracticetests.org/quiz/qcomment.php?q=1518) |

All the above statements pertaining to warm sites are true, but the main assumption behind warm sites is that the main equipment (computers) can be obtained quickly should the need arise. What makes a warm site less expensive than a hot site is the fact that it is not normally equipped with the costly main computer equipment. A warm site can prove a good alternative to a hot site, provided that the computer equipment can be replaced in timely matter to support critical functions.  
Source: [Information Systems Audit and Control Association](http://www.isaca.org/pubs2.htm), **Certified Information Systems Auditor 2002 review manual**, Chapter 5: Disaster Recovery and Business Continuity (page 253).

**Contributor:** Christian Vezina

**Study area:** **CISSP CBK - BCP and DRP**

**Covered topic:** [Alternate sites](javascript:void(0))

This question © Copyright 2003–2010 Christian Vezina, cccure.org. All rights reserved. No unauthorized use or duplication without explicit written permission of author and of cccure.org.

1. Question: 299 | Difficulty: 3/5 | Relevancy: 3/3

**Which of the following is covered under Crime Insurance Policy Coverage?**

* + Inscribed, printed and Written documents
  + Manuscripts
  + Accounts Receivable
  + **›Money and Securities**

Sorry - you had a wrong answer. Please review details below.

|  |  |
| --- | --- |
| Details | Submit a comment on [this question](http://www.freepracticetests.org/quiz/qcomment.php?q=299) |

Source: TIPTON, Harold F. & KRAUSE, MICKI, [Information Security Management Handbook, 4th Edition, Volume 1](http://www.amazon.com/exec/obidos/ASIN/0849398290/thecisspopens-20), Property Insurance overview, Page 589.

Edited: July 17, 2007, by Mike Young, CISSP

**Contributor:** Jamil Siddique

**Study area:** **CISSP CBK - BCP and DRP**

**Covered topic:** Insurance

This question © Copyright 2003–2010 Jamil Siddique, cccure.org. All rights reserved. No unauthorized use or duplication without explicit written permission of author and of cccure.org.

1. Question: 1169 | Difficulty: 3/5 | Relevancy: 3/3

**During the salvage of the Local Area Network and Servers, which of the following steps would normally be performed first?**

* + Damage mitigation
  + Install LAN communications network and servers
  + ›Assess damage to LAN and servers
  + Recover equipment

Congratulations, you got the correct answer! Details can be reviewed below.

|  |  |
| --- | --- |
| Details | Submit a comment on [this question](http://www.freepracticetests.org/quiz/qcomment.php?q=1169) |

The first activity in every recovery plan is damage assessment, immediately followed by damage mitigation.

This first activity would typically include assessing the damage to all network and server components (including cables, boards, file servers, workstations, printers, network equipment), making a list of all items to be repaired or replaced, selecting appropriate vendors and relaying findings to Emergency Management Team.

Following damage mitigation, equipment can be recovered and LAN communications network and servers can be reinstalled.

Source: BARNES, James C. & ROTHSTEIN, Philip J., [A Guide to Business Continuity Planning](http://www.amazon.com/exec/obidos/ASIN/0471530158/thecisspopens-20), John Wiley & Sons, 2001 (page 135).

Thanks to Guy Albertini for providing feedback to improve this question.

**Contributor:** Christian Vezina

**Study area:** **CISSP CBK - BCP and DRP**

**Covered topic:** [Recovery strategy](javascript:void(0))

This question © Copyright 2003–2010 Christian Vezina, cccure.org. All rights reserved. No unauthorized use or duplication without explicit written permission of author and of cccure.org.

1. Question: 1164 | Difficulty: 5/5 | Relevancy: 3/3

**During the course of a Business Impact Analysis (BIA) you will less likely:**

* + Estimate the financial and operational impacts of a disruption.
  + Identify regulatory exposure.
  + ›Determine a function's Recovery Time Objective (RTO).
  + Determine the impact upon the organization's market share and corporate image.

Congratulations, you got the correct answer! Details can be reviewed below.

|  |  |
| --- | --- |
| Details | Submit a comment on [this question](http://www.freepracticetests.org/quiz/qcomment.php?q=1164) |

During the BIA process, you will evaluate the risk of business process failures and identify critical and necessary business functions and their resource dependencies.

You will also estimate the financial and operational impacts of a disruption, identify regulatory/compliance exposure and determine the impact upon the organization's market share and corporate image.

The determination of each business function's Recovery Time Objectives is one of the results of BIA, therefore not performed during the course of it.

The BIA will be submitted to management and management will decide if they wish to implement a BCP or DRP and they will also decide what will be the scope of recovery.  The RTO would be defined as part of the recovery plan and not as part of the BIA.

Source: BARNES, James C. & ROTHSTEIN, Philip J., [A Guide to Business Continuity Planning](http://www.amazon.com/exec/obidos/ASIN/0471530158/thecisspopens-20), John Wiley & Sons, 2001 (page 68).

Special thanks to Michael Lee for providing input to improve this question.  
Thanks to Vince Martinez for providing feedback on a typo with the explanations.

**Contributor:** Christian Vezina

**Study area:** **CISSP CBK - BCP and DRP**

**Covered topic:** [Business Impact Assessment (BIA)](javascript:void(0))

This question © Copyright 2003–2010 Christian Vezina, cccure.org. All rights reserved. No unauthorized use or duplication without explicit written permission of author and of cccure.org.

1. Question: 1516 | Difficulty: 3/5 | Relevancy: 3/3

**Which of the following statements pertaining to disaster recovery is incorrect?**

* + A recovery team's primary task is to get the pre-defined critical business functions at the alternate backup processing site.
  + A salvage team's task is to ensure that the primary site returns to normal processing conditions.
  + The disaster recovery plan should include how the company will return from the alternate site to the primary site.
  + ›When returning to the primary site, the most critical applications should be brought back first.

Congratulations, you got the correct answer! Details can be reviewed below.

|  |  |
| --- | --- |
| Details | Submit a comment on [this question](http://www.freepracticetests.org/quiz/qcomment.php?q=1516) |

It's interesting to note that the steps to resume normal processing operations will be different than the steps in the recovery plan; that is, the least critical work should be brought back first to the primary site.  
*My explanation: at the point where the primary site is ready to receive operations again, less critical systems should be brought back first because one has to make sure that everything will be running smoothly at the primary site before returning critical systems, which are already operating normally at the recovery site. This will limit the possible interruption of processing to a minimum for most critical systems, thus making it the best option.*  
Source: KRUTZ, Ronald L. & VINES, Russel D., [The CISSP Prep Guide: Mastering the Ten Domains of Computer Security](http://www.amazon.com/exec/obidos/ASIN/0471413569/thecisspopens-20), John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 291).

**Contributor:** Christian Vezina

**Study area:** **CISSP CBK - BCP and DRP**

**Covered topic:** [Relocation to primary site](javascript:void(0))

This question © Copyright 2003–2010 Christian Vezina, cccure.org. All rights reserved. No unauthorized use or duplication without explicit written permission of author and of cccure.org.

1. Question: 1159 | Difficulty: 4/5 | Relevancy: 3/3

**Which of the following statements pertaining to the maintenance of an IT contingency plan is incorrect?**

* + The plan should be reviewed at least once a year for accuracy and completeness.
  + **›The Contingency Planning Coordinator should make sure that every employee gets an up-to-date copy of the plan.**
  + Strict version control should be maintained.
  + Copies of the plan should be provided to recovery personnel for storage at home and office.

Sorry - you had a wrong answer. Please review details below.

|  |  |
| --- | --- |
| Details | Submit a comment on [this question](http://www.freepracticetests.org/quiz/qcomment.php?q=1159) |

Because the contingency plan contains potentially sensitive operational and personnel information, its distribution should be marked accordingly and controlled.

Not all employees should obtain a copy, but only those involved in the plan.

All other statements are correct.

Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), [NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems](http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf), December 2001 (page 26).

**Contributor:** Christian Vezina

**Study area:** **CISSP CBK - BCP and DRP**

**Covered topic:** [Elements of contingency planning](javascript:void(0))

This question © Copyright 2003–2010 Christian Vezina, cccure.org. All rights reserved. No unauthorized use or duplication without explicit written permission of author and of cccure.org.

1. Question: 110 | Difficulty: 3/5 | Relevancy: 3/3

**Which of the following recovery plan test results would be most useful to management?**

* + elapsed time to perform various activities.
  + ›list of successful and unsuccessful activities.
  + amount of work completed.
  + description of each activity.

Congratulations, you got the correct answer! Details can be reviewed below.

|  |  |
| --- | --- |
| Details | Submit a comment on [this question](http://www.freepracticetests.org/quiz/qcomment.php?q=110) |

**The correct answer is:** *list of successful and unsuccessful activities.*

After a test has been performed the **most** useful test results for manangemwnt would be knowing what worked and what didn't so that they could correct the mistakes where needed.

**The following answers are incorrect:**

***elapsed time to perform various activities.*** This is incorrect because it is **not** the best answer, these results are not as useful as list of successful and unsuccessful activities would be to managment.

***amount of work completed.*** This is incorrect because it is **not** the best answer, these results are not as useful as list of successful and unsuccessful activities would be to managment.

***description of each activity.*** This is incorrect because it is **not** the best answer, these results are not as useful as list of successful and unsuccessful activities would be to managment.

Last modified 6/08/2007 - J. Hajec

**Comment:**

**References:**

OIG CBK Business Continuity and Disaster Recovery Planning (pages 389 - 390)

**Study area:** **CISSP CBK - BCP and DRP**

**Covered topic:** [Contigency planning testing](javascript:void(0))

This question © Copyright 2003–2010 cccure.org. All rights reserved. No unauthorized use or duplication without explicit written permission of author and of cccure.org.

1. Question: 1163 | Difficulty: 2/5 | Relevancy: 3/3

**Which of the following would best help an organization to gain a common understanding of functions that are critical to its survival?**

* + A risk assessment
  + A business assessment
  + A disaster recovery plan
  + ›A business impact analysis

Congratulations, you got the correct answer! Details can be reviewed below.

|  |  |
| --- | --- |
| Details | Submit a comment on [this question](http://www.freepracticetests.org/quiz/qcomment.php?q=1163) |

A Business Impact Analysis (BIA) is an assessment of an organization's business functions to develop an understanding of their criticality, recovery time objectives, and resources needed. By going through a Business Impact Analysis, the organization will gain a common understanding of functions that are critical to its survival. A risk assessment is an evaluation of the exposures present in an organization's external and internal environments. A Business Assessment generally comprises both the risk assessment and the business impact analysis. A disaster recovery plan is the comprehensive statement of consistent actions to be taken before, during and after a disruptive event that causes a significant loss of information systems resources.  
Source: BARNES, James C. & ROTHSTEIN, Philip J., [A Guide to Business Continuity Planning](http://www.amazon.com/exec/obidos/ASIN/0471530158/thecisspopens-20), John Wiley & Sons, 2001 (page 57).

**Contributor:** Christian Vezina

**Study area:** **CISSP CBK - BCP and DRP**

**Covered topic:** [Business Impact Assessment (BIA)](javascript:void(0))

This question © Copyright 2003–2010 Christian Vezina, cccure.org. All rights reserved. No unauthorized use or duplication without explicit written permission of author and of cccure.org.

1. Question: 379 | Difficulty: 4/5 | Relevancy: 3/3

**Business Continuity and Disaster Recovery Planning (Primarily) addresses the:**

* + ›Availability of the CIA triad
  + Confidentiality of the CIA triad
  + Integrity of the CIA triad
  + Availability, Confidentiality and Integrity of the CIA triad

Congratulations, you got the correct answer! Details can be reviewed below.

|  |  |
| --- | --- |
| Details | Submit a comment on [this question](http://www.freepracticetests.org/quiz/qcomment.php?q=379) |

The Information Technology (IT) department plays a very important role in identifying and protecting the company's internal and external information dependencies. Also, the information technology elements of the BCP should address several vital issue, including:  
\* Ensuring that the company employs sufficient physical security mechanisms to preserve vital network and hardware components. including file and print servers.  
\* Ensuring that the organization uses sufficient logical security methodologies (authentication, authorization, etc.) for sensitive data.  
Reference: KRUTZ, Ronald L. & VINES, Russel D., [The CISSP Prep Guide: Mastering the Ten Domains of Computer Security](http://www.amazon.com/exec/obidos/ASIN/0471413569/thecisspopens-20), John Wiley & Sons, 2001, page 279.

**Contributors:** *Rakesh Sud*, Paul Tracy

**Study area:** **CISSP CBK - BCP and DRP**

**Covered topics (2):** [Confidentiality, integrity and availability](javascript:void(0)), [Elements of contingency planning](javascript:void(0))

This question © Copyright 2003–2010 Rakesh Sud, cccure.org. All rights reserved. No unauthorized use or duplication without explicit written permission of author and of cccure.org.

1. Question: 248 | Difficulty: 4/5 | Relevancy: 3/3

**Which of the following is NOT a major element of Business Continuity Planning?**

* + **›Creation of a BCP committee**
  + Business Impact Analysis (BIA)
  + Business Continuity Plan Development
  + Scope plan initiation

Sorry - you had a wrong answer. Please review details below.

|  |  |
| --- | --- |
| Details | Submit a comment on [this question](http://www.freepracticetests.org/quiz/qcomment.php?q=248) |

Creating a BCP committee is part of the scope and plan initiation.  
Source: KRUTZ, Ronald L. & VINES, Russel D., [The CISSP Prep Guide: Mastering the Ten Domains of Computer Security](http://www.amazon.com/exec/obidos/ASIN/0471413569/thecisspopens-20), pages 274-275.

Special thanks to Mica Millbach for reporting a typo within this question.

**Contributor:** Eric Yandell

**Study area:** **CISSP CBK - BCP and DRP**

**Covered topic:** [Business Continuity Planning (BCP)](javascript:void(0))

This question © Copyright 2003–2010 Eric Yandell, cccure.org. All rights reserved. No unauthorized use or duplication without explicit written permission of author and of cccure.org.

1. **During a business impact analysis it is concluded that a system has maximum tolerable downtime of 2 hours. What would this system be classified as?**



* + Important
  + Vital
  + Urgent
  + Critical

1. **A Business Impact Analysis (BIA) does NOT:**



* + Recommend the appropriate recovery solution.
  + Estimate the financial and operational impact of a disruption.
  + Identify critical computer applications and the associated outage tolerance.
  + Determine critical and necessary business functions and their resource dependencies.

1. **Which of the following statements regarding an off-site information processing facility is TRUE?**



* + Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.
  + It should be easily identified from the outside so in the event of an emergency it can be easily found.
  + It should be located in proximity to the originating site so that it can quickly be made operational.
  + It should have the same amount of physical access restrictions as the primary processing site.

1. **Most threats come from:**



* + Disgruntled employees
  + Outsider threats
  + Errors and omissions
  + Fire, water and electrical

1. **Which of the following is NOT a major element of Business Continuity Planning?**



* + Scope plan initiation
  + Creation of a BCP committee
  + Business Impact Analysis (BIA)
  + Business Continuity Plan Development

1. **For which areas of the enterprise are business continuity plans required?**



* + The marketing, finance, and information processing areas.
  + All areas of the enterprise.
  + The operating areas of the enterprise.
  + The financial and information processing areas of the enterprise.

1. **After a company is out of an emergency state, what should be moved back to the original site first?**



* + Most critical work
  + Least critical work
  + IT support staff
  + Executives

1. **Contracts and agreements are unenforceable in which of the following alternate backup facilities?**



* + reciprocal agreement.
  + cold site.
  + warm site.
  + hot site.

1. **Which of the following results in the most devastating business interruptions?**



* + Loss of Hardware/Software
  + Loss of Data
  + Loss of Communication Links
  + Loss of Applications

1. **Which does NOT necessarily have to be a part of the BCP committee?**



* + Legal Department
  + IT Department
  + Business Units
  + Human Resources

1. **Which primary element of BCP includes carrying out vulnerability analysis?**



* + Business Impact Assessment
  + Business Continuity Plan Development
  + Plan Approval and Implementation
  + Scope and Plan Initiation

1. **A business impact assessment is one element in business continuity planning. What are the three primary goals of a BIA?**



* + Data processing continuity planning, data recovery plan maintenance, and testing the disaster recovery plan.
  + Scope and plan initiation, business continuity plan development, and plan approval and implementation.
  + Facility requirements planning, facility security management, and administrative personnel controls.
  + Criticality prioritization, downtime estimation, and resource requirements.

1. **During a test of a disaster recovery plan the IT systems are set up at an alternate site. The results are compared to the results of regular processing at the original site. What kind of testing has taken place?**



* + Simulation
  + Full interruption
  + Parallel
  + Checklist

1. **Which backup type has the quickest backup time?**



* + Disk Mirroring
  + Incremental Backup
  + Differential Backup
  + Full Backup

1. **Which of the following steps should be performed first in a business impact analysis (BIA)?**



* + Evaluate the criticality of business functions.
  + Estimate the Recovery Time Objectives (RTO).
  + Evaluate the impact of disruptive events.
  + Identify all CRITICAL business units within the organization.

1. **Which of the following items is NOT a benefit of cold sites?**



* + A secondary location is available to reconstruct the environment
  + Quick Recovery
  + Low Cost
  + No resource contention with other organisation

1. **Which of the following would best help an organization to gain a common understanding of functions that are critical to its survival?**



* + A business impact analysis
  + A risk assessment
  + A disaster recovery plan
  + A business assessment

1. **Which of the following focuses on sustaining an organization's *business functions* during and after a disruption?**



* + Business continuity plan
  + Business recovery plan
  + Disaster recovery plan
  + Continuity of operations plan

1. **What is the Maximum Tolerable Downtime (MTD)?**



* + Maximum elapsed time required to complete recovery of application data
  + Minimum elapsed time required to complete recovery of application data
  + Maximum elapsed time required to move back to primary site after a major disruption
  + It is maximum delay businesses can tolerate and still remain viable

1. **Which of the following is NOT a disadvantage of a hot site?**



* + It provides a false sense of security.
  + It can be administratively resource intensive.
  + There are cases of common overselling of processing capabilities by the service provider.
  + It is expensive.

1. **The results of a test of the disaster recovery plan conducted at a warm site notes that clients (internal and external clients) were unable to log on to the restored online systems as there were insufficient data lines connecting the client premises to the recovery site. The MOST likely conclusion that can be drawn is that:**



* + The business units were not sufficiently involved or consulted in plan development.
  + The external communications service providers were not involved in the test.
  + The use of a warm site is inappropriate.
  + The impact of a potential disaster was not fully analyzed.

1. **What is a Disaster Recovery Plan (DRP) for a company's computer system usually focused on?**



* + It is focused on restoring operability at an alternate site
  + Availability of compatible equipment at a hot site
  + Strategic long-range planning
  + The probability that a disaster will occur

1. **Which of the following is NOT a transaction redundancy implementation?**



* + electronic vaulting
  + remote journaling
  + database shadowing
  + on-site mirroring

1. **What is the window of time for RECOVERY of information processing capabilities based on?**



* + Criticality of the operations affected.
  + Nature of the disaster.
  + Applications that are mainframe based.
  + Quality of the data to be processed.

1. **What is a hot-site facility?**



* + A site with pre-installed computers, raised flooring, air conditioning, telecommunications and networking equipment, and UPS.
  + A site with ready made work space with telecommunications equipment, LANs, PCs, and terminals for work groups.
  + A site in which space is reserved with pre-installed wiring and raised floors.
  + A site with raised flooring, air conditioning, telecommunications, and networking equipment, and UPS.