reduce private harms such as identity theft due to unauthorized access. The U.S. Gramm-Leach-Bliley Act (GLBA) Safeguards Rule and the broader European Directive 95/46/EC, Article 17, both require that companies employ reasonable or appropriate administrative and technical security measures to protect consumer information.

The GLBA is a U.S. Federal law enacted by U.S. Congress in 1998 to allow consolidation among commercial banks. The GLBA Safeguards Rule is U.S. Federal regulation created in reaction to the GLBA and enforced by the U.S.
Federal Trade Commission (FTC). The Safeguards Rule requires companies to implement a security plan to protect the confidentiality and integrity of consumer personal information and requires the designation of an individual responsible for compliance.

Because these laws and regulations govern consumer personal information, they can lead to new requirements for information systems for which companies are responsible to comply.

The act of compliance includes demonstrating due diligence, which is defined as "reasonable efforts that persons make to satisfy legal requirements or discharge their legal obligations". Reasonableness in software systems includes industries standards and may allow for imperfection. Lawyers representing firms and other organizations, regulators, system administrators and engineers all face considerable challenge in determining what constitutes "reasonable" security measures for several reasons, including:

1. Compliance changes with the emergence of new security vulnerabilities due to innovations in information technology;

2. Compliance requires knowledge of specific security measures, however publicly available best practices typically include general goals and only address broad categories of vulnerability; and

3. Compliance is a best-effort practice, because improving security is costly and companies must prioritize security spending commensurate with risk of non-compliance. In general, the costs of improved security are certain, but the improvement in security depends on unknown variables and probabilities outside the control of companies.

The following reference(s) were used for this question:

KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 315.
http://www.cs.cmu.edu/~breaux/publications/tdbreaux-cose10.pdf

QUESTION 587
Within the legal domain what rule is concerned with the legality of how the evidence was gathered ?

A. Exclusionary rule
B. Best evidence rule
C. Hearsay rule
D. Investigation rule

Correct Answer: A
Explanation:
The exclusionary rule mentions that evidence must be gathered legally or it can't be used.

The principle based on federal Constitutional Law that evidence illegally seized by law enforcement officers in violation of a suspect's right to be free from unreasonable searches and

seizures cannot be used against the suspect in a criminal prosecution. The exclusionary rule is designed to exclude evidence obtained in violation of a criminal defendant's Fourth Amendment rights. The Fourth Amendment protects against unreasonable searches and seizures by law enforcement personnel. If the search of a criminal suspect is unreasonable, the evidence obtained in the search will be excluded from trial.

The exclusionary rule is a court-made rule. This means that it was created not in statutes passed by legislative bodies but rather by the U.S. Supreme Court. The exclusionary rule applies in federal courts by virtue of the Fourth Amendment. The Court has ruled that it applies in state courts although the due process clause of the Fourteenth Amendment.(The Bill of Rights--the first ten amendments-- applies to actions by the federal government. The Fourteenth Amendment, the Court has held, makes most of the protections in the Bill of Rights applicable to actions by the states.)

The exclusionary rule has been in existence since the early 1900s. Before the rule was fashioned, any evidence was admissible in a criminal trial if the judge found the evidence to be relevant. The manner in which the evidence had been seized was not an issue. This began to change in 1914, when the U.S. Supreme Court devised a way to enforce the Fourth Amendment. In Weeks v. United States, 232 U.S. 383, 34 S. Ct. 341, 58 L. Ed. 652 (1914), a federal agent had conducted a warrantless search for evidence of gambling at the home of Fremont Weeks. The evidence seized in the search was used at trial, and Weeks was convicted. On appeal, the Court held that the Fourth Amendment barred the use of evidence secured through a warrantless search. Weeks's conviction was reversed, and thus was born the exclusionary rule.

The best evidence rule concerns limiting potential for alteration. The best evidence rule is a common law rule of evidence which can be traced back at least as far as the 18th century. In Omychund v Barker (1745) 1 Atk, 21, 49; 26 ER 15, 33, Lord Harwicke stated that no evidence was admissible unless it was "the best that the nature of the case will allow". The general rule is that secondary evidence, such as a copy or facsimile, will be not admissible if an original document exists, and is not unavailable due to destruction or other circumstances indicating unavailability.

The rationale for the best evidence rule can be understood from the context in which it arose: in the eighteenth century a copy was usually made by hand by a clerk (or even a litigant). The best evidence rule was predicated on the assumption that, if the original was not produced, there was a significant chance of error or fraud in relying on such a copy. The hearsay rule concerns computer-generated evidence, which is considered second- hand evidence.
Hearsay is information gathered by one person from another concerning some event, condition, or thing of which the first person had no direct experience. When submitted as evidence, such statements are called hearsay evidence. As a legal term, "hearsay" can also have the narrower meaning of the use of such information as evidence to prove the truth of what is asserted. Such use of "hearsay evidence" in court is generally not allowed.
This prohibition is called the hearsay rule.

For example, a witness says "Susan told me Tom was in town". Since the witness did not see Tom in town, the statement would be hearsay evidence to the fact that Tom was in town, and not admissible. However, it would be admissible as evidence that Susan said Tom was in town, and on the issue of her knowledge of whether he was in town.

Hearsay evidence has many exception rules. For the purpose of the exam you must be familiar with the business records exception rule to the Hearsay Evidence. The business records created during the ordinary course of business are considered reliable and can usually be brought in under this exception if the proper foundation is laid when the records are introduced into evidence. Depending on which jurisdiction the case is in, either the records custodian or someone with knowledge of the records must lay a foundation for the records. Logs that are collected as

part of a document business process being carried at regular interval would fall under this exception. They could be presented in court and not be considered Hearsay.

Investigation rule is a detractor.

Source:
ROTHKE, Ben, CISSP CBK Review presentation on domain 9.
The FREE Online Law Dictionary at: http://legal-dictionary.thefreedictionary.com/Exclusionary+Rule
Wikipedia has a nice article on this subject at: http://en.wikipedia.org/wiki/Exclusionary_rule
http://en.wikipedia.org/wiki/Hearsay_in_United_States_law#Hearsay_exceptions

QUESTION 588
Which of the following is less likely to accompany a contingency plan, either within the plan itself or in the form of an appendix?

A. Contact information for all personnel.
B. Vendor contact information, including offsite storage and alternate site.
C. Equipment and system requirements lists of the hardware, software, firmware and other resources required to support system operations.
D. The Business Impact Analysis.

Correct Answer: A
Explanation:
Why is this the correct answer?
Simply because it is WRONG, you would have contact information for your emergency personnel within the plan but NOT for ALL of your personnel. Be careful of words such as ALL.
According to NIST's Special publication 800-34, contingency plan appendices provide key details not contained in the main body of the plan. The appendices should reflect the specific technical, operational, and management contingency requirements of the given system. Contact information for recovery team personnel (not all personnel) and for vendor should be included, as well as detailed system requirements to allow for supporting of system operations. The Business Impact Analysis (BIA) should also be included as an appendix for reference should the plan be activated.

Reference(s) used for this question:
SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems

QUESTION 589
When referring to a computer crime investigation, which of the following would be the MOST important step required in order to preserve and maintain a proper chain of custody of evidence:

A. Evidence has to be collected in accordance with all laws and all legal regulations.
B. Law enforcement officials should be contacted for advice on how and when to collect critical information.
C. Verifiable documentation indicating the who, what, when, where, and how the evidence was handled should be available.
D. Log files containing information regarding an intrusion are retained for at least as long as normal business records, and longer in the case of an ongoing investigation.

Correct Answer: C
Explanation:
Two concepts that are at the heart of dealing effectively with digital/electronic evidence, or any

evidence for that matter, are the chain of custody and authenticity/integrity.

The chain of custody refers to the who, what, when, where, and how the evidence was handled--from its identification through its entire life cycle, which ends with destruction or permanent archiving.

Any break in this chain can cast doubt on the integrity of the evidence and on the professionalism of those directly involved in either the investigation or the collection and handling of the evidence. The chain of custody requires following a formal process that is well documented and forms part of a standard operating procedure that is used in all cases, no exceptions.

The following are incorrect answers:
Evidence has to be collected in accordance with all laws and legal regulations. Evidence would have to be collected in accordance with applicable laws and regulations but not necessarily with ALL laws and regulations. Only laws and regulations that applies would be followed.

Law enforcement officials should be contacted for advice on how and when to collect critical information. It seems you failed to do your homework, once you have an incident it is a bit late to do this. Proper crime investigation as well as incident response is all about being prepared ahead of time. Obviously, you are improvising if you need to call law enforcement to find out what to do. It is a great way of contaminating your evidence by mistake if you don't have a well documented processs with clear procedures that needs to be followed.

Log files containing information regarding an intrusion are retained for at least as long as normal business records, and longer in the case of an ongoing investigation. Specific legal requirements exists for log retention and they are not the same as normal business records. Laws such as Basel, HIPPAA, SOX, and others has specific requirements.

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 23465-23470). Auerbach Publications. Kindle Edition.
And ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (pages 282-285).

QUESTION 590
In order to be able to successfully prosecute an intruder:

A. A point of contact should be designated to be responsible for communicating with law enforcement and other external agencies.
B. A proper chain of custody of evidence has to be preserved.
C. Collection of evidence has to be done following predefined procedures.
D. Whenever possible, analyze a replica of the compromised resource, not the original, thereby avoiding inadvertently tamping with evidence.

Correct Answer: B
Explanation:
If you intend on prosecuting an intruder, evidence has to be collected in a lawful manner and, most importantly, protected through a secure chain-of-custody procedure that tracks who has been involved in handling the evidence and where it has been stored. All other choices are all important points, but not the best answer, since no prosecution is possible without a proper, provable chain of custody of evidence.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (pages 282-285).

QUESTION 591
An Intrusion Detection System (IDS) is what type of control?

A. A preventive control.
B. A detective control.
C. A recovery control.
D. A directive control.

Correct Answer: D
Explanation:
These controls can be used to investigate what happen after the fact. Your IDS may collect information on where the attack came from, what port was use, and other details that could be used in the investigation steps.

"Preventative control" is incorrect. Preventative controls preclude events or actions that might compromise a system or cause a policy violation. An intrusion prevention system would be an example of a preventative control.

"Recovery control" is incorrect. Recover controls include processes used to return the system to a secure state after the occurrence of a security incident. Backups and redundant components are examples of recovery controls.

"Directive controls" is incorrect. Directive controls are administrative instruments such as policies, procedures, guidelines, and aggreements. An acceptable use policy is an example of a directive control.

References:
CBK, pp. 646 - 647

QUESTION 592
To understand the 'whys' in crime, many times it is necessary to understand MOM. Which of the following is not a component of MOM?

A. Opportunities
B. Methods
C. Motivation
D. Means

Correct Answer: B
Explanation:
To understand the whys in crime, many times it is necessary to understand the Motivations, Opportunities, and Means (MOM). Motivations are the who and why of a crime. Opportunities are the where and when of a crime, and Means pertains to the capabilities a criminal would need to be successful. Methods is not a component of MOM.

QUESTION 593
Recovery Site Strategies for the technology environment depend on how much downtime an organization can tolerate before the recovery must be completed. What would you call a strategy where the alternate site is internal, standby ready, with all the technology and equipment necessary to run the applications?

A. External Hot site
B. Warm Site