C. Internal Hot Site
D. Dual Data Center

Correct Answer: C
Explanation:
Internal Hot Site--This site is standby ready with all the technology and equipment necessary to run the applications positioned there. The planner will be able to effectively restart an application in a hot site recovery without having to perform any bare metal recovery of servers. If this is an internal solution, then often the organization will run non-time sensitive processes there such as development or test environments, which will be pushed aside for recovery of production when needed. When employing this strategy, it is important that the two environments be kept as close to identical as possible to avoid problems with O/S levels, hardware differences, capacity differences, etc., from preventing or delaying recovery.

Recovery Site Strategies Depending on how much downtime an organization has before the technology recovery must be complete, recovery strategies selected for the technology environment could be any one of the following:
Dual Data Center--This strategy is employed for applications, which cannot accept any downtime without negatively impacting the organization. The applications are split between two geographically dispersed data centers and either load balanced between the two centers or hot swapped between the two centers. The surviving data center must have enough head room to carry the full production load in either case.

External Hot Site--This strategy has equipment on the floor waiting, but the environment must be rebuilt for the recovery. These are services contracted through a recovery service provider. Again, it is important that the two environments be kept as close to identical as possible to avoid problems with O/S levels, hardware differences, capacity differences, etc., from preventing or delaying recovery. Hot site vendors tend to have the most commonly used hardware and software products to attract the largest number of customers to utilize the site. Unique equipment or software would generally need to be provided by the organization either at time of disaster or stored there ahead of time. Warm Site--A leased or rented facility that is usually partially configured with some equipment, but not the actual computers. It will generally have all the cooling, cabling, and networks in place to accommodate the recovery but the actual servers, mainframe, etc., equipment are delivered to the site at time of disaster. Cold Site--A cold site is a shell or empty data center space with no technology on the floor. All technology must be purchased or acquired at the time of disaster.

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 21265-21291). Auerbach Publications. Kindle Edition.

QUESTION 594
Once evidence is seized, a law enforcement officer should emphasize which of the following?

A. Chain of command
B. Chain of custody
C. Chain of control
D. Chain of communications

Correct Answer: B
Explanation:
All people that handle the evidence from the time the crime was committed through the final disposition must be identified. This is to ensure that the evidence can be used and has not been tampered with.

The following answers are incorrect:

chain of command. Is incorrect because chain of command is the order of authority and does not apply to evidence.
chain of control. Is incorrect because it is a distractor. chain of communications. Is incorrect because it is a distractor.

QUESTION 595
What is the most correct choice below when talking about the steps to resume normal operation at the primary site after the green light has been given by the salvage team?

A. The most critical operations are moved from alternate site to primary site before others
B. Operation may be carried by a completely different team than disaster recovery team
C. The least critical functions should be moved back first
D. You moves items back in the same order as the categories document in your plan or exactly in the same order as you did on your way to the alternate site

Correct Answer: C
Explanation:
It's interesting to note that the steps to resume normal processing operations will be different than the steps of the recovery plan; that is, the least critical work should be brought back first to the primary site.

The most important point above in the steps would be to move the least critical items or resources back to the primary site first. This way you can ensure that the site was really well prepared and that all is working fine.

Before that first step would be done, you would get the green light from the salvage team that it is fine to move back to the primary site. The first step after getting the green light would be to move the least critical elements first.

As stated in the Shon Harris book:
The least critical functions should be moved back first, so if there are issues in network configurations or connectivity, or important steps were not carried out, the critical operations of the company are not negatively affected. Why go through the trouble of moving the most critical systems and operations to a safe and stable site, only to return it to a main site that is untested? Let the less critical departments act as the canary. If they survive, then move over the more critical components of the company.

When it is time for the company to move back into its original site or a new site, the company enters the reconstitution phase. A company is not out of an emergency state until it is back in operation at the original primary site or a new site that was constructed to replace the primary site, because the company is always vulnerable while operating in a backup facility.

Many logistical issues need to be considered as to when a company must return from the alternate site to the original site. The following lists a few of these issues:

Ensuring the safety of employees
Ensuring an adequate environment is provided (power, facility infrastructure, water, HVAC)
Ensuring that the necessary equipment and supplies are present and in working order
Ensuring proper communications and connectivity methods are working Properly testing the new environment
Once the coordinator, management, and salvage team sign off on the readiness of the facility, the

salvage team should carry out the following steps:

Back up data from the alternate site and restore it within the new facility.
Carefully terminate contingency operations.
Securely transport equipment and personnel to the new facility.

All other choices are not the correct answer.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Location 19389). McGraw-Hill. Kindle Edition.
And KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 290.

QUESTION 596
Which of the following categories of hackers poses the greatest threat?

A. Disgruntled employees
B. Student hackers
C. Criminal hackers
D. Corporate spies

Correct Answer: A
Explanation:
According to the authors, hackers fall in these categories, in increasing threat order: security experts, students, underemployed adults, criminal hackers, corporate spies and disgruntled employees.
Disgruntled employees are the most dangerous security problem of all because they are most likely to have a good knowledge of the organization's IT systems and security measures.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 2: Hackers.

QUESTION 597
Qualitative loss resulting from the business interruption does NOT usually include:

A. Loss of revenue
B. Loss of competitive advantage or market share
C. Loss of public confidence and credibility
D. Loss of market leadership

Correct Answer: A
Explanation:
This question is testing your ability to evaluate whether items on the list are Qualitative or Quantitative. All of the items listed were Qualitative except Lost of Revenue which is Quantitative.

Those are mainly two approaches to risk analysis, see a description of each below:

A quantitative risk analysis is used to assign monetary and numeric values to all elements of the risk analysis process. Each element within the analysis (asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items) is quantified and entered into equations to determine total and residual risks. It is more of a scientific or mathematical approach to risk analysis compared to qualitative.

A qualitative risk analysis uses a "softer" approach to the data elements of a risk analysis . It does not quantify that data, which means that it does not assign numeric values to the data so that they can be used in equations.

Qualitative and quantitative impact information should be gathered and then properly analyzed and interpreted. The goal is to see exactly how a business will be affected by different threats.

The effects can be economical, operational, or both. Upon completion of the data analysis, it should be reviewed with the most knowledgeable people within the company to ensure that the findings are appropriate and that it describes the real risks and impacts the organization faces. This will help flush out any additional data points not originally obtained and will give a fuller understanding of all the possible business impacts.

Loss criteria must be applied to the individual threats that were identified. The criteria may include the following:

Loss in reputation and public confidence
Loss of competitive advantages
Increase in operational expenses
Violations of contract agreements
Violations of legal and regulatory requirements
Delayed income costs
Loss in revenue
Loss in productivity

Reference used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 909). McGraw- Hill. Kindle Edition.

QUESTION 598
Who should direct short-term recovery actions immediately following a disaster?

A. Chief Information Officer.
B. Chief Operating Officer.
C. Disaster Recovery Manager.
D. Chief Executive Officer.

Correct Answer: C
Explanation:
The Disaster Recovery Manager should also be a member of the team that assisted in the development of the Disaster Recovery Plan. Senior-level management need to support the process but would not be involved with the initial process.

The following answers are incorrect:

Chief Information Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.

Chief Operating Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.
Chief Executive Officer. Is incorrect because the Senior-level management are the ones to

authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.

QUESTION 599
Which of the following is the most complete disaster recovery plan test type, to be performed after successfully completing the Parallel test?

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

Correct Answer: A
Explanation:
The difference between this and the full-interruption test is that the primary production processing of the business does not stop; the test processing runs in parallel to the real processing. This is the most common type of disaster recovery plan testing.

A checklist test is only considered a preliminary step to a real test.

In a structured walk-through test, business unit management representatives meet to walk through the plan, ensuring it accurately reflects the organization's ability to recover successfully, at least on paper.

A simulation test is aimed at testing the ability of the personnel to respond to a simulated disaster, but not recovery process is actually performed.

Source: 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 289).

QUESTION 600
What can be best defined as the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment?

A. Risk management
B. Risk analysis
C. Threat analysis
D. Due diligence

Correct Answer: C
Explanation:
Threat analysis is the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.

The following answers are incorrect:

Risk analysis is the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact.

Risk analysis is synonymous with risk assessment and part of risk management, which is the ongoing process of assessing the risk to mission/business as part of a risk-based approach used