to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate, cost-effective controls to achieve and maintain an acceptable level or risk.

Due Diligence is identifying possible risks that could affect a company based on best practices and standards.

Reference(s) used for this question:
STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page B-3).

QUESTION 601
What would BEST define risk management?

A. The process of eliminating the risk
B. The process of assessing the risks
C. The process of reducing risk to an acceptable level
D. The process of transferring risk

Correct Answer: C
Explanation:
This is the basic process of risk management.

Risk is the possibility of damage happening and the ramifications of such damage should it occur. Information risk management (IRM) is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. There is no such thing as a 100 percent secure environment. Every environment has vulnerabilities and threats to a certain degree.

The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.

Proper risk management requires a strong commitment from senior management, a documented process that supports the organization's mission, an information risk management (IRM) policy and a delegated IRM team. Once you've identified your company's acceptable level of risk, you need to develop an information risk management policy.

The IRM policy should be a subset of the organization's overall risk management policy (risks to a company include more than just information security issues) and should be mapped to the organizational security policies, which lay out the acceptable risk and the role of security as a whole in the organization. The IRM policy is focused on risk management while the security policy is very high-level and addresses all aspects of security. The IRM policy should address the following items:

Objectives of IRM team
Level of risk the company will accept and what is considered an acceptable risk (as defined in the previous article)
Formal processes of risk identification
Connection between the IRM policy and the organization's strategic planning processes
Responsibilities that fall under IRM and the roles that are to fulfill them Mapping of risk to internal controls
Approach for changing staff behaviors and resource allocation in response to risk analysis
Mapping of risks to performance targets and budgets Key indicators to monitor the effectiveness

of controls

Shon Harris provides a 10,000-foot view of the risk management process below:
A big question that companies have to deal with is, "What is enough security?" This can be restated as, "What is our acceptable risk level?" These two questions have an inverse relationship. You can't know what constitutes enough security unless you know your necessary baseline risk level.

To set an enterprise-wide acceptable risk level for a company, a few things need to be investigated and understood. A company must understand its federal and state legal requirements, its regulatory requirements, its business drivers and objectives, and it must carry out a risk and threat analysis. (I will dig deeper into formalized risk analysis processes in a later article, but for now we will take a broad approach.) The result of these findings is then used to define the company's acceptable risk level, which is then outlined in security policies, standards, guidelines and procedures.

Although there are different methodologies for enterprise risk management, the core components of any risk analysis is made up of the following:

Identify company assets
Assign a value to each asset
Identify each asset's vulnerabilities and associated threats Calculate the risk for the identified assets

Once these steps are finished, then the risk analysis team can identify the necessary countermeasures to mitigate the calculated risks, carry out cost/benefit analysis for these countermeasures and report to senior management their findings.

When we look at information security, there are several types of risk a corporation needs to be aware of and address properly. The following items touch on the major categories:
Physical damage Fire, water, vandalism, power loss, and natural disasters

Human interaction Accidental or intentional action or inaction that can disrupt productivity

Equipment malfunction Failure of systems and peripheral devices

Inside and outside attacks Hacking, cracking, and attacking

Misuse of data Sharing trade secrets, fraud, espionage, and theft

Loss of data Intentional or unintentional loss of information through destructive means

Application error Computation errors, input errors, and buffer overflows

The following answers are incorrect:

The process of eliminating the risk is not the best answer as risk cannot be totally eliminated.

The process of assessing the risks is also not the best answer.

The process of transferring risk is also not the best answer and is one of the ways of handling a risk after a risk analysis has been performed.

References:
Shon Harris, AIO v3, Chapter 3: Security Management Practices, Page: 66-68 and

http://searchsecurity.techtarget.com/tip/Understanding-risk

QUESTION 602
Which of the following steps should be one of the first step performed in a Business Impact Analysis (BIA)?

A. Identify all CRITICAL business units within the organization.
B. Evaluate the impact of disruptive events.
C. Estimate the Recovery Time Objectives (RTO).
D. Identify and Prioritize Critical Organization Functions

Correct Answer: D
Explanation:
Project Initiation and Management

This is the first step in building the Business Continuity program is project initiation and management. During this phase, the following activities will occur:

Obtain senior management support to go forward with the project Define a project scope, the objectives to be achieved, and the planning assumptions Estimate the project resources needed to be successful, both human resources and financial resources
Define a timeline and major deliverables of the project In this phase, the program will be managed like a project, and a project manager should be assigned to the BC and DR domain.

The next step in the planning process is to have the planning team perform a BIA. The BIA will help the company decide what needs to be recovered, and how quickly. Mission functions are typically designated with terms such as critical, essential, supporting and nonessential to help determine the appropriate prioritization.

One of the first steps of a BIA is to Identify and Prioritize Critical Organization Functions. All organizational functions and the technology that supports them need to be classified based on their recovery priority. Recovery time frames for organization operations are driven by the consequences of not performing the function. The consequences may be the result of organization lost during the down period; contractual commitments not met resulting in fines or lawsuits, lost goodwill with customers.

All other answers are incorrect.

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 21073-21075). Auerbach Publications. Kindle Edition.
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20697-20710). Auerbach Publications. Kindle Edition.

QUESTION 603
Which of the following could be BEST defined as the likelihood of a threat agent taking advantage of a vulnerability?

A. A risk
B. A residual risk
C. An exposure
D. A countermeasure

Correct Answer: A
Explanation:
Risk is the likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact. If a firewall has several ports open , there is a higher likelihood that an intruder will use one to access the network in an unauthorized method.

The following answers are incorrect :
Residual Risk is very different from the notion of total risk. Residual Risk would be the risks that still exists after countermeasures have been implemented. Total risk is the amount of risk a company faces if it chooses not to implement any type of safeguard.

Exposure: An exposure is an instance of being exposed to losses from a threat agent.

Countermeasure: A countermeasure or a safeguard is put in place to mitigate the potential risk. Examples of countermeasures include strong password management , a security guard.

References:
SHON HARRIS ALL IN ONE 3rd EDITION
Chapter - 3: Security Management Practices , Pages: 57-59

QUESTION 604
Which of the following focuses on sustaining an organization's business functions during and after a disruption?

A. Business continuity plan
B. Business recovery plan
C. Continuity of operations plan
D. Disaster recovery plan

Correct Answer: A
Explanation:
A business continuity plan (BCP) focuses on sustaining an organization's business functions during and after a disruption. Information systems are considered in the BCP only in terms of their support to the larger business processes. The business recovery plan (BRP) addresses the restoration of business processes after an emergency. The BRP is similar to the BCP, but it typically lacks procedures to ensure continuity of critical processes throughout an emergency or disruption. The continuity of operations plan (COOP) focuses on restoring an organization's essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. The disaster recovery plan (DRP) applies to major, usually catastrophic events that deny access to the normal facility for an extended period. A DRP is narrower in scope than an IT contingency plan in that it does not address minor disruptions that do not require relocation.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 8).

QUESTION 605
Contracts and agreements are often times unenforceable or hard to enforce in which of the following alternate facility recovery agreement?

A. hot site
B. warm site
C. cold site

D. reciprocal agreement

Correct Answer: D
Explanation:
A reciprocal agreement is where two or more organizations mutually agree to provide facilities to the other if a disaster occurs. The organizations must have similiar hardware and software configurations. Reciprocal agreements are often not legally binding.

Reciprocal agreements are not contracts and cannot be enforced. You cannot force someone you have such an agreement with to provide processing to you.

Government regulators do not accept reciprocal agreements as valid disaster recovery sites.

Cold sites are empty computer rooms consisting only of environmental systems, such as air conditioning and raised floors, etc. They do not meet the requirements of most regulators and boards of directors that the disaster plan be tested at least annually.

Time Brokers promise to deliver processing time on other systems. They charge a fee, but cannot guaranty that processing will always be available, especially in areas that experienced multiple disasters.

With the exception of providing your own hot site, commercial hot sites provide the greatest protection. Most will allow you up to six weeks to restore your sites if you declare a disaster. They also permit an annual amount of time to test the Disaster Plan.

References:
OIG CBK Business Continuity and Disaster Recovery Planning (pages 368 - 369)

The following answers are incorrect:

hot site. Is incorrect because you have a contract in place stating what services are to be provided.
warm site. Is incorrect because you have a contract in place stating what services are to be provided.
cold site. Is incorrect because you have a contract in place stating what services are to be provided.

QUESTION 606
Which of the following backup method must be made regardless of whether Differential or Incremental methods are used?

A. Full Backup Method.
B. Incremental backup method.
C. Supplemental backup method.
D. Tape backup method.

Correct Answer: A
Explanation:
A Full Backup must be made regardless of whether Differential or Incremental methods are used.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69. And: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (pages 617-619).