B. The Business Impact Analysis (BIA)
C. The Risk Assessment (RA)
D. The Business Continuity Plan (BCP)

Correct Answer: B
Explanation:
The Business Assessment is divided into two components. Risk Assessment (RA) and Business Impact Analysis (BIA). Risk Assessment is designed to evaluate existing exposures from the organization's environment, whereas the BIA assesses potential loss that could be caused by a disaster. The Business Continuity Plan's goal is to reduce the risk of financial loss by improving the ability to recover and restore operations efficiently and effectively.

Source: BARNES, James C.& ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 57).
And: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 276).

QUESTION 544
What is the PRIMARY goal of incident handling?

A. Successfully retrieve all evidence that can be used to prosecute
B. Improve the company's ability to be prepared for threats and disasters
C. Improve the company's disaster recovery plan
D. Contain and repair any damage caused by an event.

Correct Answer: D
Explanation:
This is the PRIMARY goal of an incident handling process.

The other answers are incorrect because:

Successfully retrieve all evidence that can be used to prosecute is more often used in identifying weaknesses than in prosecuting.

Improve the company's ability to be prepared for threats and disasters is more appropriate for a disaster recovery plan.

Improve the company's disaster recovery plan is also more appropriate for disaster recovery plan.

Reference:
Shon Harris AIO v3 , Chapter - 10 : Law, Investigation, and Ethics , Page: 727-728

QUESTION 545
Which disaster recovery plan test involves functional representatives meeting to review the plan in detail?

A. Simulation test
B. Checklist test
C. Parallel test
D. Structured walk-through test

Correct Answer: D

Explanation:
The structured walk-through test occurs when the functional representatives meet to review the plan in detail. This involves a thorough look at each of the plan steps, and the procedures that are invoked at that point in the plan. This ensures that the actual planned activities are accurately described in the plan. The checklist test is a method of testing the plan by distributing copies to each of the functional areas. The simulation test plays out different scenarios. The parallel test is essentially an operational test that is performed without interrupting current processing.
Source: HARE, Chris, CISSP Study Guide: Business Continuity Planning Domain,

QUESTION 546
Which backup type run at regular intervals would take the least time to complete?

A. Full Backup
B. Differential Backup
C. Incremental Backup
D. Disk Mirroring

Correct Answer: C
Explanation:
Incremental backups only backup changed data (changes archive bit to not backup again if not changed).

Although the incremental backup is fastest to backup, it is usually more time consuming for the restore process.

In some cases, the window available for backup may not be long enough to backup all the data on the system during each backup. In that case, differential or incremental backups may be more appropriate.

In an incremental backup, only the files that changed since the last backup will be backed up.

In a differential backup, only the files that changed since the last full backup will be backed up.
In general, differentials require more space than incremental backups while incremental backups are faster to perform. On the other hand, restoring data from incremental backups requires more time than differential backups. To restore from incremental backups, the last full backup and all of the incremental backups performed are combined. In contrast, restoring from a differential backup requires only the last full backup and the latest differential.

The following are incorrect answers:

Differential backups backup all data since the last full backup (does not reset archive bit) Full backups backup all selected data, regardless of archive bit, and resets the archive bit.
Disk mirroring is not considered as a backup type.

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20385-20390). Auerbach Publications. Kindle Edition.
And HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 618).

QUESTION 547

Which of the following is NOT a correct notation for an IPv6 address?

A. 2001:0db8:0:0:0:0:1428:57ab
B. ABCD:EF01:2345:6789:ABCD:EF01:2345:6789
C. ::1
D. 2001:DB8::8:800::417A

Correct Answer: D
Explanation:
This is not a correct notation for an IPv6 address because the the "::" can only appear once in an address. The use of "::" is a shortcut notation that indicates one or more groups of 16 bits of zeros.
1 is the loopback address using the special notation
Reference:
IP Version 6 Addressing Architecture
http://tools.ietf.org/html/rfc4291#section-2.1

QUESTION 548
Within the realm of IT security, which of the following combinations best defines risk?

A. Threat coupled with a breach
B. Threat coupled with a vulnerability
C. Vulnerability coupled with an attack
D. Threat coupled with a breach of security

Correct Answer: B
Explanation:
The Correct Answer: Threat coupled with a vulnerability. Threats are circumstances or actions with the ability to harm a system. They can destroy or modify data or result an a DoS. Threats by themselves are not acted upon unless there is a vulnerability that can be taken advantage of. Risk enters the equation when a vulnerability (Flaw or weakness) exists in policies, procedures, personnel management, hardware, software or facilities and can be exploited by a threat agent. Vulnerabilities do not cause harm, but they leave the system open to harm. The combination of a threat with a vulnerability increases the risk to the system of an intrusion.

The following answers are incorrect:

Threat coupled with a breach. A threat is the potential that a particular threat-source will take advantage of a vulnerability. Breaches get around security. It does not matter if a breach is discovered or not, it has still occured and is not a risk of something occuring. A breach would quite often be termed as an incident or intrusion.

Vulnerability coupled with an attack. Vulnerabilities are weaknesses (flaws) in policies, procedures, personnel management, hardware, software or factilities that may result in a harmful intrusion to an IT system. An attack takes advantage of the flaw or vulnerability. Attacks are explicit attempts to violate security, and are more than risk as they are active.

Threat coupled with a breach of security. This is a detractor. Although a threat agent may take advantage of (Breach) vulnerabilities or flaws in systems security. A threat coupled with a breach of security is more than a risk as this is active.

The following reference(s) may be used to research the QUESTION NO: s in this question:

ISC2 OIG, 2007 p. 66-67

Shon Harris AIO v3 p. 71-72

QUESTION 549
Hierarchical Storage Management (HSM) is commonly employed in:

A. very large data retrieval systems
B. very small data retrieval systems
C. shorter data retrieval systems
D. most data retrieval systems

Correct Answer: A
Explanation:
Hierarchical Storage Management (HSM) is commonly employed in very large data retrieval systems.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 71.

QUESTION 550
What is electronic vaulting?

A. Information is backed up to tape on a hourly basis and is stored in a on-site vault.
B. Information is backed up to tape on a daily basis and is stored in a on-site vault.
C. Transferring electronic journals or transaction logs to an off-site storage facility
D. A transfer of bulk information to a remote central backup facility.

Correct Answer: D
Explanation:
Electronic vaulting is defined as "a method of transferring bulk information to off-site facilities for backup purposes". Remote Journaling is the same concept as electronic vaulting, but has to do with journals and transaction logs, not the actual files.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 619).

QUESTION 551
Which of the following backup methods is most appropriate for off-site archiving?

A. Incremental backup method
B. Off-site backup method
C. Full backup method
D. Differential backup method

Correct Answer: C
Explanation:
The full backup makes a complete backup of every file on the system every time it is run. Since a single backup set is needed to perform a full restore, it is appropriate for off-site archiving.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 69).

QUESTION 552
Which of the following results in the most devastating business interruptions?

A. Loss of Hardware/Software
B. Loss of Data
C. Loss of Communication Links
D. Loss of Applications

Correct Answer: B
Explanation:
Source: Veritas eLearning CD - Introducing Disaster Recovery Planning, Chapter 1.
All of the others can be replaced or repaired. Data that is lost and was not backed up, cannot be restored.

QUESTION 553
What is called an exception to the search warrant requirement that allows an officer to conduct a search without having the warrant in-hand if probable cause is present and destruction of the evidence is deemed imminent?

A. Evidence Circumstance Doctrine
B. Exigent Circumstance Doctrine
C. Evidence of Admissibility Doctrine
D. Exigent Probable Doctrine

Correct Answer: B
Explanation:
An Exigent Circumstance is an unusual and time-sensitive circumstance that justifies conduct that might not be permissible or lawful in other circumstances.

For example, exigent circumstances may justify actions by law enforcement officers acting without a warrant such as a mortal danger to a young child. Examples of other exigent circumstances include protecting evidence or property from imminent destruction.

In US v Martinez, Justice Thomas of the United States Court of Appeal used these words:

"As a general rule, we define exigent circumstances as those circumstances that would cause a reasonable person to believe that entry was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts."

In Alvarado, Justice Blackburn of the Court of Appeals of Georgia referred to exigent circumstances in the context of a drug bust:

"The exigent circumstance doctrine provides that when probable cause has been established to believe that evidence will be removed or destroyed before a warrant can be obtained, a warrantless search and seizure can be justified. As many courts have noted, the need for the exigent circumstance doctrine is particularly compelling in narcotics cases, because contraband and records can be easily and quickly destroyed while a search is progressing. Police officers relying on this exception must demonstrate an objectively reasonable basis for deciding that immediate action is required."

All of the other answers were only detractors made up and not legal terms.

Reference(s) used for this question:

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten