Using a write blocker is wrong because using a write blocker ensure that you cannot modify the data on the host and it prevent the host from writing to its hard drives.

Made a full-disk image is wrong because making a full-disk image can preserve all data on a hard disk, including deleted files and file fragments.

Created a message digest for log files is wrong because creating a message digest for log files. A message digest is a cryptographic checksum that can demonstrate that the integrity of a file has not been compromised (e.g. changes to the content of a log file)

Domain: LEGAL, REGULATIONS, COMPLIANCE AND INVESTIGATIONS

References:
AIO 3rd Edition, page 783-784
NIST 800-61 Computer Security Incident Handling guide page 3-18 to 3-20

QUESTION 479
Which conceptual approach to intrusion detection system is the most common?

A. Behavior-based intrusion detection
B. Knowledge-based intrusion detection
C. Statistical anomaly-based intrusion detection
D. Host-based intrusion detection

Correct Answer: B
Explanation:
There are two conceptual approaches to intrusion detection. Knowledge- based intrusion detection uses a database of known vulnerabilities to look for current attempts to exploit them on a system and trigger an alarm if an attempt is found. The other approach, not as common, is called behaviour-based or statistical analysis-based. A host- based intrusion detection system is a common implementation of intrusion detection, not a conceptual approach.
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 63).
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 193-194).

QUESTION 480
Which of the following is a disadvantage of a statistical anomaly-based intrusion detection system?

A. it may truly detect a non-attack event that had caused a momentary anomaly in the system.
B. it may falsely detect a non-attack event that had caused a momentary anomaly in the system.
C. it may correctly detect a non-attack event that had caused a momentary anomaly in the system.
D. it may loosely detect a non-attack event that had caused a momentary anomaly in the system.

Correct Answer: B
Explanation:
Some disadvantages of a statistical anomaly-based ID are that it will not detect an attack that does not significantly change the system operating characteristics, or it may falsely detect a non-attack event that had caused a momentary anomaly in the system.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

QUESTION 481
Which of the following would be LESS likely to prevent an employee from reporting an incident?

A. They are afraid of being pulled into something they don't want to be involved with.
B. The process of reporting incidents is centralized.
C. They are afraid of being accused of something they didn't do.
D. They are unaware of the company's security policies and procedures.

Correct Answer: B
Explanation:
The reporting process should be centralized else employees won't bother.

The other answers are incorrect because :

They are afraid of being pulled into something they don't want to be involved with is incorrect as most of the employees fear of this and this would prevent them to report an incident.
They are afraid of being accused of something they didn't do is also incorrect as this also prevents them to report an incident.
They are unaware of the company's security policies and procedures is also incorrect as mentioned above.

Reference:
Shon Harris AIO v3 , Ch-10: Laws , Investigatio & Ethics , Page: 675.

QUESTION 482
Organizations should not view disaster recovery as which of the following?

A. Committed expense.
B. Discretionary expense.
C. Enforcement of legal statutes.
D. Compliance with regulations.

Correct Answer: B
Explanation:
Disaster Recovery should never be considered a discretionary expense. It is far too important a task. In order to maintain the continuity of the business Disaster Recovery should be a commitment of and by the organization.

A discretionary fixed cost has a short future planning horizon--under a year. These types of costs arise from annual decisions of management to spend in specific fixed cost areas, such as marketing and research. DR would be an ongoing long term committment not a short term effort only.

A committed fixed cost has a long future planning horizon-- more than on year. These types of costs relate to a company's investment in assets such as facilities and equipment. Once such costs have been incurred, the company is required to make future payments.

The following answers are incorrect:

committed expense. Is incorrect because Disaster Recovery should be a committed expense.
enforcement of legal statutes. Is incorrect because Disaster Recovery can include enforcement of legal statutes. Many organizations have legal requirements toward Disaster Recovery.

compliance with regulations. Is incorrect because Disaster Recovery often means compliance with regulations. Many financial institutions have regulations requiring Disaster Recovery Plans and Procedures.

QUESTION 483
Which of the following steps is NOT one of the eight detailed steps of a Business Impact Assessment (BIA):

A. Notifying senior management of the start of the assessment.
B. Creating data gathering techniques.
C. Identifying critical business functions.
D. Calculating the risk for each different business function.

Correct Answer: A
Explanation:
Source: HARRIS, S., CISSP All- In-One Exam Guide, 3rd. Edition, 2005, Chapter 9, Page 701.

There have been much discussion about the steps of the BIA and I struggled with this before deciding to scrape the question about "the four steps," and re-write the question using the AIO for a reference. This question should be easy.... if you know all eight steps.

The eight detailed and granular steps of the BIA are:

1. Select Individuals to interview for the data gathering.
2. Create data gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company's critical business functions.
4. Identify the resources that these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and the threats to these functions.
7. Calculate risk for each of the different business functions.
8. Document findings and report them to management.

Shon goes on to cover each step in Chapter 9.

QUESTION 484
When a possible intrusion into your organization's information system has been detected, which of the following actions should be performed first?

A. Eliminate all means of intruder access.
B. Contain the intrusion.
C. Determine to what extent systems and data are compromised.
D. Communicate with relevant parties.

Correct Answer: C
Explanation:
Once an intrusion into your organization's information system has been detected, the first action that needs to be performed is determining to what extent systems and data are compromised (if they really are), and then take action.

This is the good old saying: "Do not cry wolf until you know there is a wolf for sure" Sometimes it smells like a wolf, it looks like a wolf, but it may not be a wolf. Technical problems or bad hardware might cause problems that looks like an intrusion even thou it might not be. You must

make sure that a crime has in fact been committed before implementing your reaction plan.

Information, as collected and interpreted through analysis, is key to your decisions and actions while executing response procedures. This first analysis will provide information such as what attacks were used, what systems and data were accessed by the intruder, what the intruder did after obtaining access and what the intruder is currently doing (if the intrusion has not been contained).

The next step is to communicate with relevant parties who need to be made aware of the intrusion in a timely manner so they can fulfil their responsibilities.

Step three is concerned with collecting and protecting all information about the compromised systems and causes of the intrusion. It must be carefully collected, labelled, catalogued, and securely stored.

Containing the intrusion, where tactical actions are performed to stop the intruder's access, limit the extent of the intrusion, and prevent the intruder from causing further damage, comes next.

Since it is more a long-term goal, eliminating all means of intruder access can only be achieved last, by implementing an ongoing security improvement process.

Reference used for this question:
ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison- Wesley, 2001, Chapter 7: Responding to Intrusions (pages 271-289).

QUESTION 485
Which backup method is used if backup time is critical and tape space is at an extreme premium?

A. Incremental backup method.
B. Differential backup method.
C. Full backup method.
D. Tape backup method.

Correct Answer: A
Explanation:
Full Backup/Archival Backup - Complete/Full backup of every selected file on the system regardless of whether it has been backup recently.. This is the slowest of the backup methods since it backups all the data. It's however the fastest for restoring data.

Incremental Backup - Any backup in which only the files that have been modified since last full back up are backed up. The archive attribute should be updated while backing up only modified files, which indicates that the file has been backed up. This is the fastest of the backup methods, but the slowest of the restore methods.

Differential Backup - The backup of all data files that have been modified since the last incremental backup or archival/full backup. Uses the archive bit to determine what files have changed since last incremental backup or full backup. The files grows each day until the next full backup is performed clearing the archive attributes. This enables the user to restore all files changed since the last full backup in one pass. This is a more neutral method of backing up data since it's not faster nor slower than the other two

Easy Way To Remember each of the backup type properties:
Backup Speed Restore Speed
Full 3 1

Differential 2 2
Incremental 1 3

Legend: 1 = Fastest 2 = Faster 3 = Slowest

Source:
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.
http://www.proprofs.com/mwiki/index.php/Full_Backup,_Incremental_%26_Differential_Bac kup

QUESTION 486
Business Continuity Planning (BCP) is not defined as a preparation that facilitates:

A. the rapid recovery of mission-critical business operations
B. the continuation of critical business functions
C. the monitoring of threat activity for adjustment of technical controls
D. the reduction of the impact of a disaster

Correct Answer: C
Explanation:
Although important, The monitoring of threat activity for adjustment of technical controls is not facilitated by a Business Continuity Planning

The following answers are incorrect:

All of the other choices are facilitated by a BCP:

the continuation of critical business functions
the rapid recovery of mission-critical business operations the reduction of the impact of a disaster

QUESTION 487
Which of the following best allows risk management results to be used knowledgeably?

A. A vulnerability analysis
B. A likelihood assessment
C. An uncertainty analysis
D. A threat identification

Correct Answer: C
Explanation:
Risk management consists of two primary and one underlying activity; risk assessment and risk mitigation are the primary activities and uncertainty analysis is the underlying one. After having performed risk assessment and mitigation, an uncertainty analysis should be performed. Risk management must often rely on speculation, best guesses, incomplete data, and many unproven assumptions. A documented uncertainty analysis allows the risk management results to be used knowledgeably. A vulnerability analysis, likelihood assessment and threat identification are all parts of the collection and analysis of data part of the risk assessment, one of the primary activities of risk management.
Source: SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (pages 19-21).