ISC

Exam SSCP

Systems Security Certified Practitioner

Verson: Demo

[Total Questions: 10]

Topic break down

Topic	No. of Questions
Topic 1: Access Control	2
Topic 2: Security Operation Adimnistration	2
Topic 3: Analysis and Monitoring	1
Topic 4: Risk, Response and Recovery	3
Topic 5: Cryptography	2

Topic 1, Access Control

Question No : 1 - (Topic 1)

The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated up to?

A. Illiminated at nine feet high with at least three foot-candles
B. Illiminated at eight feet high with at least three foot-candles
C. Illiminated at eight feet high with at least two foot-candles
D. Illuminated at nine feet high with at least two foot-candles

Answer: B

Explanation: The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated eight feet high with at least two foot-candles.

It can also be referred to as illuminating to a height of eight feet, with a BRIGHTNESS of two foot-candles.

One footcandle 10.764 lux. The footcandle (or lumen per square foot) is a non-SI unit of illuminance. Like the BTU, it is obsolete but it is still in fairly common use in the United States, particularly in construction-related engineering and in building codes. Because lux and footcandles are different units of the same quantity, it is perfectly valid to convert footcandles to lux and vice versa.

The name "footcandle" conveys "the illuminance cast on a surface by a one-candela source one foot away." As natural as this sounds, this style of name is now frowned upon, because the dimensional formula for the unit is not foot • candela, but lumens per square foot.

Some sources do however note that the "lux" can be thought of as a "metre-candle" (i.e. the illuminance cast on a surface by a one-candela source one meter away). A source that is farther away casts less illumination than one that is close, so one lux is less illuminance than one footcandle. Since illuminance follows the inverse-square law, and since one foot = 0.3048 m, one lux = 0.30482 footcandle 1/10.764 footcandle.

TIPS FROM CLEMENT:
Illuminance (light level) – The amount of light, measured in foot-candles (US unit), that falls n a surface, either horizontal or vertical.

Parking lots lighting needs to be an average of 2 foot candles; uniformity of not more than 3:1, no area less than 1 fc.

All illuminance measurements are to be made on the horizontal plane with a certified light meter calibrated to NIST standards using traceable light sources.

The CISSP Exam Cram 2 from Michael Gregg says:
Lighting is a commonly used form of perimeter protection.

Some studies have found that up to 80% of criminal acts at businesses and shopping centers happen in adjacent parking lots. Therefore, it's easy to see why lighting can be such an important concern.

Outside lighting discourages prowlers and thieves.
The National Institute of Standards and Technologies (NIST) states that, for effective perimeter control, buildings should be illuminated 8 feet high, with 2-foot candle power.

Reference used for this question:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 325.
and
Shon's AIO v5 pg 459
and
http://en.wikipedia.org/wiki/Foot-candle

Question No : 2 - (Topic 1)

Which of the following statements pertaining to access control is false?

A. Users should only access data on a need-to-know basis.
B. If access is not explicitly denied, it should be implicitly allowed.
C. Access rights should be granted based on the level of trust a company has on a subject.
D. Roles can be an efficient way to assign rights to a type of user who performs certain tasks.

Answer: B

Explanation: Access control mechanisms should default to no access to provide the necessary level of security and ensure that no security holes go unnoticed. If access is not explicitly allowed, it should be implicitly denied.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4: Access Control (page 143).

Topic 2, Security Operation Adimnistration

Question No : 3 - (Topic 2)

One purpose of a security awareness program is to modify:

A. employee's attitudes and behaviors towards enterprise's security posture
B. management's approach towards enterprise's security posture
C. attitudes of employees with sensitive data
D. corporate attitudes about safeguarding data

Answer: A

Explanation: The Answer: security awareness training is to modify employees behaviour and attitude towards towards enterprise's security posture.

Security-awareness training is performed to modify employees' behavior and attitude toward security. This can best be achieved through a formalized process of security-awareness training.

It is used to increase the overall awareness of security throughout the company. It is targeted to every single employee and not only to one group of users.

Unfortunately you cannot apply a patch to a human being, the only thing you can do is to educate employees and make them more aware of security issues and threats. Never underestimate human stupidity.

Reference(s) used for this question:

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
also see:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 130). McGraw-Hill. Kindle Edition.

Question No : 4 - (Topic 2)

Which of the following is responsible for MOST of the security issues?

A. Outside espionage
B. Hackers
C. Personnel
D. Equipment failure

Answer: C

Explanation: Personnel cause more security issues than hacker attacks, outside espionage, or equipment failure.

The following answers are incorrect because:

Outside espionage is incorrect as it is not the best answer.
Hackers is also incorrect as it is not the best answer.
Equipment failure is also incorrect as it is not the best answer.
Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 56

Topic 3, Analysis and Monitoring

Question No : 5 - (Topic 3)

In an online transaction processing system (OLTP), which of the following actions should be taken when erroneous or invalid transactions are detected?

A. The transactions should be dropped from processing.
B. The transactions should be processed after the program makes adjustments.
C. The transactions should be written to a report and reviewed.
D. The transactions should be corrected and reprocessed.

Answer: C

Explanation: In an online transaction processing system (OLTP) all transactions are recorded as they occur. When erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

As explained in the ISC2 OIG:
OLTP is designed to record all of the business transactions of an organization as they occur. It is a data processing system facilitating and managing transaction-oriented applications. These are characterized as a system used by many concurrent users who are actively adding and modifying data to effectively change real-time data.

OLTP environments are frequently found in the finance, telecommunications, insurance, retail, transportation, and travel industries. For example, airline ticket agents enter data in the database in real-time by creating and modifying travel reservations, and these are increasingly joined by users directly making their own reservations and purchasing tickets through airline company Web sites as well as discount travel Web site portals. Therefore, millions of people may be accessing the same flight database every day, and dozens of people may be looking at a specific flight at the same time.

The security concerns for OLTP systems are concurrency and atomicity.

Concurrency controls ensure that two users cannot simultaneously change the same data, or that one user cannot make changes before another user is finished with it. In an airline ticket system, it is critical for an agent processing a reservation to complete the transaction, especially if it is the last seat available on the plane.

Atomicity ensures that all of the steps involved in the transaction complete successfully. If one step should fail, then the other steps should not be able to complete. Again, in an airline ticketing system, if the agent does not enter a name into the name data field correctly, the transaction should not be able to complete.

OLTP systems should act as a monitoring system and detect when individual processes abort, automatically restart an aborted process, back out of a transaction if necessary, allow distribution of multiple copies of application servers across machines, and perform dynamic load balancing.

A security feature uses transaction logs to record information on a transaction before it is processed, and then mark it as processed after it is done. If the system fails during the transaction, the transaction can be recovered by reviewing the transaction logs.

Checkpoint restart is the process of using the transaction logs to restart the machine by running through the log to the last checkpoint or good transaction. All transactions following the last checkpoint are applied before allowing users to access the data again.

Wikipedia has nice coverage on what is OLTP:
Online transaction processing, or OLTP, refers to a class of systems that facilitate and manage transaction-oriented applications, typically for data entry and retrieval transaction processing. The term is somewhat ambiguous; some understand a "transaction" in the context of computer or database transactions, while others (such as the Transaction Processing Performance Council) define it in terms of business or commercial transactions.

OLTP has also been used to refer to processing in which the system responds immediately to user requests. An automatic teller machine (ATM) for a bank is an example of a commercial transaction processing application.

The technology is used in a number of industries, including banking, airlines, mailorder, supermarkets, and manufacturing. Applications include electronic banking, order processing, employee time clock systems, e-commerce, and eTrading.

There are two security concerns for OLTP system: Concurrency and Atomicity

ATOMICITY
In database systems, atomicity (or atomicness) is one of the ACID transaction properties. In an atomic transaction, a series of database operations either all occur, or nothing occurs. A guarantee of atomicity prevents updates to the database occurring only partially, which can cause greater problems than rejecting the whole series outright.

The etymology of the phrase originates in the Classical Greek concept of a fundamental and indivisible component; see atom.

An example of atomicity is ordering an airline ticket where two actions are required: payment, and a seat reservation. The potential passenger must either:

both pay for and reserve a seat; OR
neither pay for nor reserve a seat.

The booking system does not consider it acceptable for a customer to pay for a ticket without securing the seat, nor to reserve the seat without payment succeeding.

CONCURRENCY

Database concurrency controls ensure that transactions occur in an ordered fashion.

The main job of these controls is to protect transactions issued by different users/applications from the effects of each other. They must preserve the four characteristics of database transactions ACID test: Atomicity, Consistency, Isolation, and Durability. Read http://en.wikipedia.org/wiki/ACID for more details on the ACID test.

Thus concurrency control is an essential element for correctness in any system where two database transactions or more, executed with time overlap, can access the same data, e.g., virtually in any general-purpose database system. A well established concurrency control theory exists for database systems: serializability theory, which allows to effectively design and analyze concurrency control methods and mechanisms.

Concurrency is not an issue in itself, it is the lack of proper concurrency controls that makes it a serious issue.

The following answers are incorrect:

The transactions should be dropped from processing. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

The transactions should be processed after the program makes adjustments. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

The transactions should be corrected and reprocessed. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

References:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 12749-12768). Auerbach Publications. Kindle Edition.
and
http://en.wikipedia.org/wiki/Online_transaction_processing
and
http://databases.about.com/od/administration/g/concurrency.htm

Topic 4, Risk, Response and Recovery

Question No : 6 - (Topic 4)

A momentary power outage is a:

A. spike
B. blackout
C. surge
D. fault

Answer: D

Explanation: A momentary power outage is a fault.

Power Excess
Spike --> Too much voltage for a short period of time.
Surge --> Too much voltage for a long period of time.

Power Loss
Fault --> A momentary power outage.
Blackout --> A long power interruption.

Power Degradation
Sag or Dip --> A momentary low voltage.
Brownout --> A prolonged power supply that is below normal voltage.

Reference(s) used for this question:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.
and
https://en.wikipedia.org/wiki/Power_quality

Question No : 7 - (Topic 4)

Which of the following is a large hardware/software backup system that uses the RAID technology?

A. Tape Array.
B. Scale Array.
C. Crimson Array
D. Table Array.

Answer: A

Explanation: A Tape Array is a large hardware/software backup system based on the RAID technology.

There is a misconception that RAID can only be used with Disks.
All large storage vendor from HP, to EMC, to Compaq have Tape Array based on RAID technology they offer.

This is a VERY common type of storage at an affordable price as well.

So RAID is not exclusively for DISKS. Often time this is referred to as Tape Librairies or simply RAIT.
RAIT (redundant array of independent tapes) is similar to RAID, but uses tape drives instead of disk drives. Tape storage is the lowest-cost option for very large amounts of data, but is very slow compared to disk storage. As in RAID 1 striping, in RAIT, data are striped in parallel to multiple tape drives, with or without a redundant parity drive. This provides the high capacity at low cost typical of tape storage, with higher-than-usual tape data transfer rates and optional data integrity.

References:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 70.
and
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1271). McGraw-Hill. Kindle Edition.

Question No : 8 - (Topic 4)

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

A. Every organization must have a disaster recovery plan
B. A disaster recovery plan contains actions to be taken before, during and after a disruptive event.
C. The major goal of disaster recovery planning is to provide an organized way to make decisions if a disruptive event occurs.
D. A disaster recovery plan should cover return from alternate facilities to primary facilities.

Answer: A

Explanation: It is possible that an organization may not need a disaster recovery plan. An organization may not have any critical processing areas or system and they would be able to withstand lengthy interruptions.

Remember that DRP is related to systems needed to support your most critical business functions.

The DRP plan covers actions to be taken when a disaster occur but DRP PLANNING which is the keywork in the question would also include steps that happen before you use the plan such as development of the plan, training, drills, logistics, and a lot more.

To be effective, the plan would certainly cover before, during, and after the disaster actions.

It may take you a couple years to develop a plan for a medium size company, there is a lot that has to happen before the plan would be actually used in a real disaster scenario. Plan for the worst and hope for the best.

All other statements are true.

NOTE FROM CLEMENT:
Below is a great article on who legally needs a plan which is very much in line with this question. Does EVERY company needs a plan? The legal answer is NO. Some companies, industries, will be required according to laws or regulations to have a plan. A blank statement saying: All companies MUST have a plan would not be accurate. The article below is specific to the USA but similar laws will exist in many other countries.

Some companies such as utilities, power, etc... might also need plan if they have been defined as Critical Infrastructure by the government. The legal side of IT is always very complex and varies in different countries. Always talk to your lawyer to ensure you follow the law of the land :-)

Read the details below:
So Who, Legally, MUST Plan?

With the caveats above, let’s cover a few of the common laws where there is a duty to have a disaster recovery plan. I will try to include the basis for that requirement, where there is an implied mandate to do so, and what the difference is between the two
Banks and Financial Institutions MUST Have a Plan

The Federal Financial Institutions Examination Council (Council) was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630. In 1989, Title XI of the Financial Institutions Reform, Recovery and Enforcement Act of 1989 (FIRREA) established the Examination Council (the Council).

The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS); and to make recommendations to promote uniformity in the supervision of financial institutions. In other words, every bank, savings and loan, credit union, and other financial institution is governed by the principles adopted by the Council.

In March of 2003, the Council released its Business Continuity Planning handbook designed to provide guidance and examination procedures for examiners in evaluating financial institution and service provider risk-management processes.
Stockbrokers MUST Have a Plan

The National Association of Securities Dealers (NASD) has adopted rules that require all its members to have business continuity plans. The NASD oversees the activities of more than 5,100 brokerage firms, approximately 130,800 branch offices and more than 658,770 registered securities representatives.

As of June 14, 2004, the rules apply to all NASD member firms. The requirements, which are specified in Rule 3510, begin with the following:

3510. Business Continuity Plans. (a) Each member must create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption. Such procedures must be reasonably designed to enable the member

to meet its existing obligations to customers. In addition, such procedures must address the member's existing relationships with other broker-dealers and counter-parties. The business continuity plan must be made available promptly upon request to NASD staff.

NOTE:
The rules apply to every company that deals in securities, such as brokers, dealers, and their representatives, it does NOT apply to the listed companies themselves.
Electric Utilities WILL Need a Plan

The disaster recovery function relating to the electric utility grid is presently undergoing a change. Prior to 2005, the Federal Energy Regulatory Commission (FERC) could only coordinate volunteer efforts between utilities. This has changed with the adoption of Title XII of the Energy Policy Act of 2005 (16 U.S.C. 824o). That new law authorizes the FERC to create an Electric Reliability Organization (ERO).
The ERO will have the capability to adopt and enforce reliability standards for "all users, owners, and operators of the bulk power system" in the United States. At this time, FERC is in the process of finalizing the rules for the creation of the ERO. Once the ERO is created, it will begin the process of establishing reliability standards.

It is very safe to assume that the ERO will adopt standards for service restoration and disaster recovery, particularly after such widespread disasters as Hurricane Katrina.
Telecommunications Utilities SHOULD Have Plans, but MIGHT NOT

Telecommunications utilities are governed on the federal level by the Federal Communications Commission (FCC) for interstate services and by state Public Utility Commissions (PUCs) for services within the state.

The FCC has created the Network Reliability and Interoperability Council (NRIC). The role of the NRIC is to develop recommendations for the FCC and the telecommunications industry to "insure [sic] optimal reliability, security, interoperability and interconnectivity of, and accessibility to, public communications networks and the internet." The NRIC members are senior representatives of providers and users of telecommunications services and products, including telecommunications carriers, the satellite, cable television, wireless and computer industries, trade associations, labor and consumer representatives, manufacturers, research organizations, and government-related organizations.

There is no explicit provision that we could find that says telecommunications carriers must have a Disaster Recovery Plan. As I have stated frequently in this series of articles on disaster recovery, however, telecommunications facilities are tempting targets for terrorism. I have not changed my mind in that regard and urge caution.

You might also want to consider what the liability of a telephone company is if it does have a disaster that causes loss to your organization. In three words: It’s not much. The following is the statement used in most telephone company tariffs with regard to its liability:

The Telephone Company’s liability, if any, for its gross negligence or willful misconduct is not limited by this tariff. With respect to any other claim or suit, by a customer or any others, for damages arising out of mistakes, omissions, interruptions, delays or errors, or defects in transmission occurring in the course of furnishing services hereunder, the Telephone Company’s liability, if any, shall not exceed an amount equivalent to the proportionate charge to the customer for the period of service during which such mistake, omission, interruption, delay, error or defect in transmission or service occurs and continues. (Source, General Exchange Tariff for major carrier)

All Health Care Providers WILL Need a Disaster Recovery Plan
HIPAA is an acronym for the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, which amended the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act, the Act includes a section, Title II, entitled Administrative Simplification, requiring "Improved efficiency in healthcare delivery by standardizing electronic data interchange, and protection of confidentiality and security of health data through setting and enforcing standards."

The legislation called upon the Department of Health and Human Services (HHS) to publish new rules that will ensure security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present, or future.

The final Security Rule was published by HHS on February 20, 2003 and provides for a uniform level of protection of all health information that is housed or transmitted electronically and that pertains to an individual.

The Security Rule requires covered entities to ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) that the covered entity creates, receives, maintains, or transmits. It also requires entities to protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule, and ensure compliance by their workforce.

Required safeguards include application of appropriate policies and procedures, safeguarding physical access to ePHI, and ensuring that technical security measures are in place to protect networks, computers and other electronic devices.

Companies with More than 10 Employees

The United States Department of Labor has adopted numerous rules and regulations in regard to workplace safety as part of the Occupational Safety and Health Act. For example, 29 USC 654 specifically requires:

(a) Each employer:

(1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees;

(2) shall comply with occupational safety and health standards promulgated under this Act.

(b) Each employee shall comply with occupational safety and health standards and all rules, regulations, and orders issued pursuant to this Act which are applicable to his own actions and conduct.

Other Considerations or Expensive Research QUESTION NO: s for Lawyers (Sorry, Eddie!)

The Foreign Corrupt Practices Act of 1977
Internal Revenue Service (IRS) Law for Protecting Taxpayer Information
Food and Drug Administration (FDA) Mandated Requirements
Homeland Security and Terrorist Prevention
Pandemic (Bird Flu) Prevention
ISO 9000 Certification
Requirements for Radio and TV Broadcasters
Contract Obligations to Customers
Document Protection and Retention Laws
Personal Identity Theft...and MORE!

Suffice it to say you will need to check with your legal department for specific requirements in your business and industry!

I would like to thank my good friend, Eddie M. Pope, for his insightful contributions to this article, our upcoming book, and my ever-growing pool of lawyer jokes. If you want more information on the legal aspects of recovery planning, Eddie can be contacted at my company or via email at mailto:mempope@tellawcomlabs.com. (Eddie cannot, of course, give you legal advice, but he can point you in the right direction.)

I hope this article helps you better understand the complex realities of the legal reasons why we plan and wish you the best of luck

See original article at: http://www.informit.com/articles/article.aspx?p=777896

See another interesting article on the subject at: http://www.informit.com/articles/article.aspx?p=677910&seqNum=1

References used for this question:

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 281).

Topic 5, Cryptography

Question No : 9 - (Topic 5)

Which of the following offers confidentiality to an e-mail message?

A. The sender encrypting it with its private key.
B. The sender encrypting it with its public key.
C. The sender encrypting it with the receiver's public key.
D. The sender encrypting it with the receiver's private key.

Answer: C

Explanation: An e-mail message's confidentiality is protected when encrypted with the receiver's public key, because he is the only one able to decrypt the message. The sender is not supposed to have the receiver's private key. By encrypting a message with its private key, anybody possessing the corresponding public key would be able to read the message. By encrypting the message with its public key, not even the receiver would be able to read the message.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 517).

Question No : 10 - (Topic 5)

What is the key size of the International Data Encryption Algorithm (IDEA)?

A. 64 bits
B. 128 bits
C. 160 bits
D. 192 bits

Answer: B

Explanation: The International Data Encryption Algorithm (IDEA) is a block cipher that operates on 64 bit blocks of data with a 128-bit key. The data blocks are divided into 16 smaller blocks and each has eight rounds of mathematical functions performed on it. It is used in the PGP encryption software.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 3).