vce trainer



Reference Solution for CISM.469q

CISM

CISM

Certified Information Security Manager

Licensed to Berend Post berend.post@it-university.nl

Score: 800/1000

Version:

Time Limit: 120 Minutes

Licensed to Berend Post berend.post@it-university.nl

Exam A (469 questions)

Question 1

A test plan to validate the security controls of a new system should be developed during which phase of the project?

- ☐ Testing
- ☐ Initiation
- ☒ Design
- ☐ Development

Explanation:

Explanation:

In the design phase, security checkpoints are defined and a test plan is developed. The testing phase is too late since the system has already been developed and is in production testing. In the initiation phase, the basic security objective of the project is acknowledged. Development is the coding phase and is too late to consider test plans.

Question 2

A web server in a financial institution that has been compromised using a super-user account has been isolated, and proper forensic processes have been followed. The next step should be to:

- ☐ rebuild the server from the last verified backup.
- ☐ place the web server in quarantine.
- ☐ shut down the server in an organized manner.
- ☒ rebuild the server with original media and relevant patches.

Explanation:

Explanation:

The original media should be used since one can never be sure of all the changes a super-user may have made nor the timelines in which these changes were made. Rebuilding from the last known verified backup is incorrect since the verified backup may have been compromised by the super-user at a different time. Placing the web server in quarantine should have already occurred in the forensic process. Shut down in an organized manner is out of sequence and no longer a problem. The forensic process is already finished and evidence has already been acquired.

Licensed to Berend Post berend.post@it-university.nl

Question 3

Which of the following would BEST address the risk of data leakage?

- ☐ File backup procedures
- ☐ Database integrity checks
- ☒ Acceptable use policies
- ☐ Incident response procedures

Explanation:

Explanation:

Acceptable use policies are the best measure for preventing the unauthorized disclosure of confidential information. The other choices do not address confidentiality of information.

Question 4

Information security managers should use risk assessment techniques to:

- ☒ justify selection of risk mitigation strategies.
- ☐ maximize the return on investment (ROD.
- ☐ provide documentation for auditors and regulators.
- ☐ quantify risks that would otherwise be subjective.

Explanation:

Explanation:

Information security managers should use risk assessment techniques to justify and implement a risk mitigation strategy as efficiently as possible. None of the other choices accomplishes that task, although they are important components.

Question 5

Which of the following messages would be MOST effective in obtaining senior management's commitment to information security management?

- ☒ Effective security eliminates risk to the business
- ☐ Adopt a recognized framework with metrics
- ☐ Security is a business product and not a process
- ☐ Security supports and protects the business

Licensed to Berend Post berend.post@it-university.nl

Question 6

Based on the information provided, which of the following situations presents the GREATEST information security risk for an organization with multiple, but small, domestic processing locations?

- ☐ Systems operation procedures are not enforced
- ☒ Change management procedures are poor
- ☐ Systems development is outsourced
- ☐ Systems capacity management is not performed

Explanation:

Explanation:

The lack of change management is a severe omission and will greatly increase information security risk. Since procedures are generally nonauthoritative, their lack of enforcement is not a primary concern. Systems that are developed by third-party vendors are becoming commonplace and do not represent an increase in security risk as much as poor change management. Poor capacity management may not necessarily represent a security risk.

Question 7

Quantitative risk analysis is MOST appropriate when assessment data:

- ☐ include customer perceptions.
- ☒ contain percentage estimates.
- ☐ do not contain specific details.
- ☐ contain subjective information.

Explanation:

Explanation:

Percentage estimates are characteristic of quantitative risk analysis. Customer perceptions, lack of specific details or subjective information lend themselves more to qualitative risk analysis.

Question 8

Which of the following would be MOST relevant to include in a cost-benefit analysis of a two-factor authentication system?

- ☐ Annual loss expectancy (ALE) of incidents
- ☐ Frequency of incidents
- ☒ Total cost of ownership (TCO)
- ☐ Approved budget for the project

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The total cost of ownership (TCO) would be the most relevant piece of information in that it would establish a cost baseline and it must be considered for the full life cycle of the control. Annual loss expectancy (ALE) and the frequency of incidents could help measure the benefit, but would have more of an indirect relationship as not all incidents may be mitigated by implementing a two-factor authentication system. The approved budget for the project may have no bearing on what the project may actually cost.

Question 9

An outsource service provider must handle sensitive customer information. Which of the following is MOST important for an information security manager to know?

- ☒ Security in storage and transmission of sensitive data
- ☐ Provider's level of compliance with industry standards
- ☐ Security technologies in place at the facility
- ☐ Results of the latest independent security review

Explanation:

Explanation:

Mow the outsourcer protects the storage and transmission of sensitive information will allow an information security manager to understand how sensitive data will be protected. Choice B is an important but secondary consideration. Choice C is incorrect because security technologies are not the only components to protect the sensitive customer information. Choice D is incorrect because an independent security review may not include analysis on how sensitive customer information would be protected.

Question 10

During the initiation phase of the system development life cycle (SDLC) for a software project, information security activities should address:

- ☐ baseline security controls.
- ☐ cost-benefit analyses.
- ☐ benchmarking security metrics.
- ☒ security objectives.

Licensed to Berend Post berend.post@it-university.nl

Question 11

On which of the following should a firewall be placed?

- ☐ Web server
- ☐ Intrusion detection system (IDS) server
- ☐ Screened subnet
- ☒ Domain boundary

Explanation:

Explanation:

A firewall should be placed on a (security) domain boundary. Placing it on a web server or screened subnet, which is a demilitarized zone (DMZ), does not provide any protection. Since firewalls should be installed on hardened servers with minimal services enabled, it is inappropriate to have the firewall and the intrusion detection system (IDS) on the same physical device.

Question 12

To help ensure that contract personnel do not obtain unauthorized access to sensitive information, an information security manager should PRIMARILY:

- ☐ set their accounts to expire in six months or less.
- ☒ avoid granting system administration roles.
- ☐ ensure they successfully pass background checks.
- ☐ ensure their access is approved by the data owner.

Explanation:

Explanation:

Contract personnel should not be given job duties that provide them with power user or other administrative roles that they could then use to grant themselves access to sensitive files. Setting expiration dates, requiring background checks and having the data owner assign access are all positive elements, but these will not prevent contract personnel from obtaining access to sensitive information.

Question 13

A business impact analysis (BIA) is the BEST tool for calculating:

- ☐ total cost of ownership.
- ☒ priority of restoration.
- ☐ annualized loss expectancy (ALE).
- ☐ residual risk.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

A business impact analysis (BIA) is the best tool for calculating the priority of restoration for applications. It is not used to determine total cost of ownership, annualized loss expectancy (ALE) or residual risk to the organization.

Question 14

Which of the following devices could potentially stop a Structured Query Language (SQL) injection attack?

- ☒ An intrusion prevention system (IPS)
- ☐ An intrusion detection system (IDS)
- ☐ A host-based intrusion detection system (HIDS)
- ☐ A host-based firewall

Explanation:

Explanation:

SQL injection attacks occur at the application layer. Most IPS vendors will detect at least basic sets of SQL injection and will be able to stop them. IDS will detect, but not prevent I IIDS will be unaware of SQL injection problems. A host-based firewall, be it on the web server or the database server, will allow the connection because firewalls do not check packets at an application layer.

Question 15

Risk assessment should be built into which of the following systems development phases to ensure that risks are addressed in a development project?

- ☐ Programming
- ☐ Specification
- ☐ User testing
- ☒ Feasibility

Explanation:

Explanation:

Risk should be addressed as early as possible in the development cycle. The feasibility study should include risk assessment so that the cost of controls can be estimated before the project proceeds. Risk should also be considered in the specification phase where the controls are designed, but this would still be based on the assessment carried out in the feasibility study. Assessment would not be relevant in choice A or C.

Licensed to Berend Post berend.post@it-university.nl

Question 16

Before engaging outsourced providers, an information security manager should ensure that the organization's data classification requirements:

- ☐ are compatible with the provider's own classification.
- ☐ are communicated to the provider.
- ☐ exceed those of the outsourcer.
- ☒ are stated in the contract.

Explanation:

Explanation:

The most effective mechanism to ensure that the organization's security standards are met by a third party, would be a legal agreement. Choices A. B and C are acceptable options, but not as comprehensive or as binding as a legal contract.

Question 17

Which of the following defines the triggers within a business continuity plan (BCP)?

- ☐ Disaster recovery plan
- ☐ Needs of the organization
- ☐ Gap analysis
- ☒ Information security policy

Question 18

When performing an information risk analysis, an information security manager should FIRST:

- ☐ establish the ownership of assets.
- ☐ evaluate the risks to the assets.
- ☒ take an asset inventory.
- ☐ categorize the assets.

Explanation:

Explanation:

Assets must be inventoried before any of the other choices can be performed.

Licensed to Berend Post berend.post@it-university.nl

Question 19

Which of the following would be MOST useful in developing a series of recovery time objectives (RTOs)?

- ☐ Gap analysis
- ☐ Regression analysis
- ☐ Risk analysis
- ☒ Business impact analysis

Explanation:

Explanation:

Recovery time objectives (RTOs) are a primary deliverable of a business impact analysis. RTOs relate to the financial impact of a system not being available. A gap analysis is useful in addressing the differences between the current state and an ideal future state. Regression analysis is used to test changes to program modules. Risk analysis is a component of the business impact analysis.

Question 20

A company recently developed a breakthrough technology. Since this technology could give this company a significant competitive edge, which of the following would FIRST govern how this information is to be protected?

- ☐ Access control policy
- ☒ Data classification policy
- ☐ Encryption standards
- ☐ Acceptable use policy

Explanation:

Explanation:

Data classification policies define the level of protection to be provided for each category of data. Without this mandated ranking of degree of protection, it is difficult to determine what access controls or levels of encryption should be in place. An acceptable use policy is oriented more toward the end user and, therefore, would not specifically address what controls should be in place to adequately protect information.

Licensed to Berend Post berend.post@it-university.nl

Question 21

Which of the following will BEST prevent an employee from using a USB drive to copy files from desktop computers?

- ☒ Restrict the available drive allocation on all PCs
- ☐ Disable universal serial bus (USB) ports on all desktop devices
- ☐ Conduct frequent awareness training with noncompliance penalties
- ☐ Establish strict access controls to sensitive information

Explanation:

Explanation:

Restricting the ability of a PC to allocate new drive letters ensures that universal serial bus (USB) drives or even CD-writers cannot be attached as they would not be recognized by the operating system. Disabling USB ports on all machines is not practical since mice and other peripherals depend on these connections. Awareness training and sanctions do not prevent copying of information nor do access controls.

Question 22

An organization has verified that its customer information was recently exposed. Which of the following is the FIRST step a security manager should take in this situation?

- ☐ Inform senior management.
- ☒ Determine the extent of the compromise.
- ☐ Report the incident to the authorities.
- ☐ Communicate with the affected customers.

Explanation:

Explanation:

Before reporting to senior management, affected customers or the authorities, the extent of the exposure needs to be assessed.

Question 23

In order to ensure separation of duties, which of the following activities is BEST performed by someone other than the system administrator?

- ☒ Deleting system logs
- ☐ Using system utilities
- ☐ Monitoring system utilization
- ☐ Defining system recovery procedures

Licensed to Berend Post berend.post@it-university.nl

Question 24

An organization with a maturing incident response program conducts post-incident reviews for all major information security incidents. The PRIMARY goal of these reviews should be to:

- ☒ document and report the root cause of the incidents for senior management.
- ☐ identify security program gaps or systemic weaknesses that need correction.
- ☐ prepare properly vetted notifications regarding the incidents to external parties.
- ☐ identify who should be held accountable for the security incidents.

Question 25

A multinational organization wants to monitor outbound traffic for data leakage from the use of unapproved cloud services. Which of the following should be the information security manager's GREATEST consideration when implementing this control?

- ☐ Security of cloud services
- ☒ Data privacy regulations
- ☐ Resistance from business users
- ☐ Allocation of monitoring resources

Question 26

Which of the following would be MOST helpful when justifying the funding required for a compensating control?

- ☐ Threat assessment
- ☒ Business impact analysis
- ☐ Business case
- ☐ Risk analysis

Question 27

Which of the following techniques MOST clearly indicates whether specific risk-reduction controls should be implemented?

- ☒ Countermeasure cost-benefit analysis
- ☐ Penetration testing
- ☐ Frequent risk assessment programs
- ☐ Annual loss expectancy (ALE) calculation

Explanation:

Explanation:

In a countermeasure cost-benefit analysis, the annual cost of safeguards is compared with the expected cost of loss. This can then be used to justify a specific control measure. Penetration testing may indicate the extent of a weakness but, by itself, will not establish the cost/benefit of a control.

Licensed to Berend Post berend.post@it-university.nl

Frequent risk assessment programs will certainly establish what risk exists but will not determine the maximum cost of controls. Annual loss expectancy (ALE) is a measure which will contribute to the value of the risk but. alone, will not justify a control.

Question 28

An e-commerce order fulfillment web server should generally be placed on which of the following?

- ☐ Internal network
- ☒ Demilitarized zone (DMZ)
- ☐ Database server
- ☐ Domain controller

Explanation:

Explanation:

An e-commerce order fulfillment web server should be placed within a DMZ to protect it and the internal network from external attack. Placing it on the internal network would expose the internal network to potential attack from the Internet. Since a database server should reside on the internal network, the same exposure would exist. Domain controllers would not normally share the same physical device as a web server.

Question 29

Detailed business continuity plans should be based PRIMARILY on:

- ☐ consideration of different alternatives.
- ☐ the solution that is least expensive.
- ☐ strategies that cover all applications.
- ☒ strategies validated by senior management.

Explanation:

Explanation:

A recovery strategy identifies the best way to recover a system in ease of disaster and provides guidance based on detailed recovery procedures that can be developed. Different strategies should be developed and all alternatives presented to senior management. Senior management should select the most appropriate strategy from the alternatives provided. The selected strategy should be used for further development of the detailed business continuity plan. The selection of strategy depends on criticality of the business process and applications supporting the processes. It need not necessarily cover all applications. All recovery strategies have associated costs, which include costs of preparing for disruptions and putting them to use in the event of a disruption. The latter can be insured against, but not the former. The best recovery option need not be the least expensive.

Licensed to Berend Post berend.post@it-university.nl

Question 30

Which of the following presents the GREATEST challenge in calculating return on investment (ROI) in the security environment?

- ☒ Number of incidents cannot be predetermined
- ☐ Project cost overruns cannot be anticipated
- ☐ Cost of security tools is difficult to estimate
- ☐ Costs of security incidents cannot be estimated

Question 31

What is the FIRST action an information security manager should take when a company laptop is reported stolen?

- ☐ Evaluate the impact of the information loss
- ☐ Update the corporate laptop inventory
- ☒ Ensure compliance with reporting procedures
- ☐ Disable the user account immediately

Explanation:

Explanation:

The key step in such an incident is to report it to mitigate any loss. After this, the other actions should follow.

Question 32

Which of the following is the MOST important action to take when engaging third-party consultants to conduct an attack and penetration test?

- ☐ Request a list of the software to be used
- ☐ Provide clear directions to IT staff
- ☐ Monitor intrusion detection system (IDS) and firewall logs closely
- ☒ Establish clear rules of engagement

Explanation:

Explanation:

It is critical to establish a clear understanding on what is permissible during the engagement. Otherwise, the tester may inadvertently trigger a system outage or inadvertently corrupt files. Not as important, but still useful, is to request a list of what software will be used. As for monitoring the intrusion detection system (IDS) and firewall, and providing directions to IT staff, it is better not to alert those responsible for monitoring (other than at the management level), so that the effectiveness of that monitoring can be accurately assessed.

Licensed to Berend Post berend.post@it-university.nl

Question 33

What is the BEST way to ensure data protection upon termination of employment?

- ☐ Retrieve identification badge and card keys
- ☐ Retrieve all personal computer equipment
- ☐ Erase all of the employee's folders
- ☒ Ensure all logical access is removed

Explanation:

Explanation:

Ensuring all logical access is removed will guarantee that the former employee will not be able to access company data and that the employee's credentials will not be misused. Retrieving identification badge and card keys would only reduce the capability to enter the building. Retrieving the personal computer equipment and the employee's folders are necessary tasks, but that should be done as a second step.

Question 34

When a proposed system change violates an existing security standard, the conflict would be BEST resolved by:

- ☐ calculating the residual risk.
- ☐ enforcing the security standard.
- ☐ redesigning the system change.
- ☒ implementing mitigating controls.

Question 35

Which of the following is MOST important in developing a security strategy?

- ☐ Creating a positive business security environment
- ☒ Understanding key business objectives
- ☐ Having a reporting line to senior management
- ☐ Allocating sufficient resources to information security

Explanation:

Explanation:

Alignment with business strategy is of utmost importance. Understanding business objectives is critical in determining the security needs of the organization.

Licensed to Berend Post berend.post@it-university.nl

Question 36

Requiring all employees and contractors to meet personnel security/suitability requirements commensurate with their position sensitivity level and subject to personnel screening is an example of a security:

- ☒ policy.
- ☐ strategy.
- ☐ guideline
- ☐ baseline.

Explanation:

Explanation:

A security policy is a general statement to define management objectives with respect to security. The security strategy addresses higher level issues. Guidelines are optional actions and operational tasks. A security baseline is a set of minimum requirements that is acceptable to an organization.

Question 37

The decision on whether new risks should fall under periodic or event-driven reporting should be based on which of the following?

- ☐ Mitigating controls
- ☒ Visibility of impact
- ☐ Likelihood of occurrence
- ☐ Incident frequency

Explanation:

Explanation:

Visibility of impact is the best measure since it manages risks to an organization in the timeliest manner. Likelihood of occurrence and incident frequency are not as relevant. Mitigating controls is not a determining factor on incident reporting.

Question 38

An information security manager has been asked to develop a change control process. What is the FIRST thing the information security manager should do?

- ☐ Research best practices
- ☒ Meet with stakeholders
- ☐ Establish change control procedures
- ☐ Identify critical systems

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

No new process will be successful unless it is adhered to by all stakeholders; to the extent stakeholders have input, they can be expected to follow the process. Without consensus agreement from the stakeholders, the scope of the research is too wide; input on the current environment is necessary to focus research effectively. It is premature to implement procedures without stakeholder consensus and research. Without knowing what the process will be the parameters to baseline are unknown as well.

Question 39

An account with full administrative privileges over a production file is found to be accessible by a member of the software development team. This account was set up to allow the developer to download nonsensitive production data for software testing purposes. The information security manager should recommend which of the following?

- ☒ Restrict account access to read only
- ☐ Log all usage of this account
- ☐ Suspend the account and activate only when needed
- ☐ Require that a change request be submitted for each download

Explanation:

Explanation:

Administrative accounts have permission to change data. This is not required for the developers to perform their tasks. Unauthorized change will damage the integrity of the data. Logging all usage of the account, suspending the account and activating only when needed, and requiring that a change request be submitted for each download will not reduce the exposure created by this excessive level of access. Restricting the account to read only access will ensure that the integrity can be maintained while permitting access.

Question 40

Who would be in the BEST position to determine the recovery point objective (RPO) for business applications?

- ☐ Business continuity coordinator
- ☒ Chief operations officer (COO)
- ☐ Information security manager
- ☐ Internal audit

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The recovery point objective (RPO) is the processing checkpoint to which systems are recovered. In addition to data owners, the chief operations officer (COO) is the most knowledgeable person to make this decision. It would be inappropriate for the information security manager or an internal audit to determine the RPO because they are not directly responsible for the data or the operation.

Question 41

What is the BEST defense against a Structured Query Language (SQL) injection attack?

- ☐ Regularly updated signature files
- ☐ A properly configured firewall
- ☐ An intrusion detection system
- ☒ Strict controls on input fields

Explanation:

Explanation:

Structured Query Language (SQL) injection involves the typing of programming command statements within a data entry field on a web page, usually with the intent of fooling the application into thinking that a valid password has been entered in the password entry field. The best defense against such an attack is to have strict edits on what can be typed into a data input field so that programming commands will be rejected. Code reviews should also be conducted to ensure that such edits are in place and that there are no inherent weaknesses in the way the code is written; software is available to test for such weaknesses. All other choices would fail to prevent such an attack.

Question 42

Which of the following is the MOST important area of focus when examining potential security compromise of a new wireless network?

- ☐ Signal strength
- ☒ Number of administrators
- ☐ Bandwidth
- ☐ Encryption strength

Explanation:

Explanation:

The number of individuals with access to the network configuration presents a security risk. Encryption strength is an area where wireless networks tend to fall short; however, the potential to compromise the entire network is higher when an inappropriate number of people can alter the configuration. Signal strength and network bandwidth are secondary issues.

Licensed to Berend Post berend.post@it-university.nl

Question 43

The return on investment of information security can BEST be evaluated through which of the following?

- ☒ Support of business objectives
- ☐ Security metrics
- ☐ Security deliverables
- ☐ Process improvement models

Explanation:

Explanation:

One way to determine the return on security investment is to illustrate how information security supports the achievement of business objectives. Security metrics measure improvement and effectiveness within the security practice but do not tie to business objectives. Similarly, listing deliverables and creating process improvement models does not necessarily tie into business objectives.

Question 44

An information security manager is asked to provide evidence that the organization is fulfilling its legal obligation to protect personally identifiable information (PII).

Which of the following would be MOST helpful for this purpose?

- ☒ Metrics related to program effectiveness
- ☐ Written policies and standards
- ☐ Privacy awareness training
- ☐ Risk assessments of privacy-related applications

Question 45

An information security team is investigating an alleged breach of an organization's network. Which of the following would be the BEST single source of evidence to review?

- ☐ Intrusion detection system
- ☒ SIEM tool
- ☐ Antivirus software
- ☐ File integrity monitoring software

Licensed to Berend Post berend.post@it-university.nl

Question 46

The PRIMARY objective of a risk management program is to:

- ☐ minimize inherent risk.
- ☐ eliminate business risk.
- ☐ implement effective controls.
- ☒ minimize residual risk.

Explanation:

Explanation:

The goal of a risk management program is to ensure that residual risk remains within manageable levels. Management of risk does not always require the removal of inherent risk nor is this always possible. A possible benefit of good risk management is to reduce insurance premiums, but this is not its primary intention. Effective controls are naturally a clear objective of a risk management program, but with the choices given, choice C is an incomplete answer.

Question 47

The security responsibility of data custodians in an organization will include:

- ☐ assuming overall protection of information assets.
- ☐ determining data classification levels.
- ☐ implementing security controls in products they install.
- ☒ ensuring security measures are consistent with policy.

Explanation:

Explanation:

Security responsibilities of data custodians within an organization include ensuring that appropriate security measures are maintained and are consistent with organizational policy. Executive management holds overall responsibility for protection of the information assets. Data owners determine data classification levels for information assets so that appropriate levels of controls can be provided to meet the requirements relating to confidentiality, integrity and availability. Implementation of information security in products is the responsibility of the IT developers.

Licensed to Berend Post berend.post@it-university.nl

Question 48

Which of the following would be of GREATEST importance to the security manager in determining whether to accept residual risk?

- ☐ Historical cost of the asset
- ☐ Acceptable level of potential business impacts
- ☒ Cost versus benefit of additional mitigating controls
- ☐ Annualized loss expectancy (ALE)

Explanation:

Explanation:

The security manager would be most concerned with whether residual risk would be reduced by a greater amount than the cost of adding additional controls. The other choices, although relevant, would not be as important.

Question 49

An organization plans to allow employees to use their own devices on the organization's network. Which of the following is the information security manager's BEST course of action?

- ☐ Implement automated software
- ☒ Assess associated risk
- ☐ Conduct awareness training
- ☐ Update the security policy

Question 50

Which of the following groups would be in the BEST position to perform a risk analysis for a business?

- ☐ External auditors
- ☐ A peer group within a similar business
- ☒ Process owners
- ☐ A specialized management consultant

Explanation:

Explanation:

Process owners have the most in-depth knowledge of risks and compensating controls within their environment. External parties do not have that level of detailed knowledge on the inner workings of the business. Management consultants are expected to have the necessary skills in risk analysis techniques but are still less effective than a group with intimate knowledge of the business.

Licensed to Berend Post berend.post@it-university.nl

Question 51

Ongoing tracking of remediation efforts to mitigate identified risks can BEST be accomplished through the use of which of the following?

- ☐ Tree diagrams
- ☐ Venn diagrams
- ☒ Heat charts
- ☐ Bar charts

Explanation:

Explanation:

Meat charts, sometimes referred to as stoplight charts, quickly and clearly show the current status of remediation efforts. Venn diagrams show the connection between sets; tree diagrams are useful for decision analysis; and bar charts show relative size.

Question 52

Which of the following function is the MOST critical when initiating the removal of system access for terminated employees?

- ☐ Human resources
- ☐ Legal
- ☐ Help desk
- ☒ Information security

Question 53

Which of the following is the BEST way to ensure that a corporate network is adequately secured against external attack?

- ☐ Utilize an intrusion detection system.
- ☐ Establish minimum security baselines.
- ☐ Implement vendor recommended settings.
- ☒ Perform periodic penetration testing.

Explanation:

Explanation:

Penetration testing is the best way to assure that perimeter security is adequate. An intrusion detection system (IDS) may detect an attempted attack, hut it will not confirm whether the perimeter is secured. Minimum security baselines and applying vendor recommended settings are beneficial, but they will not provide the level of assurance that is provided by penetration testing.

Licensed to Berend Post berend.post@it-university.nl

Question 54

An organization has to comply with recently published industry regulatory requirements — compliance that potentially has high implementation costs. What should the information security manager do FIRST?

- ☐ Implement a security committee.
- ☒ Perform a gap analysis.
- ☐ Implement compensating controls.
- ☐ Demand immediate compliance.

Explanation:

Explanation:

Since they are regulatory requirements, a gap analysis would be the first step to determine the level of compliance already in place. Implementing a security committee or compensating controls would not be the first step. Demanding immediate compliance would not assess the situation.

Question 55

An information security manager has been asked to create a strategy to protect the organization's information from a variety of threat vectors. Which of the following should be done FIRST?

- ☐ Perform a threat modeling exercise
- ☒ Develop a risk profile
- ☐ Design risk management processes
- ☐ Select a governance framework

Question 56

One way to determine control effectiveness is by determining:

- ☐ whether it is preventive, detective or compensatory.
- ☐ the capability of providing notification of failure.
- ☒ the test results of intended objectives.
- ☐ the evaluation and analysis of reliability.

Explanation:

Explanation:

Control effectiveness requires a process to verify that the control process worked as intended. Examples such as dual-control or dual-entry bookkeeping provide verification and assurance that the process operated as intended. The type of control is not relevant, and notification of failure is not determinative of control strength. Reliability is not an indication of control strength; weak controls can be highly reliable, even if they are ineffective controls.

Licensed to Berend Post berend.post@it-university.nl

Question 57

An information security manager at a global organization has to ensure that the local information security program will initially ensure compliance with the:

- ☐ corporate data privacy policy.
- ☒ data privacy policy where data are collected.
- ☐ data privacy policy of the headquarters' country.
- ☐ data privacy directive applicable globally.

Explanation:

Explanation:

As a subsidiary, the local entity will have to comply with the local law for data collected in the country. Senior management will be accountable for this legal compliance. The policy, being internal, cannot supersede the local law. Additionally, with local regulations differing from the country in which the organization is headquartered, it is improbable that a group wide policy will address all the local legal requirements. In case of data collected locally (and potentially transferred to a country with a different data privacy regulation), the local law applies, not the law applicable to the head office. The data privacy laws are country-specific.

Question 58

A business case for investment in an information security management infrastructure MUST include:

- ☐ evidence that the proposed infrastructure is certified.
- ☐ specifics on the security applications needed.
- ☐ data management methods currently in use.
- ☒ impact of noncompliance with applicable standards.

Question 59

Which of the following BEST enables an information security manager to determine the comprehensiveness of an organization’s information security strategy?

- ☒ Business impact analysis
- ☐ Organizational risk appetite
- ☐ Independent security audit
- ☐ Security risk assessment

Licensed to Berend Post berend.post@it-university.nl

Question 60

Which of the following types of information would the information security manager expect to have the LOWEST level of security protection in a large, multinational enterprise?

- ☐ Strategic business plan
- ☐ Upcoming financial results
- ☐ Customer personal information
- ☒ Previous financial results

Explanation:

Explanation:

Previous financial results are public; all of the other choices are private information and should only be accessed by authorized entities.

Question 61

Which of the following represents a PRIMARY area of interest when conducting a penetration test?

- ☐ Data mining
- ☒ Network mapping
- ☐ Intrusion Detection System (IDS)
- ☐ Customer data

Explanation:

Explanation:

Network mapping is the process of determining the topology of the network one wishes to penetrate. This is one of the first steps toward determining points of attack in a network. Data mining is associated with ad hoc reporting and. together with customer data, they are potential targets after the network is penetrated. The intrusion detection mechanism in place is not an area of focus because one of the objectives is to determine how effectively it protects the network or how easy it is to circumvent.

Question 62

The BEST metric for evaluating the effectiveness of a firewall is the:

- ☒ number of attacks blocked.
- ☐ number of packets dropped.
- ☐ average throughput rate.
- ☐ number of firewall rules.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The number of attacks blocked indicates whether a firewall is performing as intended. The number of packets dropped does not necessarily indicate the level of effectiveness. The number of firewall rules and the average throughput rate are not effective measurements.

Question 63

Which of the following events generally has the highest information security impact?

- ☐ Opening a new office
- ☒ Merging with another organization
- ☐ Relocating the data center
- ☐ Rewiring the network

Explanation:

Explanation:

Merging with or acquiring another organization causes a major impact on an information security management function because new vulnerabilities and risks are inherited. Opening a new office, moving the data center to a new site, or rewiring a network may have information security risks, but generally comply with corporate security policy and are easier to secure.

Question 64

There is a time lag between the time when a security vulnerability is first published, and the time when a patch is delivered. Which of the following should be carried out FIRST to mitigate the risk during this time period?

- ☒ Identify the vulnerable systems and apply compensating controls
- ☐ Minimize the use of vulnerable systems
- ☐ Communicate the vulnerability to system users
- ☐ Update the signatures database of the intrusion detection system (IDS)

Explanation:

Explanation:

The best protection is to identify the vulnerable systems and apply compensating controls until a patch is installed. Minimizing the use of vulnerable systems and communicating the vulnerability to system users could be compensating controls but would not be the first course of action. Choice D does not make clear the timing of when the intrusion detection system (IDS) signature list would be updated to accommodate the vulnerabilities that are not yet publicly known. Therefore, this approach should not always be considered as the first option.

Licensed to Berend Post berend.post@it-university.nl

Question 65

The impact of losing frame relay network connectivity for 18-24 hours should be calculated using the:

- ☐ hourly billing rate charged by the carrier.
- ☐ value of the data transmitted over the network.
- ☐ aggregate compensation of all affected business users.
- ☒ financial losses incurred by affected business units.

Explanation:

Explanation:

The bottom line on calculating the impact of a loss is what its cost will be to the organization. The other choices are all factors that contribute to the overall monetary impact.

Question 66

A risk analysis should:

- ☐ include a benchmark of similar companies in its scope.
- ☐ assume an equal degree of protection for all assets.
- ☒ address the potential size and likelihood of loss.
- ☐ give more weight to the likelihood vs. the size of the loss.

Explanation:

Explanation:

A risk analysis should take into account the potential size and likelihood of a loss. It could include comparisons with a group of companies of similar size. It should not assume an equal degree of protection for all assets since assets may have different risk factors. The likelihood of the loss should not receive greater emphasis than the size of the loss; a risk analysis should always address both equally.

Question 67

The MOST important function of a risk management program is to:

- ☐ quantify overall risk.
- ☒ minimize residual risk.
- ☐ eliminate inherent risk.
- ☐ maximize the sum of all annualized loss expectancies (ALEs).

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

A risk management program should minimize the amount of risk that cannot be otherwise eliminated or transferred; this is the residual risk to the organization. Quantifying overall risk is important but not as critical as the end result. Eliminating inherent risk is virtually impossible. Maximizing the sum of all ALEs is actually the opposite of what is desirable.

Question 68

Evidence from a compromised server has to be acquired for a forensic investigation. What would be the BEST source?

- ☒ A bit-level copy of all hard drive data
- ☐ The last verified backup stored offsite
- ☐ Data from volatile memory
- ☐ Backup servers

Explanation:

Explanation:

The bit-level copy image file ensures forensic quality evidence that is admissible in a court of law. Choices B and D may not provide forensic quality data for investigative work, while choice C alone may not provide enough evidence.

Question 69

Which of the following provides the linkage to ensure that procedures are correctly aligned with information security policy requirements?

- ☒ Standards
- ☐ Guidelines
- ☐ Security metrics
- ☐ IT governance

Explanation:

Explanation:

Standards are the bridge between high-level policy statements and the "how to" detailed formal of procedures. Security metrics and governance would not ensure correct alignment between policies and procedures. Similarly, guidelines are not linkage documents but rather provide suggested guidance on best practices.

Licensed to Berend Post berend.post@it-university.nl

Question 70

Change management procedures to ensure that disaster recovery/business continuity plans are kept up-to-date can be BEST achieved through which of the following?

- ☐ Reconciliation of the annual systems inventory to the disaster recovery, business continuity plans
- ☐ Periodic audits of the disaster recovery/business continuity plans
- ☐ Comprehensive walk-through testing
- ☒ Inclusion as a required step in the system life cycle process

Explanation:

Explanation:

Information security should be an integral component of the development cycle; thus, it should be included at the process level. Choices A, B and C are good mechanisms to ensure compliance, but would not be nearly as timely in ensuring that the plans are always up-to-date. Choice D is a preventive control, while choices A, B and C are detective controls.

Question 71

Which of the following BEST provides message integrity, sender identity authentication and nonrepudiation?

- ☐ Symmetric cryptography
- ☒ Public key infrastructure (PKI)
- ☐ Message hashing
- ☐ Message authentication code

Explanation:

Explanation:

Public key infrastructure (PKI) combines public key encryption with a trusted third party to publish and revoke digital certificates that contain the public key of the sender. Senders can digitally sign a message with their private key and attach their digital certificate (provided by the trusted third party). These characteristics allow senders to provide authentication, integrity validation and nonrepudiation. Symmetric cryptography provides confidentiality. Mashing can provide integrity and confidentiality. Message authentication codes provide integrity.

Licensed to Berend Post berend.post@it-university.nl

Question 72

To BEST improve the alignment of the information security objectives in an organization, the chief information security officer (CISO) should:

- ☐ revise the information security program.
- ☒ evaluate a balanced business scorecard.
- ☐ conduct regular user awareness sessions.
- ☐ perform penetration tests.

Explanation:

Explanation:

The balanced business scorecard can track the effectiveness of how an organization executes it information security strategy and determine areas of improvement. Revising the information security program may be a solution, but is not the best solution to improve alignment of the information security objectives. User awareness is just one of the areas the organization must track through the balanced business scorecard. Performing penetration tests does not affect alignment with information security objectives.

Question 73

Which of the following would be the BEST metric for the IT risk management process?

- ☐ Number of risk management action plans
- ☒ Percentage of critical assets with budgeted remedial
- ☐ Percentage of unresolved risk exposures
- ☐ Number of security incidents identified

Explanation:

Explanation:

Percentage of unresolved risk exposures and the number of security incidents identified contribute to the IT risk management process, but the percentage of critical assets with budgeted remedial is the most indicative metric. Number of risk management action plans is not useful for assessing the quality of the process.

Question 74

Information security policy enforcement is the responsibility of the:

- ☐ security steering committee.
- ☐ chief information officer (CIO).
- ☒ chief information security officer (CISO).
- ☐ chief compliance officer (CCO).

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Information security policy enforcement is the responsibility of the chief information security officer (CISO), first and foremost. The board of directors and executive management should ensure that a security policy is in line with corporate objectives. The chief information officer (CIO) and the chief compliance officer (CCO) are involved in the enforcement of the policy but are not directly responsible for it.

Question 75

An information security manager is implementing a bring your own device (BYOD) program. Which of the following would BEST ensure that users adhere to the security standards?

- ☐ Monitor user activities on the network
- ☐ Publish the standards on the intranet landing page
- ☐ Establish an acceptable use policy
- ☒ Deploy a device management solution

Question 76

Which of the following is the MOST critical activity to ensure the ongoing security of outsourced IT services?

- ☐ Provide security awareness training to the third-party provider's employees
- ☒ Conduct regular security reviews of the third-party provider
- ☐ Include security requirements in the service contract
- ☐ Request that the third-party provider comply with the organization's information security policy

Explanation:

Explanation:

Regular security audits and reviews of the practices of the provider to prevent potential information security damage will help verify the security of outsourced services. Depending on the type of services outsourced, security awareness may not be necessary. Security requirements should be included in the contract, but what is most important is verifying that the requirements are met by the provider. It is not necessary to require the provider to fully comply with the policy if only some of the policy is related and applicable.

Licensed to Berend Post berend.post@it-university.nl

Question 77

A message* that has been encrypted by the sender's private key and again by the receiver's public key achieves:

- ☐ authentication and authorization.
- ☐ confidentiality and integrity.
- ☒ confidentiality and nonrepudiation.
- ☐ authentication and nonrepudiation.

Explanation:

Explanation:

Encryption by the private key of the sender will guarantee authentication and nonrepudiation. Encryption by the public key of the receiver will guarantee confidentiality.

Question 78

Which of the following is MOST effective in preventing security weaknesses in operating systems?

- ☒ Patch management
- ☐ Change management
- ☐ Security baselines
- ☐ Configuration management

Explanation:

Explanation:

Patch management corrects discovered weaknesses by applying a correction (a patch) to the original program code. Change management controls the process of introducing changes to systems. Security baselines provide minimum recommended settings. Configuration management controls the updates to the production environment.

Question 79

Which of the following is the MOST important factor in an organization's selection of a key risk indicator (KRI)?

- ☐ Return on investment
- ☐ Organizational culture
- ☐ Compliance requirements
- ☒ Criticality of information

Licensed to Berend Post berend.post@it-university.nl

Question 80

Which of the following is the MOST important reason for an information security review of contracts? To help ensure that:

- ☐ the parties to the agreement can perform.
- ☐ confidential data are not included in the agreement.
- ☒ appropriate controls are included.
- ☐ the right to audit is a requirement.

Explanation:

Explanation:

Agreements with external parties can expose an organization to information security risks that must be assessed and appropriately mitigated. The ability of the parties to perform is normally the responsibility of legal and the business operation involved. Confidential information may be in the agreement by necessity and. while the information security manager can advise and provide approaches to protect the information, the responsibility rests with the business and legal. Audit rights may be one of many possible controls to include in a third-party agreement, but is not necessarily a contract requirement, depending on the nature of the agreement.

Question 81

An organization is already certified to an international security standard. Which mechanism would BEST help to further align the organization with other data security regulatory requirements as per new business needs?

- ☐ Key performance indicators (KPIs)
- ☐ Business impact analysis (BIA)
- ☒ Gap analysis
- ☐ Technical vulnerability assessment

Explanation:

Explanation:

Gap analysis would help identify the actual gaps between the desired state and the current implementation of information security management. BIA is primarily used for business continuity planning. Technical vulnerability assessment is used for detailed assessment of technical controls, which would come later in the process and would not provide complete information in order to identify gaps.

Licensed to Berend Post berend.post@it-university.nl

Question 82

Obtaining senior management support for establishing a warm site can BEST be accomplished by:

- ☐ establishing a periodic risk assessment.
- ☐ promoting regulatory requirements.
- ☒ developing a business case.
- ☐ developing effective metrics.

Explanation:

Explanation:

Business case development, including a cost-benefit analysis, will be most persuasive to management. A risk assessment may be included in the business ease, but by itself will not be as effective in gaining management support. Informing management of regulatory requirements may help gain support for initiatives, but given that more than half of all organizations are not in compliance with regulations, it is unlikely to be sufficient in many cases. Good metrics which provide assurance that initiatives are meeting organizational goals will also be useful, but are insufficient in gaining management support.

Question 83

In assessing the degree to which an organization may be affected by new privacy legislation, information security management should FIRST:

- ☐ develop an operational plan for achieving compliance with the legislation.
- ☒ identify systems and processes that contain privacy components.
- ☐ restrict the collection of personal information until compliant.
- ☐ identify privacy legislation in other countries that may contain similar requirements.

Explanation:

Explanation:

Identifying the relevant systems and processes is the best first step. Developing an operational plan for achieving compliance with the legislation is incorrect because it is not the first step. Restricting the collection of personal information comes later. Identifying privacy legislation in other countries would not add much value.

Licensed to Berend Post berend.post@it-university.nl

Question 84

An organization that has outsourced its incident management capabilities just discovered a significant privacy breach by an unknown attacker. Which of the following is the MOST important action of the information security manager?

- ☐ Follow the outsourcer's response plan.
- ☐ Alert the appropriate law enforcement authorities.
- ☐ Refer to the organization's response plan.
- ☒ Notify the outsourcer of the privacy breach.

Question 85

An information security manager is reviewing the impact of a regulation on the organization's human resources system. The NEXT course of action should be to:

- ☒ perform a gap analysis of compliance requirements.
- ☐ assess the penalties for non-compliance.
- ☐ review the organization's most recent audit report.
- ☐ determine the cost of compliance.

Question 86

Which of the following would be the FIRST step in establishing an information security program?

- ☐ Develop the security policy.
- ☐ Develop security operating procedures.
- ☒ Develop the security plan.
- ☐ Conduct a security controls study.

Explanation:

Explanation:

A security plan must be developed to implement the security strategy. All of the other choices should follow the development of the security plan.

Question 87

Before conducting a formal risk assessment of an organization's information resources, an information security manager should FIRST:

- ☒ map the major threats to business objectives.
- ☐ review available sources of risk information.
- ☐ identify the value of the critical assets.
- ☐ determine the financial impact if threats materialize.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Risk mapping or a macro assessment of the major threats to the organization is a simple first step before performing a risk assessment. Compiling all available sources of risk information is part of the risk assessment. Choices C and D are also components of the risk assessment process, which are performed subsequent to the threats-business mapping.

Question 88

What is the BEST method to confirm that all firewall rules and router configuration settings are adequate?

- ☐ Periodic review of network configuration
- ☐ Review intrusion detection system (IDS) logs for evidence of attacks
- ☒ Periodically perform penetration tests
- ☐ Daily review of server logs for evidence of hacker activity

Explanation:

Explanation:

Due to the complexity of firewall rules and router tables, plus the sheer size of intrusion detection systems (IDSs) and server logs, a physical review will be insufficient. The best approach for confirming the adequacy of these configuration settings is to periodically perform attack and penetration tests.

Question 89

A possible breach of an organization's IT system is reported by the project manager. What is the FIRST thing the incident response manager should do?

- ☐ Run a port scan on the system
- ☐ Disable the logon ID
- ☐ Investigate the system logs
- ☒ Validate the incident

Explanation:

Explanation:

When investigating a possible incident, it should first be validated. Running a port scan on the system, disabling the logon IDs and investigating the system logs may be required based on preliminary forensic investigation, but doing so as a first step may destroy the evidence.

Licensed to Berend Post berend.post@it-university.nl

Question 90

Which resource is the MOST effective in preventing physical access tailgating/piggybacking?

- ☐ Card key door locks
- ☐ Photo identification
- ☒ Awareness training
- ☐ Biometric scanners

Explanation:

Explanation:

Awareness training would most likely result in any attempted tailgating being challenged by the authorized employee. Choices A, B and D are physical controls that, by themselves, would not be effective against tailgating.

Question 91

When building a corporate-wide business continuity plan, it is discovered there are two separate lines of business systems that could be impacted by the same threat. Which of the following is the BEST method to determine the priority of system recovery in the event of a disaster?

- ☐ Evaluating the cost associated with each system's outage
- ☐ Reviewing the business plans of each department
- ☐ Comparing the recovery point objectives
- ☒ Reviewing each system's key performance indicators

Question 92

Which of the following tools is MOST appropriate to assess whether information security governance objectives are being met?

- ☐ SWOT analysis
- ☐ Waterfall chart
- ☐ Gap analysis
- ☒ Balanced scorecard

Explanation:

Explanation:

The balanced scorecard is most effective for evaluating the degree to which information security objectives are being met. A SWOT analysis addresses strengths, weaknesses, opportunities and threats. Although useful, a SWOT analysis is not as effective a tool. Similarly, a gap analysis, while useful for identifying the difference between the current state and the desired future state, is not the most appropriate tool. A waterfall chart is used to understand the flow of one process into another.

Licensed to Berend Post berend.post@it-university.nl

Question 93

An outcome of effective security governance is:

- ☐ business dependency assessment
- ☒ strategic alignment.
- ☐ risk assessment.
- ☐ planning.

Explanation:

Explanation:

Business dependency assessment is a process of determining the dependency of a business on certain information resources. It is not an outcome or a product of effective security management. Strategic alignment is an outcome of effective security governance. Where there is good governance, there is likely to be strategic alignment. Risk assessment is not an outcome of effective security governance; it is a process. Planning comes at the beginning of effective security governance, and is not an outcome but a process.

Question 94

Which of the following is the BEST mechanism to determine the effectiveness of the incident response process?

- ☐ Incident response metrics
- ☐ Periodic auditing of the incident response process
- ☐ Action recording and review
- ☒ Post incident review

Explanation:

Explanation:

Post event reviews are designed to identify gaps and shortcomings in the actual incident response process so that these gaps may be improved over time. The other choices will not provide the same level of feedback in improving the process.

Question 95

Attackers who exploit cross-site scripting vulnerabilities take advantage of:

- ☒ a lack of proper input validation controls.
- ☐ weak authentication controls in the web application layer.
- ☐ flawed cryptographic secure sockets layer (SSL) implementations and short key lengths.
- ☐ implicit web application trust relationships.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Cross-site scripting attacks inject malformed input. Attackers who exploit weak application authentication controls can gain unauthorized access to applications and this has little to do with cross-site scripting vulnerabilities. Attackers who exploit flawed cryptographic secure sockets layer (SSI.) implementations and short key lengths can sniff network traffic and crack keys to gain unauthorized access to information. This has little to do with cross-site scripting vulnerabilities. Web application trust relationships do not relate directly to the attack.

Question 96

A CIO has asked the organization's information security manager to provide both one-year and five-year plans for the information security program. What is the PRIMARY purpose for the long-term plan?

- ☐ To create formal requirements to meet projected security needs for the future
- ☐ To create and document a consistent progression of security capabilities
- ☐ To prioritize risks on a longer scale than the one-year plan
- ☒ To facilitate the continuous improvement of the IT organization

Question 97

The PRIMARY reason for using metrics to evaluate information security is to:

- ☐ identify security weaknesses.
- ☐ justify budgetary expenditures.
- ☒ enable steady improvement.
- ☐ raise awareness on security issues.

Explanation:

Explanation:

The purpose of a metric is to facilitate and track continuous improvement. It will not permit the identification of all security weaknesses. It will raise awareness and help in justifying certain expenditures, but this is not its main purpose.

Licensed to Berend Post berend.post@it-university.nl

Question 98

Which of the following steps should be performed FIRST in the risk assessment process?

- ☐ Staff interviews
- ☐ Threat identification
- ☒ Asset identification and valuation
- ☐ Determination of the likelihood of identified risks

Explanation:

Explanation:

The first step in the risk assessment methodology is a system characterization, or identification and valuation, of all of the enterprise's assets to define the boundaries of the assessment. Interviewing is a valuable tool to determine qualitative information about an organization's objectives and tolerance for risk. Interviews are used in subsequent steps. Identification of threats comes later in the process and should not be performed prior to an inventory since many possible threats will not be applicable if there is no asset at risk. Determination of likelihood comes later in the risk assessment process.

Question 99

A security manager is preparing a report to obtain the commitment of executive management to a security program. Inclusion of which of the following would be of MOST value?

- ☐ Examples of genuine incidents at similar organizations
- ☐ Statement of generally accepted best practices
- ☒ Associating realistic threats to corporate objectives
- ☐ Analysis of current technological exposures

Explanation:

Explanation:

Linking realistic threats to key business objectives will direct executive attention to them. All other options are supportive but not of as great a value as choice C when trying to obtain the funds for a new program.

Question 100

Which of the following would be the BEST indicator that an organization is appropriately managing risk?

- ☐ The number of security incident events reported by staff has increased
- ☒ Risk assessment results are within tolerance
- ☐ A penetration test does not identify any high-risk system vulnerabilities
- ☐ The number of events reported from the intrusion detection system has declined

Licensed to Berend Post berend.post@it-university.nl

Question 101

A multinational organization operating in fifteen countries is considering implementing an information security program. Which factor will MOST influence the design of the Information security program?

- ☐ Representation by regional business leaders
- ☐ Composition of the board
- ☒ Cultures of the different countries
- ☐ IT security skills

Explanation:

Explanation:

Culture has a significant impact on how information security will be implemented. Representation by regional business leaders may not have a major influence unless it concerns cultural issues. Composition of the board may not have a significant impact compared to cultural issues. IT security skills are not as key or high impact in designing a multinational information security program as would be cultural issues.

Question 102

When application-level security controlled by business process owners is found to be poorly managed, which of the following could BEST improve current practices?

- ☒ Centralizing security management
- ☐ Implementing sanctions for noncompliance
- ☐ Policy enforcement by IT management
- ☐ Periodic compliance reviews

Explanation:

Explanation:

By centralizing security management, the organization can ensure that security standards are applied to all systems equally and in line with established policy. Sanctions for noncompliance would not be the best way to correct poor management practices caused by work overloads or insufficient knowledge of security practices. Enforcement of policies is not solely the responsibility of IT management. Periodic compliance reviews would not correct the problems, by themselves, although reports to management would trigger corrective action such as centralizing security management.

Licensed to Berend Post berend.post@it-university.nl

Question 103

Which of the following is MOST effective in preventing the introduction of a code modification that may reduce the security of a critical business application?

- ☐ Patch management
- ☒ Change management
- ☐ Security metrics
- ☐ Version control

Explanation:

Explanation:

Change management controls the process of introducing changes to systems. Failure to have good change management may introduce new weaknesses into otherwise secure systems. Patch management corrects discovered weaknesses by applying a correction to the original program code. Security metrics provide a means for measuring effectiveness. Version control is a subset of change management.

Question 104

Which of the following is MOST important to consider when developing a business case to support the investment in an information security program?

- ☐ Senior management support
- ☐ Results of a cost-benefit analysis
- ☐ Results of a risk assessment
- ☒ Impact on the risk profile

Explanation:

Explanation

The information security manager must understand the business risk profile of the organization. No model provides a complete picture, but logically categorizing the risk areas of an organization facilitates focusing on key risk management strategies and decisions. It also enables the organization to develop and implement risk treatment approaches that are relevant to the business and cost effective.

Licensed to Berend Post berend.post@it-university.nl

Question 105

When a new key business application goes into production, the PRIMARY reason to update relevant business impact analysis (BIA) and business continuity/disaster recovery plans is because:

- ☐ this is a requirement of the security policy.
- ☐ software licenses may expire in the future without warning.
- ☐ the asset inventory must be maintained.
- ☒ service level agreements may not otherwise be met.

Explanation:

Explanation:

The key requirement is to preserve availability of business operations. Choice A is a correct compliance requirement, but is not the main objective in this case. Choices B and C are supplementary requirements for business continuity/disaster recovery planning.

Question 106

What will have the HIGHEST impact on standard information security governance models?

- ☐ Number of employees
- ☐ Distance between physical locations
- ☒ Complexity of organizational structure
- ☐ Organizational budget

Explanation:

Explanation:

Information security governance models are highly dependent on the overall organizational structure. Some of the elements that impact organizational structure are multiple missions and functions across the organization, leadership and lines of communication. Number of employees and distance between physical locations have less impact on information security governance models since well-defined process, technology and people components intermingle to provide the proper governance. Organizational budget is not a major impact once good governance models are in place; hence governance will help in effective management of the organization's budget.

Question 107

Which of the following is the PRIMARY advantage of desk checking a business continuity plan (BCP)?

- ☐ Assesses the availability and compatibility a backup hardware
- ☐ Allows for greater participation be management and the IT department
- ☒ Ensures that appropriate follow-up work is performed on noted issues
- ☐ Provides a low-cost method of assessing the BCP's completeness

Licensed to Berend Post berend.post@it-university.nl

Question 108

A major trading partner with access to the internal network is unwilling or unable to remediate serious information security exposures within its environment. Which of the following is the BEST recommendation?

- ☐ Sign a legal agreement assigning them all liability for any breach
- ☐ Remove all trading partner access until the situation improves
- ☒ Set up firewall rules restricting network traffic from that location
- ☐ Send periodic reminders advising them of their noncompliance

Explanation:

Explanation:

It is incumbent on an information security manager to see to the protection of their organization's network, but to do so in a manner that does not adversely affect the conduct of business. This can be accomplished by adding specific traffic restrictions for that particular location. Removing all access will likely result in lost business. Agreements and reminders do not protect the integrity of the network.

Question 109

During the restoration of several servers, a critical process that services external customers was restored late due to a failure, resulting in lost revenue. Which of the following would have BEST help to prevent this occurrence?

- ☐ Validation of senior management's risk tolerance
- ☐ Updates to the business impact analysis (BIA)
- ☐ More effective disaster recovery plan (DRP) testing
- ☒ Improvements to incident identification methods

Question 110

In order to highlight to management, the importance of network security, the security manager should FIRST:

- ☐ develop a security architecture.
- ☐ install a network intrusion detection system (NIDS) and prepare a list of attacks.
- ☐ develop a network security policy.
- ☒ conduct a risk assessment.

Explanation:

Explanation:

A risk assessment would be most helpful to management in understanding at a very high level the threats, probabilities and existing controls. Developing a security architecture, installing a network

Licensed to Berend Post berend.post@it-university.nl

intrusion detection system (NIDS) and preparing a list of attacks on the network and developing a network security policy would not be as effective in highlighting the importance to management and would follow only after performing a risk assessment.

Question 111

Which of the following is MOST effective for securing wireless networks as a point of entry into a corporate network?

- ☐ Boundary router
- ☒ Strong encryption
- ☐ Internet-facing firewall
- ☐ Intrusion detection system (IDS)

Explanation:

Explanation:

Strong encryption is the most effective means of protecting wireless networks. Boundary routers, intrusion detection systems (IDSs) and firewalling the Internet would not be as effective.

Question 112

The MOST important factor in ensuring the success of an information security program is effective:

- ☐ communication of information security requirements to all users in the organization.
- ☐ formulation of policies and procedures for information security.
- ☒ alignment with organizational goals and objectives.
- ☐ monitoring compliance with information security policies and procedures.

Explanation:

Explanation:

The success of security programs is dependent upon alignment with organizational goals and objectives. Communication is a secondary step. Effective communication and education of users is a critical determinant of success but alignment with organizational goals and objectives is the most important factor for success. Mere formulation of policies without effective communication to users will not ensure success. Monitoring compliance with information security policies and procedures can be, at best, a detective mechanism that will not lead to success in the midst of uninformed users.

Licensed to Berend Post berend.post@it-university.nl

Question 113

What is the PRIMARY role of the information security manager in the process of information classification within an organization?

- ☒ Defining and ratifying the classification structure of information assets
- ☐ Deciding the classification levels applied to the organization's information assets
- ☐ Securing information assets in accordance with their classification
- ☐ Checking if information assets have been classified properly

Explanation:

Explanation:

Defining and ratifying the classification structure of information assets is the primary role of the information security manager in the process of information classification within the organization. Choice B is incorrect because the final responsibility for deciding the classification levels rests with the data owners. Choice C is incorrect because the job of securing information assets is the responsibility of the data custodians. Choice D may be a role of an information security manager but is not the key role in this context.

Question 114

Which of the following architectures for e-business BEST ensures high availability?

- ☐ Availability of an adjacent hot site and a standby server with mirrored copies of critical data
- ☐ Intelligent middleware to direct transactions from a downed system to an alternative
- ☐ A single point of entry allowing transactions to be received and processed quickly
- ☒ Automatic failover to the web site of another e-business that meets the user's needs

Question 115

The PRIMARY objective of security awareness is to:

- ☐ ensure that security policies are understood.
- ☒ influence employee behavior.
- ☐ ensure legal and regulatory compliance
- ☐ notify of actions for noncompliance.

Explanation:

Explanation:

It is most important that security-conscious behavior be encouraged among employees through training that influences expected responses to security incidents. Ensuring that policies are read and understood, giving employees fair warning of potential disciplinary action, or meeting legal and regulatory requirements is important but secondary.

Licensed to Berend Post berend.post@it-university.nl

Question 116

The criticality and sensitivity of information assets is determined on the basis of:

- ☐ threat assessment.
- ☐ vulnerability assessment.
- ☐ resource dependency assessment.
- ☒ impact assessment.

Explanation:

Explanation:

The criticality and sensitivity of information assets depends on the impact of the probability of the threats exploiting vulnerabilities in the asset, and takes into consideration the value of the assets and the impairment of the value. Threat assessment lists only the threats that the information asset is exposed to. It does not consider the value of the asset and impact of the threat on the value. Vulnerability assessment lists only the vulnerabilities inherent in the information asset that can attract threats. It does not consider the value of the asset and the impact of perceived threats on the value. Resource dependency assessment provides process needs but not impact.

Question 117

Which of the following would BEST ensure that security risk assessment is integrated into the life cycle of major IT projects?

- ☐ Integrating the risk assessment into the internal audit program
- ☒ Applying global security standards to the IT projects
- ☐ Training project managers on risk assessment
- ☐ Having the information security manager participate on the project setting committees

Question 118

It is important to classify and determine relative sensitivity of assets to ensure that:

- ☐ cost of protection is in proportion to sensitivity.
- ☐ highly sensitive assets are protected.
- ☐ cost of controls is minimized.
- ☒ countermeasures are proportional to risk.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Classification of assets needs to be undertaken to determine sensitivity of assets in terms of risk to the business operation so that proportional countermeasures can be effectively implemented. While higher costs are allowable to protect sensitive assets, and it is always reasonable to minimize the costs of controls, it is most important that the controls and countermeasures are commensurate to the risk since this will justify the costs. Choice B is important but it is an incomplete answer because it does not factor in risk. Therefore, choice D is the most important.

Question 119

After a risk assessment study, a bank with global operations decided to continue doing business in certain regions of the world where identity theft is rampant. The information security manager should encourage the business to:

- ☐ increase its customer awareness efforts in those regions.
- ☒ implement monitoring techniques to detect and react to potential fraud.
- ☐ outsource credit card processing to a third party.
- ☐ make the customer liable for losses if they fail to follow the bank's advice.

Explanation:

Explanation:

While customer awareness will help mitigate the risks, this is insufficient on its own to control fraud risk. Implementing monitoring techniques which will detect and deal with potential fraud cases is the most effective way to deal with this risk. If the bank outsources its processing, the bank still retains liability. While making the customer liable for losses is a possible approach, nevertheless, the bank needs to be seen to be proactive in managing its risks.

Question 120

What is an appropriate frequency for updating operating system (OS) patches on production servers?

- ☐ During scheduled rollouts of new applications
- ☐ According to a fixed security patch management schedule
- ☐ Concurrently with quarterly hardware maintenance
- ☒ Whenever important security patches are released

Explanation:

Explanation:

Patches should be applied whenever important security updates are released. They should not be delayed to coincide with other scheduled rollouts or maintenance. Due to the possibility of creating a system outage, they should not be deployed during critical periods of application activity such as month-end or quarter-end closing.

Licensed to Berend Post berend.post@it-university.nl

Question 121

The PRIMARY goal of a corporate risk management program is to ensure that an organization's:

- ☐ IT assets in key business functions are protected.
- ☐ business risks are addressed by preventive controls.
- ☒ stated objectives are achievable.
- ☐ IT facilities and systems are always available.

Explanation:

Explanation:

Risk management's primary goal is to ensure an organization maintains the ability to achieve its objectives. Protecting IT assets is one possible goal as well as ensuring infrastructure and systems availability. However, these should be put in the perspective of achieving an organization's objectives. Preventive controls are not always possible or necessary; risk management will address issues with an appropriate mix of preventive and corrective controls.

Question 122

Which of the following is the MOST important element of an information security strategy?

- ☒ Defined objectives
- ☐ Time frames for delivery
- ☐ Adoption of a control framework
- ☐ Complete policies

Explanation:

Explanation:

Without defined objectives, a strategy — the plan to achieve objectives — cannot be developed. Time frames for delivery are important but not critical for inclusion in the strategy document. Similarly, the adoption of a control framework is not critical to having a successful information security strategy. Policies are developed subsequent to, and as a part of, implementing a strategy.

Question 123

When designing the technical solution for a disaster recovery site, the PRIMARY factor that should be taken into consideration is the:

- ☐ services delivery objective.
- ☐ recovery time objective (RTO).
- ☒ recovery window.
- ☐ maximum tolerable outage (MTO).

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

The length of the recovery window is defined by business management and determines the acceptable time frame between a disaster and the restoration of critical services/applications. The technical implementation of the disaster recovery (DR) site will be based on this constraint, especially the choice between a hot, warm or cold site. The service delivery objective is supported during the alternate process mode until the normal situation is restored, which is directly related to business needs. The recovery time objective (RTO) is commonly agreed to be the time frame between a disaster and the return to normal operations. It is then longer than the interruption window and is very difficult to estimate in advance. The time frame between the reduced operation mode at the end of the interruption window and the return to normal operations depends on the magnitude of the disaster. Technical disaster recovery solutions alone will not be used for returning to normal operations. Maximum tolerable outage (MTO) is the maximum time acceptable by a company operating in reduced mode before experiencing losses. Theoretically, recovery time objectives (RTOs) equal the interruption window plus the maximum tolerable outage. This will not be the primary factor for the choice of the technical disaster recovery solution.

Question 124

An information security organization should PRIMARILY:

☒ support the business objectives of the company by providing security-related support services.

☐ be responsible for setting up and documenting the information security responsibilities of the information security team members.

☐ ensure that the information security policies of the company are in line with global best practices and standards.

☐ ensure that the information security expectations are conveyed to employees.

Explanation:

Explanation:

The information security organization is responsible for options B and D within an organization, but they are not its primary mission. Reviewing and adopting appropriate standards (option C) is a requirement. The primary objective of an information security organization is to ensure that security supports the overall business objectives of the company.

Licensed to Berend Post berend.post@it-university.nl

Question 125

Who should drive the risk analysis for an organization?

- ☐ Senior management
- ☒ Security manager
- ☐ Quality manager
- ☐ Legal department

Explanation:

Explanation:

Although senior management should support and sponsor a risk analysis, the know-how and the management of the project will be with the security department. Quality management and the legal department will contribute to the project.

Question 126

Which of the following would be the MOST significant security risk in a pharmaceutical institution?

- ☐ Compromised customer information
- ☐ Unavailability of online transactions
- ☐ Theft of security tokens
- ☒ Theft of a Research and Development laptop

Explanation:

Explanation:

The research and development department is usually the most sensitive area of the pharmaceutical organization, Theft of a laptop from this area could result in the disclosure of sensitive formulas and other intellectual property which could represent the greatest security breach. A pharmaceutical organization does not normally have direct contact with end customers and their transactions are not time critical: therefore, compromised customer information and unavailability of online transactions are not the most significant security risks. Theft of security tokens would not be as significant since a pin would still be required for their use.

Question 127

When security policies are strictly enforced, the initial impact is that:

- ☐ they may have to be modified more frequently.
- ☐ they will be less subject to challenge.
- ☒ the total cost of security is increased.
- ☐ the need for compliance reviews is decreased.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

When security policies are strictly enforced, more resources are initially required, thereby increasing, the total cost of security. There would be less need for frequent modification. Challenges would be rare and the need for compliance reviews would not necessarily be less.

Question 128

A digital signature using a public key infrastructure (PKI) will:

- ☐ not ensure the integrity of a message.
- ☒ rely on the extent to which the certificate authority (CA) is trusted.
- ☐ require two parties to the message exchange.
- ☐ provide a high level of confidentiality.

Explanation:

Explanation:

The certificate authority (CA) is a trusted third party that attests to the identity of the signatory, and reliance will be a function of the level of trust afforded the CA. A digital signature would provide a level of assurance of message integrity, but it is a three-party exchange, including the CA. Digital signatures do not require encryption of the message in order to preserve confidentiality.

Question 129

Which if the following would be the MOST important information to include in a business case for an information security project in a highly regulated industry?

- ☒ Compliance risk assessment
- ☐ Critical audit findings
- ☐ Industry comparison analysis
- ☐ Number of reported security incidents

Question 130

Which of the following would MOST likely require a business continuity plan to be invoked?

- ☐ An unauthorized visitor discovered in the data center
- ☒ A distributed denial of service attack on an e-mail server
- ☐ An epidemic preventing staff from performing job functions
- ☐ A hacker holding personally identifiable information hostage

Licensed to Berend Post berend.post@it-university.nl

Question 131

To ensure that payroll systems continue on in an event of a hurricane hitting a data center, what would be the FIRS T crucial step an information security manager would take in ensuring business continuity planning?

- ☐ Conducting a qualitative and quantitative risk analysis.
- ☐ Assigning value to the assets.
- ☐ Weighing the cost of implementing the plan vs. financial loss.
- ☒ Conducting a business impact analysis (BIA).

Explanation:

Explanation:

BIA is an essential component of an organization's business continuity plan; it includes an exploratory component to reveal any vulnerabilities and a planning component to develop strategies for minimizing risk. It is the first crucial step in business continuity planning. Qualitative and quantitative risk analysis will have been completed to define the dangers to individuals, businesses and government agencies posed by potential natural and human-caused adverse events. Assigning value to assets is part of the BIA process. Weighing the cost of implementing the plan vs. financial loss is another part of the BIA.

Question 132

A global organization processes and stores large volumes of personal data. Which of the following would be the MOST important attribute in creating a data access policy?

- ☐ Availability
- ☐ Integrity
- ☐ Reliability
- ☒ Confidentiality

Question 133

Which of the following features is normally missing when using Secure Sockets Layer (SSL) in a web browser?

- ☒ Certificate-based authentication of web client
- ☐ Certificate-based authentication of web server
- ☐ Data confidentiality between client and web server
- ☐ Multiple encryption algorithms

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Web browsers have the capability of authenticating through client-based certificates; nevertheless, it is not commonly used. When using https, servers always authenticate with a certificate and, once the connection is established, confidentiality will be maintained between client and server. By default, web browsers and servers support multiple encryption algorithms and negotiate the best option upon connection.

Question 134

The MAIN reason for continuous monitoring of a security strategy is to:

- ☐ optimize resource allocation.
- ☐ confirm benefits are being realized.
- ☒ evaluate the implementation of the strategy.
- ☐ allocate funds for information security

Question 135

An organization faces severe fines and penalties if not in compliance with local regulatory requirements by an established deadline. Senior management has asked the information security manager to prepare an action plan to achieve compliance. Which of the following would provide the MOST useful information for planning purposes?

- ☐ Results from a gap analysis
- ☐ Results from a business impact analysis
- ☐ Deadlines and penalties for noncompliance
- ☒ An inventory of security controls currently in place

Question 136

The PRIMARY advantage of single sign-on (SSO) is that it will:

- ☐ support multiple authentication mechanisms.
- ☐ increase the security related applications.
- ☐ strengthen user password.
- ☒ increase efficiency of access management.

Question 137

Risk management programs are designed to reduce risk to:

- ☐ a level that is too small to be measurable.
- ☐ the point at which the benefit exceeds the expense.
- ☒ a level that the organization is willing to accept.
- ☐ a rate of return that equals the current cost of capital.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Risk should be reduced to a level that an organization is willing to accept. Reducing risk to a level too small to measure is impractical and is often cost-prohibitive. To tie risk to a specific rate of return ignores the qualitative aspects of risk that must also be considered. Depending on the risk preference of an organization, it may or may not choose to pursue risk mitigation to the point at which the benefit equals or exceeds the expense. Therefore, choice C is a more precise answer.

Question 138

To ensure that all information security procedures are functional and accurate, they should be designed with the involvement of:

- ☐ end users.
- ☐ legal counsel.
- ☒ operational units.
- ☐ audit management.

Explanation:

Explanation:

Procedures at the operational level must be developed by or with the involvement of operational units that will use them. This will ensure that they are functional and accurate. End users and legal counsel are normally not involved in procedure development. Audit management generally oversees information security operations but does not get involved at the procedural level.

Question 139

Priority should be given to which of the following to ensure effective implementation of information security governance?

- ☐ Consultation
- ☐ Negotiation
- ☐ Facilitation
- ☒ Planning

Explanation:

Explanation:

Planning is the key to effective implementation of information security governance. Consultation, negotiation and facilitation come after planning.

Licensed to Berend Post berend.post@it-university.nl

Question 140

Logging is an example of which type of defense against systems compromise?

- ☐ Containment
- ☒ Detection
- ☐ Reaction
- ☐ Recovery

Explanation:

Explanation:

Detection defenses include logging as well as monitoring, measuring, auditing, detecting viruses and intrusion. Examples of containment defenses are awareness, training and physical security defenses. Examples of reaction defenses are incident response, policy and procedure change, and control enhancement. Examples of recovery defenses are backups and restorations, failover and remote sites, and business continuity plans and disaster recovery plans.

Question 141

Which of the following presents the GREATEST exposure to internal attack on a network?

- ☐ User passwords are not automatically expired
- ☐ All network traffic goes through a single switch
- ☒ User passwords are encoded but not encrypted
- ☐ All users reside on a single internal subnet

Explanation:

Explanation:

When passwords are sent over the internal network in an encoded format, they can easily be converted to clear text. All passwords should be encrypted to provide adequate security. Not automatically expiring user passwords does create an exposure, but not as great as having unencrypted passwords. Using a single switch or subnet does not present a significant exposure.

Question 142

Which of the following would present the GREATEST risk to information security?

- ☐ Virus signature files updates are applied to all servers every day
- ☐ Security access logs are reviewed within five business days
- ☐ Critical patches are applied within 24 hours of their release
- ☒ Security incidents are investigated within five business days

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Security incidents are configured to capture system events that are important from the security perspective; they include incidents also captured in the security access logs and other monitoring tools. Although, in some instances, they could wait for a few days before they are researched, from the options given this would have the greatest risk to security. Most often, they should be analyzed as soon as possible. Virus signatures should be updated as often as they become available by the vendor, while critical patches should be installed as soon as they are reviewed and tested, which could occur in 24 hours.

Question 143

Which of the following is the MOST effective solution for preventing individuals external to the organization from modifying sensitive information on a corporate database?

- ☒ Screened subnets
- ☐ Information classification policies and procedures
- ☐ Role-based access controls
- ☐ Intrusion detection system (IDS)

Explanation:

Explanation:

Screened subnets are demilitarized zones (DMZs) and are oriented toward preventing attacks on an internal network by external users. The policies and procedures to classify information will ultimately result in better protection but they will not prevent actual modification. Role-based access controls would help ensure that users only had access to files and systems appropriate for their job role. Intrusion detection systems (IDS) are useful to detect invalid attempts but they will not prevent attempts.

Question 144

An organization that outsourced its payroll processing performed an independent assessment of the security controls of the third party, per policy requirements. Which of the following is the MOST useful requirement to include in the contract?

- ☒ Right to audit
- ☐ Nondisclosure agreement
- ☐ Proper firewall implementation
- ☐ Dedicated security manager for monitoring compliance

Explanation:

Explanation:

Right to audit would be the most useful requirement since this would provide the company the ability to perform a security audit/assessment whenever there is a business need to examine whether the controls are working effectively at the third party. Options B, C and D are important

Licensed to Berend Post berend.post@it-university.nl

requirements and can be examined during the audit. A dedicated security manager would be a costly solution and not always feasible for most situations.

Question 145

During the security review of organizational servers, it was found that a file server containing confidential human resources (HR) data was accessible to all user IDs. As a FIRST step, the security manager should:

- ☐ copy sample files as evidence.
- ☐ remove access privileges to the folder containing the data.
- ☒ report this situation to the data owner.
- ☐ train the HR team on properly controlling file permissions.

Explanation:

Explanation:

The data owner should be notified prior to any action being taken. Copying sample files as evidence is not advisable since it breaches confidentiality requirements on the file. Removing access privileges to the folder containing the data should be done by the data owner or by the security manager in consultation with the data owner, however, this would be done only after formally reporting the incident. Training the human resources (MR) team on properly controlling file permissions is the method to prevent such incidents in the future, but should take place once the incident reporting and investigation activities are completed.

Question 146

Which of the following is the MOST important risk associated with middleware in a client-server environment?

- ☐ Server patching may be prevented
- ☐ System backups may be incomplete
- ☒ System integrity may be affected
- ☐ End-user sessions may be hijacked

Explanation:

Explanation:

The major risk associated with middleware in a client-server environment is that system integrity may be adversely affected because of the very purpose of middleware, which is intended to support multiple operating environments interacting concurrently. Lack of proper software to control portability of data or programs across multiple platforms could result in a loss of data or program integrity. All other choices are less likely to occur.

Licensed to Berend Post berend.post@it-university.nl

Question 147

Which of the following metrics would provide management with the MOST useful information about the progress of a security awareness program?

- ☐ Increased number of downloads of the organization's security policy
- ☐ Increased reported of security incidents
- ☐ Completion rate of user awareness training within each business unit
- ☒ Decreased number of security incidents

Question 148

An organization has decided to implement a security information and event management (SIEM) system. It is MOST important for the organization to consider:

- ☒ industry best practices.
- ☐ data ownership.
- ☐ log sources.
- ☐ threat assessments.

Question 149

Data owners must provide a safe and secure environment to ensure confidentiality, integrity and availability of the transaction. This is an example of an information security:

- ☐ baseline.
- ☐ strategy.
- ☐ procedure.
- ☒ policy.

Explanation:

Explanation:

A policy is a high-level statement of an organization's beliefs, goals, roles and objectives. Baselines assume a minimum security level throughout an organization. The information security strategy aligns the information security program with business objectives rather than making control statements. A procedure is a step-by-step process of how policy and standards will be implemented.

Licensed to Berend Post berend.post@it-university.nl

Question 150

Which of the following would be the MOST appropriate physical security solution for the main entrance to a data center"?

- ☐ Mantrap
- ☒ Biometric lock
- ☐ Closed-circuit television (CCTV)
- ☐ Security guard

Explanation:

Explanation:

A biometric device will ensure that only the authorized user can access the data center. A mantrap, by itself, would not be effective. Closed-circuit television (CCTV) and a security guard provide a detective control, but would not be as effective in authenticating the access rights of each individual.

Question 151

Which of the following is the BEST method to provide a new user with their initial password for e-mail system access?

- ☐ Interoffice a system-generated complex password with 30 days expiration
- ☒ Give a dummy password over the telephone set for immediate expiration
- ☐ Require no password but force the user to set their own in 10 days
- ☐ Set initial password equal to the user ID with expiration in 30 days

Explanation:

Explanation:

Documenting the password on paper is not the best method even if sent through interoffice mail if the password is complex and difficult to memorize, the user will likely keep the printed password and this creates a security concern. A dummy (temporary) password that will need to be changed upon first logon is the best method because it is reset immediately and replaced with the user's choice of password, which will make it easier for the user to remember. If it is given to the wrong person, the legitimate user will likely notify security if still unable to access the system, so the security risk is low. Setting an account with no initial password is a security concern even if it is just for a few days. Choice D provides the greatest security threat because user IDs are typically known by both users and security staff, thus compromising access for up to 30 days.

Licensed to Berend Post berend.post@it-university.nl

Question 152

In assessing risk, it is MOST essential to:

- ☐ provide equal coverage for all asset types.
- ☐ use benchmarking data from similar organizations.
- ☒ consider both monetary value and likelihood of loss.
- ☐ focus primarily on threats and recent business losses.

Explanation:

Explanation:

A risk analysis should take into account the potential financial impact and likelihood of a loss. It should not weigh all potential losses evenly, nor should it focus primarily on recent losses or losses experienced by similar firms. Although this is important supplementary information, it does not reflect the organization's real situation. Geography and other factors come into play as well.

Question 153

To justify the need to invest in a forensic analysis tool, an information security manager should FIRST:

- ☐ review the functionalities and implementation requirements of the solution.
- ☐ review comparison reports of tool implementation in peer companies.
- ☐ provide examples of situations where such a tool would be useful.
- ☒ substantiate the investment in meeting organizational needs.

Explanation:

Explanation:

Any investment must be reviewed to determine whether it is cost effective and supports the organizational strategy. It is important to review the features and functionalities provided by such a tool, and to provide examples of situations where the tool would be useful, but that comes after substantiating the investment and return on investment to the organization.

Question 154

When a user employs a client-side digital certificate to authenticate to a web server through Secure Socket Layer (SSL), confidentiality is MOST vulnerable to which of the following?

- ☐ IP spoofing
- ☐ Man-in-the-middle attack
- ☐ Repudiation
- ☒ Trojan

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

A Trojan is a program that gives the attacker full control over the infected computer, thus allowing the attacker to hijack, copy or alter information after authentication by the user. IP spoofing will not work because IP is not used as an authentication mechanism. Man-in-the-middle attacks are not possible if using SSL with client-side certificates. Repudiation is unlikely because client-side certificates authenticate the user.

Question 155

Which of the following should be of MOST concern to an information security manager reviewing an organization's data classification program?

- ☐ The program allows exceptions to be granted.
- ☒ Labeling is not consistent throughout the organization.
- ☐ Data retention requirement are not defined.
- ☐ The classifications do not follow industry best practices.

Question 156

Which of the following technologies is utilized to ensure that an individual connecting to a corporate internal network over the Internet is not an intruder masquerading as an authorized user?

- ☐ Intrusion detection system (IDS)
- ☐ IP address packet filtering
- ☒ Two-factor authentication
- ☐ Embedded digital signature

Explanation:

Explanation:

Two-factor authentication provides an additional security mechanism over and above that provided by passwords alone. This is frequently used by mobile users needing to establish connectivity to a corporate network. IP address packet filtering would protect against spoofing an internal address but would not provide strong authentication. An intrusion detection system (IDS) can be used to detect an external attack but would not help in authenticating a user attempting to connect. Digital signatures ensure that transmitted information can be attributed to the named sender.

Question 157

The PRIMARY benefit of performing an information asset classification is to:

- ☐ link security requirements to business objectives.
- ☒ identify controls commensurate to risk.
- ☐ define access rights.
- ☐ establish ownership.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

All choices are benefits of information classification. However, identifying controls that are proportional to the risk in all cases is the primary benefit of the process.

Question 158

Which of the following would be the BEST option to improve accountability for a system administrator who has security functions?

- ☒ Include security responsibilities in the job description
- ☐ Require the administrator to obtain security certification
- ☐ Train the system administrator on penetration testing and vulnerability assessment
- ☐ Train the system administrator on risk assessment

Explanation:

Explanation:

The first step to improve accountability is to include security responsibilities in a job description. This documents what is expected and approved by the organization. The other choices are methods to ensure that the system administrator has the training to fulfill the responsibilities included in the job description.

Question 159

Nonrepudiation can BEST be ensured by using:

- ☐ strong passwords.
- ☐ a digital hash.
- ☐ symmetric encryption.
- ☒ digital signatures.

Explanation:

Explanation:

Digital signatures use a private and public key pair, authenticating both parties. The integrity of the contents exchanged is controlled through the hashing mechanism that is signed by the private key of the exchanging party. A digital hash in itself helps in ensuring integrity of the contents, but not nonrepudiation. Symmetric encryption wouldn't help in nonrepudiation since the keys are always shared between parties. Strong passwords only ensure authentication to the system and cannot be used for nonrepudiation involving two or more parties.

Licensed to Berend Post berend.post@it-university.nl

Question 160

An organization is in the process of adopting a hybrid data infrastructure, transferring all non-core applications to cloud service providers and maintaining all core business functions house. The information security manager has determined a defense in depth strategy should be used. Which of the following BEST describes this strategy?

- ☐ Multi-factor login requirements for cloud service applications, timeouts, and complex passwords
- ☐ Deployments of nested firewalls within the infrastructure
- ☒ Separate security controls for applications, platforms, programs, and endpoints
- ☐ Strict enforcement of role-based access control (RBAC)

Question 161

Which of the following is the MOST appropriate method to protect a password that opens a confidential file?

- ☐ Delivery path tracing
- ☐ Reverse lookup translation
- ☒ Out-of-band channels
- ☐ Digital signatures

Explanation:

Explanation:

Out-of-band channels are useful when it is necessary, for confidentiality, to break a message into two parts that are then sent by different means. Digital signatures only provide nonrepudiation. Reverse lookup translation involves converting; in Internet Protocol (IP) address to a username. Delivery path tracing shows the route taken but does not confirm the identity of the sender.

Question 162

What is the PRIMARY objective of a post-event review in incident response?

- ☐ Adjust budget provisioning
- ☐ Preserve forensic data
- ☒ Improve the response process
- ☐ Ensure the incident is fully documented

Explanation:

Explanation:

The primary objective is to find any weakness in the current process and improve it. The other choices are all secondary.

Licensed to Berend Post berend.post@it-university.nl

Question 163

The PRIMARY objective of an Internet usage policy is to prevent:

- ☐ access to inappropriate sites.
- ☐ downloading malicious code.
- ☐ violation of copyright laws.
- ☒ disruption of Internet access.

Explanation:

Explanation:

Unavailability of Internet access would cause a business disruption. The other three objectives are secondary.

Question 164

Which of the following sites would be MOST appropriate in the case of a very short recovery time objective (RTO)?

- ☒ Warm
- ☐ Redundant
- ☐ Shared
- ☐ Mobile

Explanation:

Reference https://searchdisasterrecovery.techtarget.com/answer/Whats-the-difference-between-a-hot-site-and-cold-site-for-disaster-recovery

Question 165

The PRIMARY reason for initiating a policy exception process is when:

- ☐ operations are too busy to comply.
- ☒ the risk is justified by the benefit.
- ☐ policy compliance would be difficult to enforce.
- ☐ users may initially be inconvenienced.

Explanation:

Explanation:

Exceptions to policy are warranted in circumstances where compliance may be difficult or impossible and the risk of noncompliance is outweighed by the benefits. Being busy is not a justification for policy exceptions, nor is the fact that compliance cannot be enforced. User inconvenience is not a reason to automatically grant exception to a policy.

Licensed to Berend Post berend.post@it-university.nl

Question 166

Which of the following are the essential ingredients of a business impact analysis (B1A)?

- ☒ Downtime tolerance, resources and criticality
- ☐ Cost of business outages in a year as a factor of the security budget
- ☐ Business continuity testing methodology being deployed
- ☐ Structure of the crisis management team

Explanation:

Explanation:

The main purpose of a BIA is to measure the downtime tolerance, associated resources and criticality of a business function. Options B, C and D are all associated with business continuity planning, but are not related to the BIA.

Question 167

Which of the following would be MOST important to include in a bring your own device (BYOD) policy with regard to lost or stolen devices? The need for employees to:

- ☐ initiate the company's incident reporting process.
- ☐ seek advice from the mobile service provider.
- ☐ notify local law enforcement.
- ☒ request a remote wipe of the device.

Question 168

Which of the following is the MOST important consideration when implementing an intrusion detection system (IDS)?

- ☒ Tuning
- ☐ Patching
- ☐ Encryption
- ☐ Packet filtering

Explanation:

Explanation:

If an intrusion detection system (IDS) is not properly tuned it will generate an unacceptable number of false positives and/or fail to sound an alarm when an actual attack is underway. Patching is more related to operating system hardening, while encryption and packet filtering would not be as relevant.

Licensed to Berend Post berend.post@it-university.nl

Question 169

Which of the following would represent a violation of the chain of custody when a backup tape has been identified as evidence in a fraud investigation? The tape was:

- ☐ removed into the custody of law enforcement investigators.
- ☒ kept in the tape library' pending further analysis.
- ☐ sealed in a signed envelope and locked in a safe under dual control.
- ☐ handed over to authorized independent investigators.

Explanation:

Explanation:

Since a number of individuals would have access to the tape library, and could have accessed and tampered with the tape, the chain of custody could not be verified. All other choices provide clear indication of who was in custody of the tape at all times.

Question 170

When outsourcing data to a cloud service provider, which of the following should be the information security manager's MOST important consideration?

- ☐ Roles and responsibilities have been defined for the subscriber organization.
- ☐ Cloud servers are located in the same country as the organization.
- ☐ Access authorization includes biometric security verification.
- ☒ Data stored at the cloud service provider is not co-mingled.

Question 171

Which of the following would help management determine the resources needed to mitigate a risk to the organization?

- ☐ Risk analysis process
- ☒ Business impact analysis (BIA)
- ☐ Risk management balanced scorecard
- ☐ Risk-based audit program

Explanation:

Explanation:

The business impact analysis (BIA) determines the possible outcome of a risk and is essential to determine the appropriate cost of control. The risk analysis process provides comprehensive data, but does not determine definite resources to mitigate the risk as does the BIA. The risk management balanced scorecard is a measuring tool for goal attainment. A risk-based audit program is used to focus the audit process on the areas of greatest importance to the organization.

Licensed to Berend Post berend.post@it-university.nl

Question 172

It is MOST important for an information security manager to ensure that security risk assessments are performed:

- ☒ consistently throughout the enterprise
- ☐ during a root cause analysis
- ☐ as part of the security business case
- ☐ in response to the threat landscape

Explanation:

Reference https://m.isaca.org/Certification/Additional-Resources/Documents/CISM-Item-Development-Guide_bro_Eng_0117.pdf (14)

Question 173

Which of the following is the MOST important guideline when using software to scan for security exposures within a corporate network?

- ☐ Never use open source tools
- ☐ Focus only on production servers
- ☐ Follow a linear process for attacks
- ☒ Do not interrupt production processes

Explanation:

Explanation:

The first rule of scanning for security exposures is to not break anything. This includes the interruption of any running processes. Open source tools are an excellent resource for performing scans. Scans should focus on both the test and production environments since, if compromised, the test environment could be used as a platform from which to attack production servers. Finally, the process of scanning for exposures is more of a spiral process than a linear process.

Question 174

Who can BEST approve plans to implement an information security governance framework?

- ☐ Internal auditor
- ☐ Information security management
- ☒ Steering committee
- ☐ Infrastructure management

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Senior management that is part of the security steering committee is in the best position to approve plans to implement an information security governance framework. An internal auditor is secondary' to the authority and influence of senior management. Information security management should not have the authority to approve the security governance framework. Infrastructure management will not be in the best position since it focuses more on the technologies than on the business.

Question 175

Which program element should be implemented FIRST in asset classification and control?

- ☐ Risk assessment
- ☐ Classification
- ☒ Valuation
- ☐ Risk mitigation

Explanation:

Explanation:

Valuation is performed first to identify and understand the assets needing protection. Risk assessment is performed to identify and quantify threats to information assets that are selected by the first step, valuation. Classification and risk mitigation are steps following valuation.

Question 176

A critical device is delivered with a single user and password that is required to be shared for multiple users to access the device. An information security manager has been tasked with ensuring all access to the device is authorized. Which of the following would be the MOST efficient means to accomplish this?

- ☒ Enable access through a separate device that requires adequate authentication
- ☐ Implement manual procedures that require password change after each use
- ☐ Request the vendor to add multiple user IDs
- ☐ Analyze the logs to detect unauthorized access

Explanation:

Explanation:

Choice A is correct because it allows authentication tokens to be provisioned and terminated for individuals and also introduces the possibility of logging activity by individual. Choice B is not effective because users can circumvent the manual procedures. Choice C is not the best option because vendor enhancements may take time and development, and this is a critical device. Choice D could, in some cases, be an effective complementary control but. because it is detective, it would not be the most effective in this instance.

Licensed to Berend Post berend.post@it-university.nl

Question 177

Which of the following is the MOST important item to consider when evaluating products to monitor security across the enterprise?

- ☐ Ease of installation
- ☐ Product documentation
- ☐ Available support
- ☒ System overhead

Explanation:

Explanation:

Monitoring products can impose a significant impact ON system overhead for servers and networks. Product documentation, telephone support and ease of installation, while all important, would be secondary.

Question 178

Which of the following provides the MOST comprehensive understanding of an organization's information security posture?

- ☒ Risk management metrics
- ☐ External audit findings
- ☐ Results of vulnerability assessments
- ☐ The organization's security incident trends

Question 179

An organization is planning to open a new office in another country. Sensitive data will be routinely sent between two offices. What should be the information security manager's FIRST course of action?

- ☒ Identify applicable regulatory requirements to establish security policies.
- ☐ Update privacy policies to include the other country's laws and regulations.
- ☐ Apply the current corporate security policies to the new office.
- ☐ Encrypt the data for transfer to the head office based on security manager approval.

Licensed to Berend Post berend.post@it-university.nl

Question 180

Primary direction on the impact of compliance with new regulatory requirements that may lead to major application system changes should be obtained from the:

- ☐ corporate internal auditor.
- ☐ System developers/analysts.
- ☒ key business process owners.
- ☐ corporate legal counsel.

Explanation:

Explanation:

Business process owners are in the best position to understand how new regulatory requirements may affect their systems. Legal counsel and infrastructure management, as well as internal auditors, would not be in as good a position to fully understand all ramifications.

Question 181

A risk management approach to information protection is:

- ☒ managing risks to an acceptable level, commensurate with goals and objectives.
- ☐ accepting the security posture provided by commercial security products.
- ☐ implementing a training program to educate individuals on information protection and risks.
- ☐ managing risk tools to ensure that they assess all information protection vulnerabilities.

Explanation:

Explanation:

Risk management is identifying all risks within an organization, establishing an acceptable level of risk and effectively managing risks which may include mitigation or transfer. Accepting the security-posture provided by commercial security products is an approach that would be limited to technology components and may not address all business operations of the organization. Education is a part of the overall risk management process. Tools may be limited to technology and would not address non-technology risks.

Licensed to Berend Post berend.post@it-university.nl

Question 182

Which of the following would the BEST demonstrate the added value of an information security program?

- ☐ Security baselines
- ☒ A SWOT analysis
- ☐ A gap analysis
- ☐ A balanced scorecard

Question 183

Who is MOST important to include when establishing the response process for a significant security breach that would impact the IT infrastructure and cause customer data loss?

- ☐ An independent auditor for identification of control deficiencies
- ☐ A damage assessment expert for calculating losses
- ☒ A forensics expert for evidence management
- ☐ A penetration tester to validate the attack

Question 184

An information security manager uses security metrics to measure the:

- ☒ performance of the information security program.
- ☐ performance of the security baseline.
- ☐ effectiveness of the security risk analysis.
- ☐ effectiveness of the incident response team.

Explanation:

Explanation:

The security metrics should be designed so that there is a relationship to the performance of the overall security program in terms of effectiveness measurement. Use of security metrics occurs after the risk assessment process and does not measure it. Measurement of the incident response team performance is included in the overall program performance, so this is an incomplete answer.

Question 185

Access control to a sensitive intranet application by mobile users can BEST be implemented through:

- ☐ data encryption.
- ☐ digital signatures.
- ☐ strong passwords.
- ☒ two-factor authentication.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Two-factor authentication through the use of strong passwords combined with security tokens provides the highest level of security. Data encryption, digital signatures and strong passwords do not provide the same level of protection.

Question 186

Which of the following will BEST prevent external security attacks?

- ☐ Static IP addressing
- ☒ Network address translation
- ☐ Background checks for temporary employees
- ☐ Securing and analyzing system access logs

Explanation:

Explanation:

Network address translation is helpful by having internal addresses that are nonroutable. Background checks of temporary employees are more likely to prevent an attack launched from within the enterprise. Static IP addressing does little to prevent an attack. Writing all computer logs to removable media does not help in preventing an attack.

Question 187

Which of the following BEST describes the scope of risk analysis?

- ☐ Key financial systems
- ☒ Organizational activities
- ☐ Key systems and infrastructure
- ☐ Systems subject to regulatory compliance

Explanation:

Explanation:

Risk analysis should include all organizational activities. It should not be limited to subsets of systems or just systems and infrastructure.

Licensed to Berend Post berend.post@it-university.nl

Question 188

An online banking institution is concerned that the breach of customer personal information will have a significant financial impact due to the need to notify and compensate customers whose personal information may have been compromised. The institution determines that residual risk will always be too high and decides to:

- ☒ mitigate the impact by purchasing insurance.
- ☐ implement a circuit-level firewall to protect the network.
- ☐ increase the resiliency of security measures in place.
- ☐ implement a real-time intrusion detection system.

Explanation:

Explanation:

Since residual risk will always be too high, the only practical solution is to mitigate the financial impact by purchasing insurance.

Question 189

Because of its importance to the business, an organization wants to quickly implement a technical solution which deviates from the company's policies. An information security manager should:

- ☐ conduct a risk assessment and allow or disallow based on the outcome.
- ☒ recommend a risk assessment and implementation only if the residual risks are accepted.
- ☐ recommend against implementation because it violates the company's policies.
- ☐ recommend revision of current policy.

Explanation:

Explanation:

Whenever the company's policies cannot be followed, a risk assessment should be conducted to clarify the risks. It is then up to management to accept the risks or to mitigate them. Management determines the level of risk they are willing to take. Recommending revision of current policy should not be triggered by a single request.

Licensed to Berend Post berend.post@it-university.nl

Question 190

An unauthorized user gained access to a merchant's database server and customer credit card information. Which of the following would be the FIRST step to preserve and protect unauthorized intrusion activities?

- ☐ Shut down and power off the server.
- ☐ Duplicate the hard disk of the server immediately.
- ☒ Isolate the server from the network.
- ☐ Copy the database log file to a protected server.

Explanation:

Explanation:

Isolating the server will prevent further intrusions and protect evidence of intrusion activities left in memory and on the hard drive. Some intrusion activities left in virtual memory may be lost if the system is shut down. Duplicating the hard disk will only preserve the evidence on the hard disk, not the evidence in virtual memory, and will not prevent further unauthorized access attempts. Copying the database log file to a protected server will not provide sufficient evidence should the organization choose to pursue legal recourse.

Question 191

The MAIN reason why asset classification is important to a successful information security program is because classification determines:

- ☐ the priority and extent of risk mitigation efforts.
- ☐ the amount of insurance needed in case of loss.
- ☒ the appropriate level of protection to the asset.
- ☐ how protection levels compare to peer organizations.

Explanation:

Explanation:

Protection should be proportional to the value of the asset. Classification is based upon the value of the asset to the organization. The amount of insurance needed in case of loss may not be applicable in each case. Peer organizations may have different classification schemes for their assets.

Licensed to Berend Post berend.post@it-university.nl

Question 192

When personal information is transmitted across networks, there MUST be adequate controls over:

- ☐ change management.
- ☒ privacy protection.
- ☐ consent to data transfer.
- ☐ encryption devices.

Explanation:

Explanation:

Privacy protection is necessary to ensure that the receiving party has the appropriate level of protection of personal data. Change management primarily protects only the information, not the privacy of the individuals. Consent is one of the protections that is frequently, but not always, required. Encryption is a method of achieving the actual control, but controls over the devices may not ensure adequate privacy protection and. therefore, is a partial answer.

Question 193

When considering the value of assets, which of the following would give the information security manager the MOST objective basis for measurement of value delivery in information security governance?

- ☐ Number of controls
- ☒ Cost of achieving control objectives
- ☐ Effectiveness of controls
- ☐ Test results of controls

Explanation:

Explanation:

Comparison of cost of achievement of control objectives and corresponding value of assets sought to be protected would provide a sound basis for the information security manager to measure value delivery. Number of controls has no correlation with the value of assets unless the effectiveness of the controls and their cost are also evaluated. Effectiveness of controls has no correlation with the value of assets unless their costs are also evaluated. Test results of controls have no correlation with the value of assets unless the effectiveness of the controls and their cost are also evaluated.

Licensed to Berend Post berend.post@it-university.nl

Question 194

Which of the following is the MOST important item to include when developing web hosting agreements with third-party providers?

- ☐ Termination conditions
- ☐ Liability limits
- ☒ Service levels
- ☐ Privacy restrictions

Explanation:

Explanation:

Service levels are key to holding third parties accountable for adequate delivery of services. This is more important than termination conditions, privacy restrictions or liability limitations.

Question 195

Of the following, who should have PRIMARY responsibility for assessing the security risk associated with an outsourced cloud provider contract?

- ☐ Information security manager
- ☐ Compliance manager
- ☐ Chief information officer
- ☒ Service delivery manager

Question 196

Which of the following BEST reduces the likelihood of leakage of private information via email?

- ☐ Email encryption
- ☐ User awareness training
- ☐ Strong user authentication protocols
- ☒ Prohibition on the personal use of email

Question 197

Isolation and containment measures for a compromised computer has been taken and information security management is now investigating. What is the MOST appropriate next step?

- ☐ Run a forensics tool on the machine to gather evidence
- ☐ Reboot the machine to break remote connections
- ☒ Make a copy of the whole system's memory
- ☐ Document current connections and open Transmission Control Protocol/User Datagram Protocol (TCP/ I'DP) ports

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

When investigating a security breach, it is important to preserve all traces of evidence left by the invader. For this reason, it is imperative to preserve the memory' contents of the machine in order to analyze them later. The correct answer is choice C because a copy of the whole system's memory is obtained for future analysis by running the appropriate tools. This is also important from a legal perspective since an attorney may suggest that the system was changed during the conduct of the investigation. Running a computer forensics tool in the compromised machine will cause the creation of at least one process that may overwrite evidence. Rebooting the machine will delete the contents of the memory, erasing potential evidence. Collecting information about current connections and open Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports is correct, but doing so by using tools may also erase memory contents.

Question 198

Why is "slack space" of value to an information security manager as pan of an incident investigation?

- ☒ Hidden data may be stored there
- ☐ The slack space contains login information
- ☐ Slack space is encrypted
- ☐ It provides flexible space for the investigation

Explanation:

Explanation:

"Slack space" is the unused space between where the fdc data end and the end of the cluster the data occupy. Login information is not typically stored in the slack space. Encryption for the slack space is no different from the rest of the file system. The slack space is not a viable means of storage during an investigation.

Question 199

Who should determine the appropriate classification of accounting ledger data located on a database server and maintained by a database administrator in the IT department?

- ☐ Database administrator (DBA)
- ☒ Finance department management
- ☐ Information security manager
- ☐ IT department management

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Data owners are responsible for determining data classification; in this case, management of the finance department would be the owners of accounting ledger data. The database administrator (DBA) and IT management are the custodians of the data who would apply the appropriate security levels for the classification, while the security manager would act as an advisor and enforcer.

Question 200

Which of the following results from the risk assessment process would BEST assist risk management decision making?

- ☐ Control risk
- ☐ Inherent risk
- ☐ Risk exposure
- ☒ Residual risk

Explanation:

Explanation:

Residual risk provides management with sufficient information to decide to the level of risk that an organization is willing to accept. Control risk is the risk that a control may not succeed in preventing an undesirable event. Risk exposure is the likelihood of an undesirable event occurring. Inherent risk is an important factor to be considered during the risk assessment.

Question 201

Which of the following is the MOST appropriate individual to ensure that new exposures have not been introduced into an existing application during the change management process?

- ☐ System analyst
- ☒ System user
- ☐ Operations manager
- ☐ Data security officer

Explanation:

Explanation:

System users, specifically the user acceptance testers, would be in the best position to note whether new exposures are introduced during the change management process. The system designer or system analyst, data security officer and operations manager would not be as closely involved in testing code changes.

Licensed to Berend Post berend.post@it-university.nl

Question 202

After a risk assessment, it is determined that the cost to mitigate the risk is much greater than the benefit to be derived. The information security manager should recommend to business management that the risk be:

- ☐ transferred.
- ☐ treated.
- ☒ accepted.
- ☐ terminated.

Explanation:

Explanation:

When the cost of control is more than the cost of the risk, the risk should be accepted. Transferring, treating or terminating the risk is of limited benefit if the cost of that control is more than the cost of the risk itself.

Question 203

At what stage of the applications development process should the security department initially become involved?

- ☐ When requested
- ☐ At testing
- ☐ At programming
- ☒ At detail requirements

Explanation:

Explanation:

Information security has to be integrated into the requirements of the application's design. It should also be part of the information security governance of the organization. The application owner may not make a timely request for security involvement. It is too late during systems testing, since the requirements have already been agreed upon. Code reviews are part of the final quality assurance process.

Licensed to Berend Post berend.post@it-university.nl

Question 204

Which of the following is the MOST appropriate method for deploying operating system (OS) patches to production application servers?

- ☐ Batch patches into frequent server updates
- ☒ Initially load the patches on a test machine
- ☐ Set up servers to automatically download patches
- ☐ Automatically push all patches to the servers

Explanation:

Explanation:

Some patches can conflict with application code. For this reason, it is very important to first test all patches in a test environment to ensure that there are no conflicts with existing application systems. For this reason, choices C and D are incorrect as they advocate automatic updating. As for frequent server updates, this is an incomplete (vague) answer from the choices given.

Question 205

Which of the following is the MOST important consideration for an organization interacting with the media during a disaster?

- ☒ Communicating specially drafted messages by an authorized person
- ☐ Refusing to comment until recovery
- ☐ Referring the media to the authorities
- ☐ Reporting the losses and recovery strategy to the media

Explanation:

Explanation:

Proper messages need to be sent quickly through a specific identified person so that there are no rumors or statements made that may damage reputation. Choices B, C and D are not recommended until the message to be communicated is made clear and the spokesperson has already spoken to the media.

Question 206

Which of the following would BEST assist an IS manager in gaining strategic support from executive management?

- ☐ Annual report of security incidents within the organization
- ☐ Research on trends in global information security breaches
- ☐ Rating of the organization's security, based on international standards
- ☒ Risk analysis specific to the organization

Licensed to Berend Post berend.post@it-university.nl

Question 207

Which of the following is the PRIMARY prerequisite to implementing data classification within an organization?

- ☐ Defining job roles
- ☐ Performing a risk assessment
- ☒ Identifying data owners
- ☐ Establishing data retention policies

Explanation:

Explanation:

Identifying the data owners is the first step, and is essential to implementing data classification. Defining job roles is not relevant. Performing a risk assessment is important, but will require the participation of data owners (who must first be identified). Establishing data retention policies may occur after data have been classified.

Question 208

The PRIMARY purpose of using risk analysis within a security program is to:

- ☐ justify the security expenditure.
- ☐ help businesses prioritize the assets to be protected.
- ☐ inform executive management of residual risk value.
- ☒ assess exposures and plan remediation.

Explanation:

Explanation:

Risk analysis explores the degree to which an asset needs protecting so this can be managed effectively. Risk analysis indirectly supports the security expenditure, but justifying the security expenditure is not its primary purpose. Helping businesses prioritize the assets to be protected is an indirect benefit of risk analysis, but not its primary purpose. Informing executive management of residual risk value is not directly relevant.

Question 209

Which of the following would be the MOST important factor to be considered in the loss of mobile equipment with unencrypted data?

- ☐ Disclosure of personal information
- ☐ Sufficient coverage of the insurance policy for accidental losses
- ☒ Intrinsic value of the data stored on the equipment
- ☐ Replacement cost of the equipment

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

When mobile equipment is lost or stolen, the information contained on the equipment matters most in determining the impact of the loss. The more sensitive the information, the greater the liability. If staff carries mobile equipment for business purposes, an organization must develop a clear policy as to what information should be kept on the equipment and for what purpose. Personal information is not defined in the question as the data that were lost. Insurance may be a relatively smaller issue as compared with information theft or opportunity loss, although insurance is also an important factor for a successful business. Cost of equipment would be a less important issue as compared with other choices.

Question 210

Which of the following would be the BEST defense against sniffing?

- ☐ Password protect the files
- ☐ Implement a dynamic IP address scheme
- ☒ Encrypt the data being transmitted
- ☐ Set static mandatory access control (MAC) addresses

Explanation:

Explanation:

Encrypting the data will obfuscate the data so that they are not visible in plain text. Someone would have to collate the entire data stream and try decrypting it, which is not easy. Passwords can be recovered by brute-force attacks and by password crackers, so this is not the best defense against sniffing. IP addresses can always be discovered, even if dynamic IP addresses are implemented. The person sniffing traffic can initiate multiple sessions for possible IP addresses. Setting static mandatory access control (MAC) addresses can prevent address resolution protocol (ARP) poisoning, but it does not prevent sniffing.

Question 211

The PRIMARY purpose for continuous monitoring of security controls is to ensure:

- ☐ system availability.
- ☐ control gaps are minimized.
- ☒ effectiveness of controls.
- ☐ alignment with compliance requirements.

Licensed to Berend Post berend.post@it-university.nl

Question 212

Which of the following would BEST help to identify vulnerabilities introduced by changes to an organization's technical infrastructure?

- ☐ An intrusion detection system
- ☐ Established security baselines
- ☒ Penetration testing
- ☐ Log aggregation and correlation

Question 213

To justify its ongoing security budget, which of the following would be of MOST use to the information security' department?

- ☐ Security breach frequency
- ☐ Annualized loss expectancy (ALE)
- ☒ Cost-benefit analysis
- ☐ Peer group comparison

Explanation:

Explanation:

Cost-benefit analysis is the legitimate way to justify budget. The frequency of security breaches may assist the argument for budget but is not the key tool; it does not address the impact. Annualized loss expectancy (ALE) does not address the potential benefit of security investment. Peer group comparison would provide a good estimate for the necessary security budget but it would not take into account the specific needs of the organization.

Question 214

Who is responsible for ensuring that information is classified?

- ☐ Senior management
- ☐ Security manager
- ☒ Data owner
- ☐ Custodian

Explanation:

Explanation:

The data owner is responsible for applying the proper classification to the data. Senior management is ultimately responsible for the organization. The security officer is responsible for applying security protection relative to the level of classification specified by the owner. The technology group is delegated the custody of the data by the data owner, but the group does not classify the information.

Licensed to Berend Post berend.post@it-university.nl

Question 215

Security awareness training is MOST likely to lead to which of the following?

- ☐ Decrease in intrusion incidents
- ☒ Increase in reported incidents
- ☐ Decrease in security policy changes
- ☐ Increase in access rule violations

Explanation:

Explanation:

Reported incidents will provide an indicator as to the awareness level of staff. An increase in reported incidents could indicate that staff is paying more attention to security. Intrusion incidents and access rule violations may or may not have anything to do with awareness levels. A decrease in changes to security policies may or may not correlate to security awareness training.

Question 216

Which of the following is the BEST tool to maintain the currency and coverage of an information security program within an organization?

- ☒ The program's governance oversight mechanisms
- ☐ Information security periodicals and manuals
- ☐ The program's security architecture and design
- ☐ Training and certification of the information security team

Explanation:

Explanation:

While choices B, C and D will all assist the currency and coverage of the program, its governance oversight mechanisms are the best method.

Question 217

An operating system (OS) noncritical patch to enhance system security cannot be applied because a critical application is not compatible with the change. Which of the following is the BEST solution?

- ☐ Rewrite the application to conform to the upgraded operating system
- ☒ Compensate for not installing the patch with mitigating controls
- ☐ Alter the patch to allow the application to run in a privileged state
- ☐ Run the application on a test platform; tune production to allow patch and application

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Since the operating system (OS) patch will adversely impact a critical application, a mitigating control should be identified that will provide an equivalent level of security. Since the application is critical, the patch should not be applied without regard for the application; business requirements must be considered. Altering the OS patch to allow the application to run in a privileged state may create new security weaknesses. Finally, running a production application on a test platform is not an acceptable alternative since it will mean running a critical production application on a platform not subject to the same level of security controls.

Question 218

When designing an information security quarterly report to management, the MOST important element to be considered should be the:

- ☐ information security metrics.
- ☐ knowledge required to analyze each issue.
- ☒ linkage to business area objectives.
- ☐ baseline against which metrics are evaluated.

Explanation:

Explanation:

The link to business objectives is the most important clement that would be considered by management. Information security metrics should be put in the context of impact to management objectives. Although important, the security knowledge required would not be the first element to be considered. Baselining against the information security metrics will be considered later in the process.

Question 219

A project manager is developing a developer portal and requests that the security manager assign a public IP address so that it can be accessed by in-house staff and by external consultants outside the organization's local area network (LAN). What should the security manager do FIRST?

- ☒ Understand the business requirements of the developer portal
- ☐ Perform a vulnerability assessment of the developer portal
- ☐ Install an intrusion detection system (IDS)
- ☐ Obtain a signed nondisclosure agreement (NDA) from the external consultants before allowing external access to the server

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The information security manager cannot make an informed decision about the request without first understanding the business requirements of the developer portal. Performing a vulnerability assessment of developer portal and installing an intrusion detection system (IDS) are best practices but are subsequent to understanding the requirements. Obtaining a signed nondisclosure agreement will not take care of the risks inherent in the organization's application.

Question 220

An emergency change was made to an IT system as a result of a failure. Which of the following should be of GREATEST concern to the organization's information security manager?

- ☐ The change did not include a proper assessment of risk.
- ☐ Documentation of the change was made after implementation.
- ☐ The information security manager did not review the change prior to implementation.
- ☒ The operations team implemented the change without regression testing.

Question 221

In order to highlight to management, the importance of integrating information security in the business processes, a newly hired information security officer should FIRST:

- ☐ prepare a security budget.
- ☒ conduct a risk assessment.
- ☐ develop an information security policy.
- ☐ obtain benchmarking information.

Explanation:

Explanation:

Risk assessment, evaluation and impact analysis will be the starting point for driving management's attention to information security. All other choices will follow the risk assessment.

Question 222

Which would be one of the BEST metrics an information security manager can employ to effectively evaluate the results of a security program?

- ☐ Number of controls implemented
- ☒ Percent of control objectives accomplished
- ☐ Percent of compliance with the security policy
- ☐ Reduction in the number of reported security incidents

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Control objectives are directly related to business objectives; therefore, they would be the best metrics. Number of controls implemented does not have a direct relationship with the results of a security program. Percentage of compliance with the security policy and reduction in the number of security incidents are not as broad as choice B.

Question 223

Which of the following devices should be placed within a demilitarized zone (DMZ)?

- ☐ Network switch
- ☒ Web server
- ☐ Database server
- ☐ File/print server

Explanation:

Explanation:

A web server should normally be placed within a demilitarized zone (DMZ) to shield the internal network. Database and file/print servers may contain confidential or valuable data and should always be placed on the internal network, never on a DMZ that is subject to compromise. Switches may bridge a DMZ to another network but do not technically reside within the DMZ network segment.

Question 224

Which of the following would be MOST critical to the successful implementation of a biometric authentication system?

- ☐ Budget allocation
- ☐ Technical skills of staff
- ☒ User acceptance
- ☐ Password requirements

Explanation:

Explanation:

End users may react differently to the implementation, and may have specific preferences. The information security manager should be aware that what is viewed as reasonable in one culture may not be acceptable in another culture. Budget allocation will have a lesser impact since what is rejected as a result of culture cannot be successfully implemented regardless of budgetary considerations. Technical skills of staff will have a lesser impact since new staff can be recruited or existing staff can be trained. Although important, password requirements would be less likely to guarantee the success of the implementation.

Licensed to Berend Post berend.post@it-university.nl

Question 225

Which of the following is the MOST appropriate frequency for updating antivirus signature files for antivirus software on production servers?

- ☒ Daily
- ☐ Weekly
- ☐ Concurrently with O/S patch updates
- ☐ During scheduled change control updates

Explanation:

Explanation:

New viruses are being introduced almost daily. The effectiveness of virus detection software depends on frequent updates to its virus signatures, which are stored on antivirus signature files so updates may be carried out several times during the day. At a minimum, daily updating should occur. Patches may occur less frequently. Weekly updates may potentially allow new viruses to infect the system.

Question 226

To achieve effective strategic alignment of security initiatives, it is important that:

- ☐ Steering committee leadership be selected by rotation.
- ☒ Inputs be obtained and consensus achieved between the major organizational units.
- ☐ The business strategy be updated periodically.
- ☐ Procedures and standards be approved by all departmental heads.

Explanation:

Explanation:

It is important to achieve consensus on risks and controls, and obtain inputs from various organizational entities since security needs to be aligned to the needs of the organization. Rotation of steering committee leadership does not help in achieving strategic alignment. Updating business strategy does not lead to strategic alignment of security initiatives. Procedures and standards need not be approved by all departmental heads

Question 227

Which of the following authentication methods prevents authentication replay?

- ☐ Password hash implementation
- ☒ Challenge/response mechanism
- ☐ Wired Equivalent Privacy (WEP) encryption usage
- ☐ HTTP Basic Authentication

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

A challenge/response mechanism prevents replay attacks by sending a different random challenge in each authentication event. The response is linked to that challenge. Therefore, capturing the authentication handshake and replaying it through the network will not work. Using hashes by itself will not prevent a replay. A WEP key will not prevent sniffing (it just takes a few more minutes to break the WEP key if the attacker does not already have it) and therefore will not be able to prevent recording and replaying an authentication handshake. HTTP Basic Authentication is clear text and has no mechanisms to prevent replay.

Question 228

Information security policies should:

- ☐ address corporate network vulnerabilities.
- ☐ address the process for communicating a violation.
- ☒ be straightforward and easy to understand.
- ☐ be customized to specific groups and roles.

Explanation:

Explanation:

As high-level statements, information security policies should be straightforward and easy to understand. They arc high-level and, therefore, do not address network vulnerabilities directly or the process for communicating a violation. As policies, they should provide a uniform message to all groups and user roles.

Question 229

Which of the following is the MOST appropriate use of gap analysis?

- ☐ Evaluating a business impact analysis (BIA)
- ☐ Developing a balanced business scorecard
- ☐ Demonstrating the relationship between controls
- ☒ Measuring current state vs. desired future state

Explanation:

Explanation:

A gap analysis is most useful in addressing the differences between the current state and an ideal future state. It is not as appropriate for evaluating a business impact analysis (BIA), developing a balanced business scorecard or demonstrating the relationship between variables.

Licensed to Berend Post berend.post@it-university.nl

Question 230

An information security program should focus on:

- ☐ best practices also in place at peer companies.
- ☐ solutions codified in international standards.
- ☒ key controls identified in risk assessments.
- ☐ continued process improvement.

Explanation:

Explanation:

Risk assessment identifies the appropriate controls to mitigate identified business risks that the program should implement to protect the business. Peer industry best practices, international standards and continued process improvement can be used to support the program, but these cannot be blindly implemented without the consideration of business risk.

Question 231

The recovery point objective (RPO) requires which of the following?

- ☐ Disaster declaration
- ☒ Before-image restoration
- ☐ System restoration
- ☐ After-image processing

Explanation:

Explanation:

The recovery point objective (RPO) is the point in the processing flow at which system recovery should occur. This is the predetermined state of the application processing and data used to restore the system and to continue the processing flow. Disaster declaration is independent of this processing checkpoint. Restoration of the system can occur at a later date, as does the return to normal, after-image processing.

Question 232

Ensuring that activities performed by outsourcing providers comply with information security policies can BEST be accomplished through the use of:

- ☒ service level agreements.
- ☐ explicit contract language.
- ☐ local regulations.
- ☐ independent audits.

Licensed to Berend Post berend.post@it-university.nl

Question 233

The PRIMARY focus of the change control process is to ensure that changes are:

- ☒ authorized.
- ☐ applied.
- ☐ documented.
- ☐ tested.

Explanation:

Explanation:

All steps in the change control process must be signed off on to ensure proper authorization. It is important that changes are applied, documented and tested; however, they are not the primary focus.

Question 234

The FIRST step in developing an information security management program is to:

- ☐ identify business risks that affect the organization.
- ☒ clarify organizational purpose for creating the program.
- ☐ assign responsibility for the program.
- ☐ assess adequacy of controls to mitigate business risks.

Explanation:

Explanation:

In developing an information security management program, the first step is to clarify the organization's purpose for creating the program. This is a business decision based more on judgment than on any specific quantitative measures. After clarifying the purpose, the other choices are assigned and acted upon.

Question 235

When properly tested, which of the following would MOST effectively support an information security manager in handling a security breach?

- ☐ Business continuity plan
- ☐ Disaster recovery plan
- ☒ Incident response plan
- ☐ Vulnerability management plan

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

An incident response plan documents the step-by-step process to follow, as well as the related roles and responsibilities pertaining to all parties involved in responding to an information security breach. A business continuity plan or disaster recovery plan would be triggered during the execution of the incident response plan in the case of a breach impacting the business continuity. A vulnerability management plan is a procedure to address technical vulnerabilities and mitigate the risk through configuration changes (patch management).

Question 236

A global financial institution has decided not to take any further action on a denial of service (DoS) risk found by the risk assessment team. The MOST likely reason they made this decision is that:

- ☐ there are sufficient safeguards in place to prevent this risk from happening.
- ☐ the needed countermeasure is too complicated to deploy.
- ☒ the cost of countermeasure outweighs the value of the asset and potential loss.
- ☐ The likelihood of the risk occurring is unknown.

Explanation:

Explanation:

An organization may decide to live with specific risks because it would cost more to protect themselves than the value of the potential loss. The safeguards need to match the risk level. While countermeasures could be too complicated to deploy, this is not the most compelling reason. It is unlikely that a global financial institution would not be exposed to such attacks and the frequency could not be predicted.

Question 237

Which of the following should be in place before a black box penetration test begins?

- ☐ IT management approval
- ☐ Proper communication and awareness training
- ☒ A clearly stated definition of scope
- ☐ An incident response plan

Explanation:

Explanation:

Having a clearly stated definition of scope is most important to ensure a proper understanding of risk as well as success criteria, IT management approval may not be required based on senior management decisions. Communication, awareness and an incident response plan are not a necessary requirement. In fact, a penetration test could help promote the creation and execution of the incident response plan.

Licensed to Berend Post berend.post@it-university.nl

Question 238

The "separation of duties" principle is violated if which of the following individuals has update rights to the database access control list (ACL)?

- ☐ Data owner
- ☐ Data custodian
- ☒ Systems programmer
- ☐ Security administrator

Explanation:

Explanation:

A systems programmer should not have privileges to modify the access control list (ACL) because this would give the programmer unlimited control over the system. The data owner would request and approve updates to the ACL, but it is not a violation of the separation of duties principle if the data owner has update rights to the ACL. The data custodian and the security administrator could carry out the updates on the ACL since it is part of their duties as delegated to them by the data owner.

Question 239

Which of the following is the BEST method to securely transfer a message?

- ☐ Password-protected removable media
- ☐ Facsimile transmission in a secured room
- ☒ Using public key infrastructure (PKI) encryption
- ☐ Steganography

Explanation:

Explanation:

Using public key infrastructure (PKI) is currently accepted as the most secure method to transmit e-mail messages. PKI assures confidentiality, integrity and nonrepudiation. The other choices are not methods that are as secure as PKI. Steganography involves hiding a message in an image.

Question 240

Which of the following is the MOST immediate consequence of failing to tune a newly installed intrusion detection system (IDS) with the threshold set to a low value?

- ☒ The number of false positives increases
- ☐ The number of false negatives increases
- ☐ Active probing is missed
- ☐ Attack profiles are ignored

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Failure to tune an intrusion detection system (IDS) will result in many false positives, especially when the threshold is set to a low value. The other options are less likely given the fact that the threshold for sounding an alarm is set to a low value.

Question 241

The PRIMARY driver to obtain external resources to execute the information security program is that external resources can:

- ☒ contribute cost-effective expertise not available internally.
- ☐ be made responsible for meeting the security program requirements.
- ☐ replace the dependence on internal resources.
- ☐ deliver more effectively on account of their knowledge.

Explanation:

Explanation:

Choice A represents the primary driver for the information security manager to make use of external resources. The information security manager will continue to be responsible for meeting the security program requirements despite using the services of external resources. The external resources should never completely replace the role of internal resources from a strategic perspective. The external resources cannot have a better knowledge of the business of the information security manager's organization than do the internal resources.

Question 242

What is the BEST technique to determine which security controls to implement with a limited budget?

- ☐ Risk analysis
- ☐ Annualized loss expectancy (ALE) calculations
- ☒ Cost-benefit analysis
- ☐ Impact analysis

Explanation:

Explanation:

Cost-benefit analysis is performed to ensure that the cost of a safeguard does not outweigh its benefit and that the best safeguard is provided for the cost of implementation. Risk analysis identifies the risks and suggests appropriate mitigation. The annualized loss expectancy (ALE) is a subset of a cost-benefit analysis. Impact analysis would indicate how much could be lost if a specific threat occurred.

Licensed to Berend Post berend.post@it-university.nl

Question 243

Which of the following is the PRIMARY benefit of implementing a maturity model for information security management?

- ☐ Information security management costs will be optimized.
- ☐ Information security strategy will be in line with industry best practice.
- ☒ Gaps between current and desirable levels will be addressed.
- ☐ Staff awareness of information security compliance will be promoted.

Question 244

In organizations where availability is a primary concern, the MOST critical success factor of the patch management procedure would be the:

- ☒ testing time window prior to deployment.
- ☐ technical skills of the team responsible.
- ☐ certification of validity for deployment.
- ☐ automated deployment to all the servers.

Explanation:

Explanation:

Having the patch tested prior to implementation on critical systems is an absolute prerequisite where availability is a primary concern because deploying patches that could cause a system to fail could be worse than the vulnerability corrected by the patch. It makes no sense to deploy patches on every system. Vulnerable systems should be the only candidate for patching. Patching skills are not required since patches are more often applied via automated tools.

Question 245

Which of the following is the MOST effective solution for preventing internal users from modifying sensitive and classified information?

- ☐ Baseline security standards
- ☐ System access violation logs
- ☒ Role-based access controls
- ☐ Exit routines

Explanation:

Explanation:

Role-based access controls help ensure that users only have access to files and systems appropriate for their job role. Violation logs are detective and do not prevent unauthorized access. Baseline

Licensed to Berend Post berend.post@it-university.nl

security standards do not prevent unauthorized access. Exit routines are dependent upon appropriate role-based access.

Question 246

Which of the following has the MOST direct impact on the usability of an organization's asset classification program?

- ☒ The granularity of classifications in the hierarchy
- ☐ The frequency of updates to the organization's risk register
- ☐ The business objectives of the organization
- ☐ The support of senior management for the classification scheme

Question 247

Which of the following will BEST protect against malicious activity by a former employee?

- ☐ Preemployment screening
- ☐ Close monitoring of users
- ☐ Periodic awareness training
- ☒ Effective termination procedures

Explanation:

Explanation:

When an employee leaves an organization, the former employee may attempt to use their credentials to perform unauthorized or malicious activity. Accordingly, it is important to ensure timely revocation of all access at the time an individual is terminated. Security awareness training, preemployment screening and monitoring are all important, but are not as effective in preventing this type of situation.

Question 248

The BEST strategy for risk management is to:

- ☐ achieve a balance between risk and organizational goals.
- ☒ reduce risk to an acceptable level.
- ☐ ensure that policy development properly considers organizational risks.
- ☐ ensure that all unmitigated risks are accepted by management.

Explanation:

Explanation:

The best strategy for risk management is to reduce risk to an acceptable level, as this will take into account the organization's appetite for risk and the fact that it would not be practical to eliminate all

Licensed to Berend Post berend.post@it-university.nl

risk. Achieving balance between risk and organizational goals is not always practical. Policy development must consider organizational risks as well as business objectives. It may be prudent to ensure that management understands and accepts risks that it is not willing to mitigate, but that is a practice and is not sufficient to l>e considered a strategy.

Question 249

Emergency actions are taken at the early stage of a disaster with the purpose of preventing injuries or loss of life and:

- ☐ determining the extent of property damage.
- ☐ preserving environmental conditions.
- ☐ ensuring orderly plan activation.
- ☒ reducing the extent of operational damage.

Explanation:

Explanation:

During an incident, emergency actions should minimize or eliminate casualties and damage to the business operation, thus reducing business interruptions. Determining the extent of property damage is not the consideration; emergency actions should minimize, not determine, the extent of the damage. Protecting/preserving environmental conditions may not be relevant. Ensuring orderly plan activation is important but not as critical as reducing damage to the operation.

Question 250

The PRIMARY purpose of involving third-party teams for carrying out post event reviews of information security incidents is to:

- ☒ enable independent and objective review of the root cause of the incidents.
- ☐ obtain support for enhancing the expertise of the third-party teams.
- ☐ identify lessons learned for further improving the information security management process.
- ☐ obtain better buy-in for the information security program.

Explanation:

Explanation:

It is always desirable to avoid the conflict of interest involved in having the information security team carries out the post event review. Obtaining support for enhancing the expertise of the third-party teams is one of the advantages, but is not the primary driver. Identifying lessons learned for further improving the information security management process is the general purpose of carrying out the post event review. Obtaining better buy-in for the information security program is not a valid reason for involving third-party teams.

Licensed to Berend Post berend.post@it-university.nl

Question 251

Which of the following guarantees that data in a file have not changed?

- ☐ Inspecting the modified date of the file
- ☐ Encrypting the file with symmetric encryption
- ☐ Using stringent access control to prevent unauthorized access
- ☒ Creating a hash of the file, then comparing the file hashes

Explanation:

Explanation:

A hashing algorithm can be used to mathematically ensure that data haven't been changed by hashing a file and comparing the hashes after a suspected change.

Question 252

Security audit reviews should PRIMARILY:

- ☒ ensure that controls operate as required.
- ☐ ensure that controls are cost-effective.
- ☐ focus on preventive controls.
- ☐ ensure controls are technologically current.

Explanation:

Explanation:

The primary objective of a security review or audit should be to provide assurance on the adequacy of security controls. Reviews should focus on all forms of control, not just on preventive control. Cost-effectiveness and technological currency are important but not as critical.

Question 253

The implementation of a capacity plan would prevent:

- ☐ file system overload arising from distributed denial-of-service attacks
- ☐ system downtime for scheduled security maintenance
- ☐ software failures arising from exploitation of buffer capacity vulnerabilities
- ☒ application failures arising from insufficient hardware resources

Licensed to Berend Post berend.post@it-university.nl

Question 254

The MOST important reason for formally documenting security procedures is to ensure:

- ☒ processes are repeatable and sustainable.
- ☐ alignment with business objectives.
- ☐ auditability by regulatory agencies.
- ☐ objective criteria for the application of metrics.

Explanation:

Explanation:

Without formal documentation, it would be difficult to ensure that security processes are performed in the proper manner every time that they are performed. Alignment with business objectives is not a function of formally documenting security procedures. Processes should not be formally documented merely to satisfy an audit requirement. Although potentially useful in the development of metrics, creating formal documentation to assist in the creation of metrics is a secondary objective.

Question 255

Which of the following is the BEST method to ensure the overall effectiveness of a risk management program?

- ☐ User assessments of changes
- ☐ Comparison of the program results with industry standards
- ☐ Assignment of risk within the organization
- ☒ Participation by all members of the organization

Explanation:

Explanation:

Effective risk management requires participation, support and acceptance by all applicable members of the organization, beginning with the executive levels. Personnel must understand their responsibilities and be trained on how to fulfill their roles.

Licensed to Berend Post berend.post@it-university.nl

Question 256

A company's mail server allows anonymous file transfer protocol (FTP) access which could be exploited. What process should the information security manager deploy to determine the necessity for remedial action?

- ☐ A penetration test
- ☐ A security baseline review
- ☒ A risk assessment
- ☐ A business impact analysis (BIA)

Explanation:

Explanation:

A risk assessment will identify- the business impact of such vulnerability being exploited and is, thus, the correct process. A penetration test or a security baseline review may identify the vulnerability but not the remedy. A business impact analysis (BIA) will more likely identify the impact of the loss of the mail server.

Question 257

Which of the following is a potential indicator of inappropriate Internet use by staff?

- ☐ Increased help desk calls for password resets
- ☐ Reduced number of pings on firewalls
- ☒ Increased reports of slow system performance
- ☐ Increased number of weakness from vulnerability scans

Question 258

Which of the following is the MOST important prerequisite for establishing information security management within an organization?

- ☒ Senior management commitment
- ☐ Information security framework
- ☐ Information security organizational structure
- ☐ Information security policy

Explanation:

Explanation:

Senior management commitment is necessary in order for each of the other elements to succeed. Without senior management commitment, the other elements will likely be ignored within the organization.

Licensed to Berend Post berend.post@it-university.nl

Question 259

Risk assessment is MOST effective when performed:

- ☐ at the beginning of security program development.
- ☒ on a continuous basis.
- ☐ while developing the business case for the security program.
- ☐ during the business change process.

Explanation:

Explanation:

Risk assessment needs to be performed on a continuous basis because of organizational and technical changes. Risk assessment must take into account all significant changes in order to be effective.

Question 260

Which of the following is MOST essential for a risk management program to be effective?

- ☐ Flexible security budget
- ☐ Sound risk baseline
- ☒ New risks detection
- ☐ Accurate risk reporting

Explanation:

Explanation:

All of these procedures are essential for implementing risk management. However, without identifying new risks, other procedures will only be useful for a limited period.

Question 261

Which of the following is MOST important to the success of an information security program?

- ☐ Security' awareness training
- ☐ Achievable goals and objectives
- ☒ Senior management sponsorship
- ☐ Adequate start-up budget and staffing

Explanation:

Explanation:

Sufficient senior management support is the most important factor for the success of an information security program. Security awareness training, although important, is secondary. Achievable goals

Licensed to Berend Post berend.post@it-university.nl

and objectives as well as having adequate budgeting and staffing are important factors, but they will not ensure success if senior management support is not present.

Question 262

A large organization is considering a policy that would allow employees to bring their own smartphones into the organizational environment. The MOST important concern to the information security manager should be the:

- ☐ higher costs in supporting end users
- ☐ impact on network capacity
- ☐ decrease in end user productivity
- ☒ lack of a device management solution

Explanation:

Reference https://www.isaca.org/Journal/archives/2013/Volume-4/Pages/Leveraging-and-Securing-the-Bring-Your-Own-Device-and-Technology-Approach.aspx

Question 263

In implementing information security governance, the information security manager is PRIMARILY responsible for:

- ☒ developing the security strategy.
- ☐ reviewing the security strategy.
- ☐ communicating the security strategy.
- ☐ approving the security strategy

Explanation:

Explanation:

The information security manager is responsible for developing a security strategy based on business objectives with the help of business process owners. Reviewing the security strategy is the responsibility of a steering committee. The information security manager is not necessarily responsible for communicating or approving the security strategy.

Licensed to Berend Post berend.post@it-university.nl

Question 264

Once a suite of security controls has been successfully implemented for an organization's business units, it is MOST important for the information security manager to:

- ☒ ensure the controls are regularly tested for ongoing effectiveness.
- ☐ hand over the controls to the relevant business owners.
- ☐ prepare to adapt the controls for future system upgrades.
- ☐ perform testing to compare control performance against industry levels.

Question 265

In business-critical applications, user access should be approved by the:

- ☐ information security manager.
- ☒ data owner.
- ☐ data custodian.
- ☐ business management.

Explanation:

Explanation:

A data owner is in the best position to validate access rights to users due to their deep understanding of business requirements and of functional implementation within the application. This responsibility should be enforced by the policy. An information security manager will coordinate and execute the implementation of the role-based access control. A data custodian will ensure that proper safeguards are in place to protect the data from unauthorized access; it is not the data custodian's responsibility to assign access rights. Business management is not. in all cases, the owner of the data.

Question 266

An information security manager believes that a network file server was compromised by a hacker. Which of the following should be the FIRST action taken?

- ☐ Unsure that critical data on the server are backed up.
- ☐ Shut down the compromised server.
- ☒ Initiate the incident response process.
- ☐ Shut down the network.

Explanation:

Explanation:

The incident response process will determine the appropriate course of action. If the data have been corrupted by a hacker, the backup may also be corrupted. Shutting down the server is likely to destroy any forensic evidence that may exist and may be required by the investigation. Shutting down the network is a drastic action, especially if the hacker is no longer active on the network.

Licensed to Berend Post berend.post@it-university.nl

Question 267

If an organization considers taking legal action on a security incident, the information security manager should focus PRIMARILY on:

- ☐ obtaining evidence as soon as possible.
- ☒ preserving the integrity of the evidence.
- ☐ disconnecting all IT equipment involved.
- ☐ reconstructing the sequence of events.

Explanation:

Explanation:

The integrity of evidence should be kept, following the appropriate forensic techniques to obtain the evidence and a chain of custody procedure to maintain the evidence (in order to be accepted in a court of law). All other options are pan of the investigative procedure, but they are not as important as preserving the integrity of the evidence.

Question 268

Which of the following mechanisms is the MOST secure way to implement a secure wireless network?

- ☐ Filter media access control (MAC) addresses
- ☒ Use a Wi-Fi Protected Access (WPA2) protocol
- ☐ Use a Wired Equivalent Privacy (WEP) key
- ☐ Web-based authentication

Explanation:

Explanation:

WPA2 is currently one of the most secure authentication and encryption protocols for mainstream wireless products. MAC address filtering by itself is not a good security mechanism since allowed MAC addresses can be easily sniffed and then spoofed to get into the network. WEP is no longer a secure encryption mechanism for wireless communications. The WEP key can be easily broken within minutes using widely available software. And once the WEP key is obtained, all communications of every other wireless client are exposed. Finally, a web-based authentication mechanism can be used to prevent unauthorized user access to a network, but it will not solve the wireless network's main security issues, such as preventing network sniffing.

Licensed to Berend Post berend.post@it-university.nl

Question 269

Which of the following risks would BEST be assessed using qualitative risk assessment techniques?

- ☐ Theft of purchased software
- ☐ Power outage lasting 24 hours
- ☒ Permanent decline in customer confidence
- ☐ Temporary loss of e-mail due to a virus attack

Explanation:

Explanation:

A permanent decline in customer confidence does not lend itself well to measurement by quantitative techniques. Qualitative techniques are more effective in evaluating things such as customer loyalty and goodwill. Theft of software, power outages and temporary loss of e-mail can be quantified into monetary amounts easier than can be assessed with quantitative techniques.

Question 270

Phishing is BEST mitigated by which of the following?

- ☐ Security monitoring software
- ☐ Encryption
- ☐ Two-factor authentication
- ☒ User awareness

Explanation:

Explanation:

Phishing can best be detected by the user. It can be mitigated by appropriate user awareness. Security monitoring software would provide some protection, but would not be as effective as user awareness. Encryption and two-factor authentication would not mitigate this threat.

Question 271

Managing the life cycle of a digital certificate is a role of a(n):

- ☐ system administrator.
- ☐ security administrator.
- ☐ system developer.
- ☒ independent trusted source.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Digital certificates must be managed by an independent trusted source in order to maintain trust in their authenticity. The other options are not necessarily entrusted with this capability.

Question 272

A security risk assessment exercise should be repeated at regular intervals because:

- ☒ business threats are constantly changing.
- ☐ omissions in earlier assessments can be addressed.
- ☐ repetitive assessments allow various methodologies.
- ☐ they help raise awareness on security in the business.

Explanation:

Explanation:

As business objectives and methods change, the nature and relevance of threats change as well. Choice B does not, by itself, justify regular reassessment. Choice C is not necessarily true in all cases. Choice D is incorrect because there are better ways of raising security awareness than by performing a risk assessment.

Question 273

While implementing information security governance an organization should FIRST:

- ☐ adopt security standards.
- ☐ determine security baselines.
- ☒ define the security strategy.
- ☐ establish security policies.

Explanation:

Explanation:

The first step in implementing information security governance is to define the security strategy based on which security baselines are determined. Adopting suitable security- standards, performing risk assessment and implementing security policy are steps that follow the definition of the security strategy.

Licensed to Berend Post berend.post@it-university.nl

Question 274

What is the MOST important success factor in launching a corporate information security awareness program?

- ☐ Adequate budgetary support
- ☐ Centralized program management
- ☒ Top-down approach
- ☐ Experience of the awareness trainers

Explanation:

Explanation:

Senior management support will provide enough resources and will focus attention to the program: training should start at the top levels to gain support and sponsorship. Funding is not a primary concern. Centralized management does not provide sufficient support. Trainer experience, while important, is not the primary success factor.

Question 275

A payroll application system accepts individual user sign-on IDs and then connects to its database using a single application ID. The GREATEST weakness under this system architecture is that:

- ☐ users can gain direct access to the application ID and circumvent data controls.
- ☐ when multiple sessions with the same application ID collide, the database locks up.
- ☐ the database becomes unavailable if the password of the application ID expires.
- ☒ an incident involving unauthorized access to data cannot be tied to a specific user.

Question 276

Of the following, whose input is of GREATEST importance in the development of an information security strategy?

- ☐ End users
- ☐ Corporate auditors
- ☐ Process owners
- ☒ Security architects

Question 277

A risk assessment should be conducted:

- ☐ once a year for each business process and subprocess.
- ☐ every three to six months for critical business processes.
- ☐ by external parties to maintain objectivity.
- ☒ annually or whenever there is a significant change.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Risks are constantly changing. Choice D offers the best alternative because it takes into consideration a reasonable time frame and allows flexibility to address significant change. Conducting a risk assessment once a year is insufficient if important changes take place. Conducting a risk assessment every three-to-six months for critical processes may not be necessary, or it may not address important changes in a timely manner. It is not necessary for assessments to be performed by external parties.

Question 278

An organization shares customer information across its globally dispersed branches. Which of the following should be the GREATEST concern to information security management?

- ☐ Cross-cultural differences between branches
- ☐ Conflicting data protection regulations
- ☒ Insecure wide area networks (WANs)
- ☐ Decentralization of information security

Question 279

Which of the following is the BEST approach for an organization desiring to protect its intellectual property?

- ☐ Conduct awareness sessions on intellectual property policy
- ☐ Require all employees to sign a nondisclosure agreement
- ☐ Promptly remove all access when an employee leaves the organization
- ☒ Restrict access to a need-to-know basis

Explanation:

Explanation:

Security awareness regarding intellectual property policy will not prevent violations of this policy. Requiring all employees to sign a nondisclosure agreement and promptly removing all access when an employee leaves the organization are good controls, but not as effective as restricting access to a need-to- know basis.

Licensed to Berend Post berend.post@it-university.nl

Question 280

The systems administrator did not immediately notify the security officer about a malicious attack. An information security manager could prevent this situation by:

- ☒ periodically testing the incident response plans.
- ☐ regularly testing the intrusion detection system (IDS).
- ☐ establishing mandatory training of all personnel.
- ☐ periodically reviewing incident response procedures.

Explanation:

Explanation:

Security incident response plans should be tested to find any deficiencies and improve existing processes. Testing the intrusion detection system (IDS) is a good practice but would not have prevented this situation. All personnel need to go through formal training to ensure that they understand the process, tools and methodology involved in handling security incidents. However, testing of the actual plans is more effective in ensuring the process works as intended. Reviewing the response procedures is not enough; the security response plan needs to be tested on a regular basis.

Question 281

When messages are encrypted and digitally signed to protect documents transferred between trading partners, the GREATEST concern is that:

- ☐ trading partners can repudiate the transmission of messages.
- ☐ hackers can eavesdrop on messages.
- ☐ trading partners can repudiate the receipt of messages.
- ☒ hackers can introduce forgery messages.

Question 282

The decision as to whether a risk has been reduced to an acceptable level should be determined by:

- ☒ organizational requirements.
- ☐ information systems requirements.
- ☐ information security requirements.
- ☐ international standards.

Explanation:

Explanation:

Organizational requirements should determine when a risk has been reduced to an acceptable level. Information systems and information security should not make the ultimate determination. Since each organization is unique, international standards of best practice do not represent the best solution.

Licensed to Berend Post berend.post@it-university.nl

Question 283

An information security manager mapping a job description to types of data access is MOST likely to adhere to which of the following information security principles?

- ☐ Ethics
- ☒ Proportionality
- ☐ Integration
- ☐ Accountability

Explanation:

Explanation:

Information security controls should be proportionate to the risks of modification, denial of use or disclosure of the information. It is advisable to learn if the job description is apportioning more data than are necessary for that position to execute the business rules (types of data access). Principles of ethics and integration have the least to do with mapping job description to types of data access. The principle of accountability would be the second most adhered to principle since people with access to data may not always be accountable but may be required to perform an operation.

Question 284

Which of the following would be a MAJOR consideration for an organization defining its business continuity plan (BCP) or disaster recovery program (DRP)?

- ☐ Setting up a backup site
- ☐ Maintaining redundant systems
- ☒ Aligning with recovery time objectives (RTOs)
- ☐ Data backup frequency

Explanation:

Explanation:

BCP, DRP should align with business RTOs. The RTO represents the amount of time allowed for the recovery of a business function or resource after a disaster occurs. The RTO must be taken into consideration when prioritizing systems for recovery efforts to ensure that those systems that the business requires first are the ones that are recovered first.

Licensed to Berend Post berend.post@it-university.nl

Question 285

Which of the following is the MOST effective, positive method to promote security awareness?

- ☒ Competitions and rewards for compliance
- ☐ Lock-out after three incorrect password attempts
- ☐ Strict enforcement of password formats
- ☐ Disciplinary action for noncompliance

Explanation:

Explanation:

Competitions and rewards are a positive encouragement to user participation in the security program. Merely locking users out for forgetting their passwords does not enhance user awareness. Enforcement of password formats and disciplinary actions do not positively promote awareness.

Question 286

Which of the following BEST ensures that modifications made to in-house developed business applications do not introduce new security exposures?

- ☐ Stress testing
- ☐ Patch management
- ☒ Change management
- ☐ Security baselines

Explanation:

Explanation:

Change management controls the process of introducing changes to systems to ensure that unintended changes are not introduced. Patch management involves the correction of software weaknesses and helps ensure that newly identified exploits are mitigated in a timely fashion. Security baselines provide minimum recommended settings. Stress testing ensures that there are no scalability problems.

Question 287

The advantage of Virtual Private Network (VPN) tunneling for remote users is that it:

- ☒ helps ensure that communications are secure.
- ☐ increases security between multi-tier systems.
- ☐ allows passwords to be changed less frequently.
- ☐ eliminates the need for secondary authentication.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Virtual Private Network (VPN) tunneling for remote users provides an encrypted link that helps ensure secure communications. It does not affect password change frequency, nor does it eliminate the need for secondary authentication or affect security within the internal network.

Question 288

Which of the following is the MOST important consideration when securing customer credit card data acquired by a point-of-sale (POS) cash register?

- ☐ Authentication
- ☐ Hardening
- ☒ Encryption
- ☐ Nonrepudiation

Explanation:

Explanation:

Cardholder data should be encrypted using strong encryption techniques. Hardening would be secondary in importance, while nonrepudiation would not be as relevant. Authentication of the point-of-sale (POS) terminal is a previous step to acquiring the card information.

Question 289

The PRIMARY reason for assigning classes of sensitivity and criticality to information resources is to provide a basis for:

- ☐ determining the scope for inclusion in an information security program.
- ☒ defining the level of access controls.
- ☐ justifying costs for information resources.
- ☐ determining the overall budget of an information security program.

Explanation:

Explanation:

The assigned class of sensitivity and criticality of the information resource determines the level of access controls to be put in place. The assignment of sensitivity and criticality takes place with the information assets that have already been included in the information security program and has only an indirect bearing on the costs to be incurred. The assignment of sensitivity and criticality contributes to, but does not decide, the overall budget of the information security program.

Licensed to Berend Post berend.post@it-university.nl

Question 290

What of the following is MOST important to include in an information security policy?

- ☐ Maturity levels
- ☐ Best practices
- ☒ Management objectives
- ☐ Baselines

Question 291

Which of the following will BEST protect confidential data when connecting large wireless networks to an existing wired-network infrastructure?

- ☒ Mandatory access control (MAC) address filtering
- ☐ Strong passwords
- ☐ Virtual private network (VPN)
- ☐ Firewall

Question 292

Which of the following attacks is BEST mitigated by utilizing strong passwords?

- ☐ Man-in-the-middle attack
- ☒ Brute force attack
- ☐ Remote buffer overflow
- ☐ Root kit

Explanation:

Explanation:

A brute force attack is normally successful against weak passwords, whereas strong passwords would not prevent any of the other attacks. Man-in-the-middle attacks intercept network traffic, which could contain passwords, but is not naturally password-protected. Remote buffer overflows rarely require a password to exploit a remote host. Root kits hook into the operating system's kernel and, therefore, operate underneath any authentication mechanism.

Question 293

The PRIMARY consideration when defining recovery time objectives (RTOs) for information assets is:

- ☐ regulatory' requirements.
- ☒ business requirements.
- ☐ financial value.
- ☐ IT resource availability.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

The criticality to business should always drive the decision. Regulatory requirements could be more flexible than business needs. The financial value of an asset could not correspond to its business value. While a consideration, IT resource availability is not a primary factor.

Question 294

What is the MOST effective access control method to prevent users from sharing files with unauthorized users?

- ☒ Mandatory
- ☐ Discretionary
- ☐ Walled garden
- ☐ Role-based

Explanation:

Explanation:

Mandatory access controls restrict access to files based on the security classification of the file. This prevents users from sharing files with unauthorized users. Role-based access controls grant access according to the role assigned to a user; they do not prohibit file sharing. Discretionary and lattice-based access controls are not as effective as mandatory access controls in preventing file sharing. A walled garden is an environment that controls a user's access to web content and services. In effect, the walled garden directs the user's navigation within particular areas, and does not necessarily prevent sharing of other material.

Question 295

The MAIN goal of an information security strategic plan is to:

- ☐ develop a risk assessment plan.
- ☐ develop a data protection plan.
- ☒ protect information assets and resources.
- ☐ establish security governance.

Explanation:

Explanation:

The main goal of an information security strategic plan is to protect information assets and resources. Developing a risk assessment plan and H data protection plan, and establishing security governance refer to tools utilized in the security strategic plan that achieve the protection of information assets and resources.

Licensed to Berend Post berend.post@it-university.nl

Question 296

An intranet server should generally be placed on the:

- ☒ internal network.
- ☐ firewall server.
- ☐ external router.
- ☐ primary domain controller.

Explanation:

Explanation:

An intranet server should be placed on the internal network. Placing it on an external router leaves it defenseless. Since firewalls should be installed on hardened servers with minimal services enabled, it is inappropriate to store the intranet server on the same physical device as the firewall. Similarly, primary- domain controllers do not normally share the physical device as the intranet server.

Question 297

Which of the following security activities should be implemented in the change management process to identify key vulnerabilities introduced by changes?

- ☐ Business impact analysis (BIA)
- ☒ Penetration testing
- ☐ Audit and review
- ☐ Threat analysis

Explanation:

Explanation:

Penetration testing focuses on identifying vulnerabilities. None of the other choices would identify vulnerabilities introduced by changes.

Question 298

Which of the following threats is prevented by using token-based authentication?

- ☒ Password sniffing attack on the network
- ☐ Denial of service attack over the network
- ☐ Main-in-the middle attack on the client
- ☐ Session eavesdropping attack on the network

Licensed to Berend Post berend.post@it-university.nl

Question 299

An internal review of a web-based application system finds the ability to gain access to all employees' accounts by changing the employee's ID on the URL used for accessing the account. The vulnerability identified is:

- ☒ broken authentication.
- ☐ unvalidated input.
- ☐ cross-site scripting.
- ☐ structured query language (SQL) injection.

Explanation:

Explanation:

The authentication process is broken because, although the session is valid, the application should reauthenticate when the input parameters are changed. The review provided valid employee IDs, and valid input was processed. The problem here is the lack of reauthentication when the input parameters are changed. Cross-site scripting is not the problem in this case since the attack is not transferred to any other user's browser to obtain the output. Structured query language (SQL) injection is not a problem since input is provided as a valid employee ID and no SQL queries are injected to provide the output.

Question 300

Which of the following documents would be the BEST reference to determine whether access control mechanisms are appropriate for a critical application?

- ☐ User security procedures
- ☐ Business process flow
- ☒ IT security policy
- ☐ Regulatory requirements

Explanation:

Explanation:

IT management should ensure that mechanisms are implemented in line with IT security policy. Procedures are determined by the policy. A user security procedure does not describe the access control mechanism in place. The business process flow is not relevant to the access control mechanism. The organization's own policy and procedures should take into account regulatory requirements.

Licensed to Berend Post berend.post@it-university.nl

Question 301

What is the MOST important element to include when developing user security awareness material?

- ☐ Information regarding social engineering
- ☐ Detailed security policies
- ☐ Senior management endorsement
- ☒ Easy-to-read and compelling information

Explanation:

Explanation:

Making security awareness material easy and compelling to read is the most important success factor. Users must be able to understand, in easy terms, complex security concepts in a way that makes compliance more accessible. Choice A would also be important but it needs to be presented in an adequate format. Detailed security policies might not necessarily be included in the training materials. Senior management endorsement is important for the security program as a whole and not necessarily for the awareness training material.

Question 302

A risk management program would be expected to:

- ☐ remove all inherent risk.
- ☒ maintain residual risk at an acceptable level.
- ☐ implement preventive controls for every threat.
- ☐ reduce control risk to zero.

Explanation:

Explanation:

The object of risk management is to ensure that all residual risk is maintained at a level acceptable to the business; it is not intended to remove every identified risk or implement controls for every threat since this may not be cost-effective. Control risk, i.e., that a control may not be effective, is a component of the program but is unlikely to be reduced to zero.

Question 303

When performing a risk assessment, the MOST important consideration is that:

- ☐ management supports risk mitigation efforts.
- ☐ annual loss expectations (ALEs) have been calculated for critical assets.
- ☒ assets have been identified and appropriately valued.
- ☐ attack motives, means and opportunities be understood.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Identification and valuation of assets provides the basis for risk management efforts as it relates to the criticality and sensitivity of assets. Management support is always important, but is not relevant when determining the proportionality of risk management efforts. ALE calculations are only valid if assets have first been identified and appropriately valued. Motives, means and opportunities should already be factored in as a part of a risk assessment.

Question 304

Which of the following devices should be placed within a DMZ?

- ☐ Proxy server
- ☒ Application server
- ☐ Departmental server
- ☐ Data warehouse server

Explanation:

Explanation:

An application server should normally be placed within a demilitarized zone (DMZ) to shield the internal network. Data warehouse and departmental servers may contain confidential or valuable data and should always be placed on the internal network, never on a DMZ that is subject to compromise. A proxy server forms the inner boundary of the DMZ but is not placed within it.

Question 305

An organization has a process in place that involves the use of a vendor. A risk assessment was completed during the development of the process. A year after the implementation a monetary decision has been made to use a different vendor. What, if anything, should occur?

- ☐ Nothing, since a risk assessment was completed during development.
- ☐ A vulnerability assessment should be conducted.
- ☒ A new risk assessment should be performed.
- ☐ The new vendor's SAS 70 type II report should be reviewed.

Explanation:

Explanation:

The risk assessment process is continual and any changes to an established process should include a new- risk assessment. While a review of the SAS 70 report and a vulnerability assessment may be components of a risk assessment, neither would constitute sufficient due diligence on its own.

Licensed to Berend Post berend.post@it-university.nl

Question 306

Which of the following is generally used to ensure that information transmitted over the Internet is authentic and actually transmitted by the named sender?

- ☐ Biometric authentication
- ☐ Embedded steganographic
- ☐ Two-factor authentication
- ☒ Embedded digital signature

Explanation:

Explanation:

Digital signatures ensure that transmitted information can be attributed to the named sender; this provides nonrepudiation. Steganographic techniques are used to hide messages or data within other files. Biometric and two-factor authentication is not generally used to protect internet data transmissions.

Question 307

Which of the following is the MOST effective method of determining security priorities?

- ☒ Impact analysis
- ☐ Threat assessment
- ☐ Vulnerability assessment
- ☐ Gap analysis

Question 308

When supporting an organization's privacy officer, which of the following is the information security manager's PRIMARY role regarding primacy requirements?

- ☐ Monitoring the transfer of private data
- ☐ Conducting privacy awareness programs
- ☒ Ensuring appropriate controls are in place
- ☐ Determining data classification

Licensed to Berend Post berend.post@it-university.nl

Question 309

A new regulation has been announced that requires mandatory reporting of security incidents that affect personal client information. Which of the following should be the information security manager's FIRST course of action?

- ☒ Review the current security policy.
- ☐ Inform senior management of the new regulation.
- ☐ Update the security incident management process.
- ☐ Determine impact to the business.

Question 310

A common concern with poorly written web applications is that they can allow an attacker to:

- ☐ gain control through a buffer overflow.
- ☐ conduct a distributed denial of service (DoS) attack.
- ☐ abuse a race condition.
- ☒ inject structured query language (SQL) statements.

Explanation:

Explanation:

Structured query language (SQL) injection is one of the most common and dangerous web application vulnerabilities. Buffer overflows and race conditions are very difficult to find and exploit on web applications. Distributed denial of service (DoS) attacks have nothing to do with the quality of a web application.

Question 311

What mechanisms are used to identify deficiencies that would provide attackers with an opportunity to compromise a computer system?

- ☐ Business impact analyses
- ☒ Security gap analyses
- ☐ System performance metrics
- ☐ Incident response processes

Explanation:

Explanation:

A security gap analysis is a process which measures all security controls in place against typically good business practice, and identifies related weaknesses. A business impact analysis is less suited to identify security deficiencies. System performance metrics may indicate security weaknesses, but that is not their primary purpose. Incident response processes exist for cases where security weaknesses are exploited.

Licensed to Berend Post berend.post@it-university.nl

Question 312

The MOST effective way to ensure that outsourced service providers comply with the organization's information security policy would be:

- ☐ service level monitoring.
- ☐ penetration testing.
- ☒ periodically auditing.
- ☐ security awareness training.

Explanation:

Explanation:

Regular audit exercise can spot any gap in the information security compliance. Service level monitoring can only pinpoint operational issues in the organization's operational environment. Penetration testing can identify security vulnerability but cannot ensure information compliance Training can increase users' awareness on the information security policy, but is not more effective than auditing.

Question 313

An organization to integrate information security into its human resource management processes. Which of the following should be the FIRST step?

- ☐ Evaluate the cost of information security integration
- ☒ Assess the business objectives of the processes
- ☐ Identify information security risk associated with the processes
- ☐ Benchmark the processes with best practice to identify gaps

Question 314

Information security awareness programs are MOST effective when they are:

- ☒ customized for each target audience.
- ☐ sponsored by senior management.
- ☐ reinforced by computer-based training.
- ☐ conducted at employee orientation

Licensed to Berend Post berend.post@it-university.nl

Question 315

The PRIMARY objective of a security steering group is to:

- ☐ ensure information security covers all business functions.
- ☒ ensure information security aligns with business goals.
- ☐ raise information security awareness across the organization.
- ☐ implement all decisions on security management across the organization.

Explanation:

Explanation:

The security steering group comprises senior management of key business functions and has the primary objective to align the security strategy with the business direction. Option A is incorrect because all business areas may not be required to be covered by information security; but, if they do, the main purpose of the steering committee would be alignment more so than coverage. While raising awareness is important, this goal would not be carried out by the committee itself. The steering committee may delegate part of the decision making to the information security manager; however, if it retains this authority, it is not the primary' goal.

Question 316

What would a security manager PRIMARILY utilize when proposing the implementation of a security solution?

- ☐ Risk assessment report
- ☐ Technical evaluation report
- ☒ Business case
- ☐ Budgetary requirements

Explanation:

Explanation:

The information security manager needs to prioritize the controls based on risk management and the requirements of the organization. The information security manager must look at the costs of the various controls and compare them against the benefit the organization will receive from the security solution. The information security manager needs to have knowledge of the development of business cases to illustrate the costs and benefits of the various controls. All other choices are supplemental.

Licensed to Berend Post berend.post@it-university.nl

Question 317

Which of the following is the MOST important reason for performing vulnerability assessments periodically?

- ☐ Management requires regular reports.
- ☒ The environment changes constantly.
- ☐ Technology risks must be mitigated.
- ☐ The current threat levels are being assessed.

Question 318

When a newly installed system for synchronizing passwords across multiple systems and platforms abnormally terminates without warning, which of the following should automatically occur FIRST?

- ☐ The firewall should block all inbound traffic during the outage
- ☐ All systems should block new logins until the problem is corrected
- ☒ Access control should fall back to no synchronized mode
- ☐ System logs should record all user activity for later analysis

Explanation:

Explanation:

The best mechanism is for the system to fallback to the original process of logging on individually to each system. Blocking traffic and new logins would be overly restrictive to the conduct of business, while recording all user activity would add little value.

Question 319

An organization has decided to implement additional security controls to treat the risks of a new process. This is an example of:

- ☐ eliminating the risk.
- ☐ transferring the risk.
- ☒ mitigating the risk.
- ☐ accepting the risk.

Explanation:

Explanation:

Risk can never be eliminated entirely. Transferring the risk gives it away such as buying insurance so the insurance company can take the risk. Implementing additional controls is an example of mitigating risk. Doing nothing to mitigate the risk would be an example of accepting risk.

Licensed to Berend Post berend.post@it-university.nl

Question 320

Which of the following risks is represented in the risk appetite of an organization?

- ☐ Control
- ☐ Inherent
- ☒ Residual
- ☐ Audit

Explanation:

Explanation:

Residual risk is unmanaged, i.e., inherent risk which remains uncontrolled. This is key to the organization's risk appetite and is the amount of residual risk that a business is living with that affects its viability. Hence, inherent risk is incorrect. Control risk, the potential for controls to fail, and audit risk, which relates only to audit's approach to their work, are not relevant in this context.

Question 321

In order to protect a network against unauthorized external connections to corporate systems, the information security manager should BEST implement:

- ☒ a strong authentication.
- ☐ IP antispoofing filtering.
- ☐ network encryption protocol.
- ☐ access lists of trusted devices.

Explanation:

Explanation:

Strong authentication will provide adequate assurance on the identity of the users, while IP antispoofing is aimed at the device rather than the user. Encryption protocol ensures data confidentiality and authenticity while access lists of trusted devices are easily exploited by spoofed identity of the clients.

Question 322

Which of the following tools is MOST appropriate for determining how long a security project will take to implement?

- ☐ Gantt chart
- ☐ Waterfall chart
- ☒ Critical path
- ☐ Rapid Application Development (RAD)

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

The critical path method is most effective for determining how long a project will take. A waterfall chart is used to understand the flow of one process into another. A Gantt chart facilitates the proper estimation and allocation of resources. The Rapid Application Development (RAD) method is used as an aid to facilitate and expedite systems development.

Question 323

What is the GREATEST risk when there is an excessive number of firewall rules?

- ☒ One rule may override another rule in the chain and create a loophole
- ☐ Performance degradation of the whole network
- ☐ The firewall may not support the increasing number of rules due to limitations
- ☐ The firewall may show abnormal behavior and may crash or automatically shut down

Explanation:

Explanation:

If there are many firewall rules, there is a chance that a particular rule may allow an external connection although other associated rules are overridden. Due to the increasing number of rules, it becomes complex to test them and. over time, a loophole may occur.

Question 324

The MOST important reason that statistical anomaly-based intrusion detection systems (slat IDSs) are less commonly used than signature-based IDSs, is that stat IDSs:

- ☐ create more overhead than signature-based IDSs.
- ☐ cause false positives from minor changes to system variables.
- ☒ generate false alarms from varying user or system actions.
- ☐ cannot detect new types of attacks.

Explanation:

Explanation:

A statistical anomaly-based intrusion detection system (stat IDS) collects data from normal traffic and establishes a baseline. It then periodically samples the network activity based on statistical methods and compares samples to the baseline. When the activity is outside the baseline parameter (clipping level), the IDS notifies the administrator. The baseline variables can include a host's memory or central processing unit (CPU) usage, network packet types and packet quantities. If actions of the users or the systems on the network vary widely with periods of low activity and periods of frantic packet exchange, a stat IDS may not be suitable, as the dramatic swing from one level to another almost certainly will generate false alarms. This weakness will have the largest impact on the

 Licensed to Berend Post berend.post@it-university.nl

operation of the IT systems. Due to the nature of stat IDS operations (i.e., they must constantly attempt to match patterns of activity to the baseline parameters), a stat IDS requires much more overhead and processing than signature-based versions. Due to the nature of a stat IDS — based on statistics and comparing data with baseline parameters — this type of IDS may not detect minor changes to system variables and may generate many false positives. Choice D is incorrect; since the stat IDS can monitor multiple system variables, it can detect new types of variables by tracing for abnormal activity of any kind.

Question 325

An information security manager has completed a risk assessment and has determined the residual risk. Which of the following should be the NEXT step?

- ☐ Conduct an evaluation of controls
- ☒ Determine if the risk is within the risk appetite
- ☐ Implement countermeasures to mitigate risk
- ☐ Classify all identified risks

Question 326

Which of the following is a key area of the ISO 27001 framework?

- ☐ Operational risk assessment
- ☐ Financial crime metrics
- ☐ Capacity management
- ☒ Business continuity management

Explanation:

Explanation:

Operational risk assessment, financial crime metrics and capacity management can complement the information security framework, but only business continuity management is a key component.

Question 327

During which phase of development is it MOST appropriate to begin assessing the risk of a new application system?

- ☒ Feasibility
- ☐ Design
- ☐ Development
- ☐ Testing

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Risk should be addressed as early in the development of a new application system as possible. In some cases, identified risks could be mitigated through design changes. If needed changes are not identified until design has already commenced, such changes become more expensive. For this reason, beginning risk assessment during the design, development or testing phases is not the best solution.

Question 328

The MOST effective use of a risk register is to:

- ☐ identify risks and assign roles and responsibilities for mitigation.
- ☐ identify threats and probabilities.
- ☒ facilitate a thorough review of all IT-related risks on a periodic basis.
- ☐ record the annualized financial amount of expected losses due to risks.

Explanation:

Explanation:

A risk register is more than a simple list — it should lie used as a tool to ensure comprehensive documentation, periodic review and formal update of all risk elements in the enterprise's IT and related organization. Identifying risks and assigning roles and responsibilities for mitigation are elements of the register. Identifying threats and probabilities are two elements that are defined in the risk matrix, as differentiated from the broader scope of content in, and purpose for, the risk register. While the annualized loss expectancy (ALE) should be included in the register, this quantification is only a single element in the overall risk analysis program.

Question 329

A newly hired information security manager reviewing an existing security investment plan is MOST likely to be concerned when the plan:

- ☒ is based solely on a review of security threats and vulnerabilities in existing IT systems
- ☐ identifies potential impacts that the implementation may have on business processes
- ☐ focuses on compliance with common international security standards
- ☐ has summarized IT costs for implementation rather than providing detail

Licensed to Berend Post berend.post@it-university.nl

Question 330

In the course of responding 10 an information security incident, the BEST way to treat evidence for possible legal action is defined by:

- ☐ international standards.
- ☒ local regulations.
- ☐ generally accepted best practices.
- ☐ organizational security policies.

Explanation:

Explanation:

Legal follow-up will most likely be performed locally where the incident took place; therefore, it is critical that the procedure of treating evidence is in compliance with local regulations. In certain countries, there are strict regulations on what information can be collected. When evidence collected is not in compliance with local regulations, it may not be admissible in court. There are no common regulations to treat computer evidence that are accepted internationally. Generally accepted best practices such as a common chain-of-custody concept may have different implementation in different countries, and thus may not be a good assurance that evidence will be admissible. Local regulations always take precedence over organizational security policies.

Question 331

Which of the following is the MOST effective way to treat a risk such as a natural disaster that has a low probability and a high impact level?

- ☐ Implement countermeasures.
- ☐ Eliminate the risk.
- ☒ Transfer the risk.
- ☐ Accept the risk.

Explanation:

Explanation:

Risks are typically transferred to insurance companies when the probability of an incident is low but the impact is high. Examples include: hurricanes, tornados and earthquakes. Implementing countermeasures may not be the most cost-effective approach to security management. Eliminating the risk may not be possible. Accepting the risk would leave the organization vulnerable to a catastrophic disaster which may cripple or ruin the organization. It would be more cost effective to pay recurring insurance costs than to be affected by a disaster from which the organization cannot financially recover.

Licensed to Berend Post berend.post@it-university.nl

Question 332

The PRIMARY concern of an information security manager documenting a formal data retention policy would be:

- ☐ generally accepted industry best practices.
- ☒ business requirements.
- ☐ legislative and regulatory requirements.
- ☐ storage availability.

Explanation:

Explanation:

The primary concern will be to comply with legislation and regulation but only if this is a genuine business requirement. Best practices may be a useful guide but not a primary concern. Legislative and regulatory requirements are only relevant if compliance is a business need. Storage is irrelevant since whatever is needed must be provided

Question 333

How would an information security manager balance the potentially conflicting requirements of an international organization's security standards and local regulation?

- ☐ Give organization standards preference over local regulations
- ☐ Follow local regulations only
- ☐ Make the organization aware of those standards where local regulations causes conflicts
- ☒ Negotiate a local version of the organization standards

Explanation:

Explanation:

Adherence to local regulations must always be the priority. Not following local regulations can prove detrimental to the group organization. Following local regulations only is incorrect since there needs to be some recognition of organization requirements. Making an organization aware of standards is a sensible step, but is not a total solution. Negotiating a local version of the organization standards is the most effective compromise in this situation.

Licensed to Berend Post berend.post@it-university.nl

Question 334

Which of the following is an inherent weakness of signature-based intrusion detection systems?

- ☐ A higher number of false positives
- ☒ New attack methods will be missed
- ☐ Long duration probing will be missed
- ☐ Attack profiles can be easily spoofed

Explanation:

Explanation:

Signature-based intrusion detection systems do not detect new attack methods for which signatures have not yet been developed. False positives are not necessarily any higher, and spoofing is not relevant in this case. Long duration probing is more likely to fool anomaly-based systems (boiling frog technique).

Question 335

Most security vulnerabilities in software exit because:

- ☐ security features are not tested adequately.
- ☐ software has undocumented features.
- ☐ security is not properly designed.
- ☒ software is developed without adherence to standards.

Question 336

When performing a qualitative risk analysis, which of the following will BEST produce reliable results?

- ☐ Estimated productivity losses
- ☒ Possible scenarios with threats and impacts
- ☐ Value of information assets
- ☐ Vulnerability assessment

Explanation:

Explanation:

Listing all possible scenarios that could occur, along with threats and impacts, will better frame the range of risks and facilitate a more informed discussion and decision. Estimated productivity losses, value of information assets and vulnerability assessments would not be sufficient on their own.

Licensed to Berend Post berend.post@it-university.nl

Question 337

An information security strategy document that includes specific links to an organization's business activities is PRIMARILY an indicator of:

- ☐ performance measurement.
- ☐ integration.
- ☒ alignment.
- ☐ value delivery.

Explanation:

Explanation:

Strategic alignment of security with business objectives is a key indicator of performance measurement. In guiding a security program, a meaningful performance measurement will also rely on an understanding of business objectives, which will be an outcome of alignment. Business linkages do not by themselves indicate integration or value delivery. While alignment is an important precondition, it is not as important an indicator.

Question 338

The MAIN advantage of implementing automated password synchronization is that it:

- ☒ reduces overall administrative workload.
- ☐ increases security between multi-tier systems.
- ☐ allows passwords to be changed less frequently.
- ☐ reduces the need for two-factor authentication.

Explanation:

Explanation:

Automated password synchronization reduces the overall administrative workload of resetting passwords. It does not increase security between multi-tier systems, allow passwords to be changed less frequently or reduce the need for two-factor authentication.

Question 339

Who in an organization has the responsibility for classifying information?

- ☐ Data custodian
- ☐ Database administrator
- ☐ Information security officer
- ☒ Data owner

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The data owner has full responsibility over data. The data custodian is responsible for securing the information. The database administrator carries out the technical administration. The information security officer oversees the overall classification management of the information.

Question 340

Which of the following ensures that newly identified security weaknesses in an operating system are mitigated in a timely fashion?

- ☒ Patch management
- ☐ Change management
- ☐ Security baselines
- ☐ Acquisition management

Explanation:

Explanation:

Patch management involves the correction of software weaknesses and helps ensure that newly identified exploits are mitigated in a timely fashion. Change management controls the process of introducing changes to systems. Security baselines provide minimum recommended settings. Acquisition management controls the purchasing process.

Question 341

The MOST basic requirement for an information security governance program is to:

- ☒ be aligned with the corporate business strategy.
- ☐ be based on a sound risk management approach.
- ☐ provide adequate regulatory compliance.
- ☐ provide best practices for security- initiatives.

Explanation:

Explanation:

To receive senior management support, an information security program should be aligned with the corporate business strategy. Risk management is a requirement of an information security program which should take into consideration the business strategy. Security governance is much broader than just regulatory compliance. Best practice is an operational concern and does not have a direct impact on a governance program.

Licensed to Berend Post berend.post@it-university.nl

Question 342

An information security manager reviewed the access control lists and observed that privileged access was granted to an entire department. Which of the following should the information security manager do FIRST?

- ☐ Review the procedures for granting access
- ☐ Establish procedures for granting emergency access
- ☒ Meet with data owners to understand business needs
- ☐ Redefine and implement proper access rights

Explanation:

Explanation:

An information security manager must understand the business needs that motivated the change prior to taking any unilateral action. Following this, all other choices could be correct depending on the priorities set by the business unit.

Question 343

A good privacy statement should include:

- ☐ notification of liability on accuracy of information.
- ☐ notification that information will be encrypted.
- ☒ what the company will do with information it collects.
- ☐ a description of the information classification process.

Explanation:

Explanation:

Most privacy laws and regulations require disclosure on how information will be used. Choice A is incorrect because that information should be located in the web site's disclaimer. Choice B is incorrect because, although encryption may be applied, this is not generally disclosed. Choice D is incorrect because information classification would be contained in a separate policy.

Question 344

Which of the following practices completely prevents a man-in-the-middle (MitM) attack between two hosts?

- ☐ Use security tokens for authentication
- ☒ Connect through an IPSec VPN
- ☐ Use https with a server-side certificate
- ☐ Enforce static media access control (MAC) addresses

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

IPSec effectively prevents man-in-the-middle (MitM) attacks by including source and destination IPs within the encrypted portion of the packet. The protocol is resilient to MitM attacks. Using token-based authentication does not prevent a MitM attack; however, it may help eliminate reusability of stolen cleartext credentials. An https session can be intercepted through Domain Name Server (DNS) or Address Resolution Protocol (ARP) poisoning. ARP poisoning — a specific kind of MitM attack — may be prevented by setting static media access control (MAC) addresses. Nevertheless, DNS and NetBIOS resolution can still be attacked to deviate traffic.

Question 345

The information classification scheme should:

- ☒ consider possible impact of a security breach.
- ☐ classify personal information in electronic form.
- ☐ be performed by the information security manager.
- ☐ classify systems according to the data processed.

Explanation:

Explanation:

Data classification is determined by the business risk, i.e., the potential impact on the business of the loss, corruption or disclosure of information. It must be applied to information in all forms, both electronic and physical (paper), and should be applied by the data owner, not the security manager. Choice B is an incomplete answer because it addresses only privacy issues, while choice A is a more complete response. Data classification is determined by the business risk, i.e., the potential impact on the business of the loss, corruption or disclosure of information. It must be applied to information in all forms, both electronic and physical (paper), and should be applied by the data owner, not the security manager.

Question 346

The IT function has declared that, when putting a new application into production, it is not necessary to update the business impact analysis (BIA) because it does not produce modifications in the business processes. The information security manager should:

- ☒ verify the decision with the business units.
- ☐ check the system's risk analysis.
- ☐ recommend update after post implementation review.
- ☐ request an audit review.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Verifying the decision with the business units is the correct answer because it is not the IT function's responsibility to decide whether a new application modifies business processes Choice B does not consider the change in the applications. Choices C and D delay the update.

Question 347

In business critical applications, where shared access to elevated privileges by a small group is necessary, the BEST approach to implement adequate segregation of duties is to:

- ☐ ensure access to individual functions can be granted to individual users only.
- ☒ implement role-based access control in the application.
- ☐ enforce manual procedures ensuring separation of conflicting duties.
- ☐ create service accounts that can only be used by authorized team members.

Explanation:

Explanation:

Role-based access control is the best way to implement appropriate segregation of duties. Roles will have to be defined once and then the user could be changed from one role to another without redefining the content of the role each time. Access to individual functions will not ensure appropriate segregation of duties. Giving a user access to all functions and implementing, in parallel, a manual procedure ensuring segregation of duties is not an effective method, and would be difficult to enforce and monitor. Creating service accounts that can be used by authorized team members would not provide any help unless their roles are properly segregated.

Question 348

Who is responsible for raising awareness of the need for adequate funding for risk action plans?

- ☐ Chief information officer (CIO)
- ☐ Chief financial officer (CFO)
- ☒ Information security manager
- ☐ Business unit management

Explanation:

Explanation:

The information security manager is responsible for raising awareness of the need for adequate funding for risk-related action plans. Even though the chief information officer (CIO), chief financial officer (CFO) and business unit management are involved in the final approval of fund expenditure, it is the information security manager who has the ultimate responsibility for raising awareness.

Licensed to Berend Post berend.post@it-university.nl

Question 349

Which of the following is MOST important for a successful information security program?

- ☐ Adequate training on emerging security technologies
- ☐ Open communication with key process owners
- ☐ Adequate policies, standards and procedures
- ☒ Executive management commitment

Explanation:

Explanation:

Sufficient executive management support is the most important factor for the success of an information security program. Open communication, adequate training, and good policies and procedures, while important, are not as important as support from top management; they will not ensure success if senior management support is not present.

Question 350

The configuration management plan should PRIMARILY be based upon input from:

- ☐ business process owners.
- ☐ the information security manager.
- ☐ the security steering committee.
- ☒ IT senior management.

Explanation:

Explanation:

Although business process owners, an information security manager and the security steering committee may provide input regarding a configuration management plan, its final approval is the primary responsibility of IT senior management.

Question 351

The service level agreement (SLA) for an outsourced IT function does not reflect an adequate level of protection. In this situation an information security manager should:

- ☐ ensure the provider is made liable for losses.
- ☐ recommend not renewing the contract upon expiration.
- ☐ recommend the immediate termination of the contract.
- ☒ determine the current level of security.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

It is important to ensure that adequate levels of protection are written into service level agreements (SLAs) and other outsourcing contracts. Information must be obtained from providers to determine how that outsource provider is securing information assets prior to making any recommendation or taking any action in order to support management decision making. Choice A is not acceptable in most situations and therefore not a good answer.

Question 352

Which of the following factors is a PRIMARY driver for information security governance that does not require any further justification?

- ☐ Alignment with industry best practices
- ☐ Business continuity investment
- ☐ Business benefits
- ☒ Regulatory compliance

Explanation:

Explanation:

Regulatory compliance can be a standalone driver for an information security governance measure. No further analysis nor justification is required since the entity has no choice in the regulatory requirements. Buy-in from business managers must be obtained by the information security manager when an information security governance measure is sought based on its alignment with industry best practices. Business continuity investment needs to be justified by business impact analysis. When an information security governance measure is sought based on qualitative business benefits, further analysis is required to determine whether the benefits outweigh the cost of the information security governance measure in question.

Question 353

It is important to develop an information security baseline because it helps to define:

- ☐ critical information resources needing protection.
- ☐ a security policy for the entire organization.
- ☒ the minimum acceptable security to be implemented.
- ☐ required physical and logical access controls.

Explanation:

Explanation:

Developing an information security baseline helps to define the minimum acceptable security that will be implemented to protect the information resources in accordance with the respective criticality levels. Before determining the security baseline, an information security manager must establish the security policy, identify criticality levels of organization's information resources and assess the risk environment in which those resources operate.

Licensed to Berend Post berend.post@it-university.nl

Question 354

Data owners are PRIMARILY responsible for establishing risk mitigation methods to address which of the following areas?

- ☐ Platform security
- ☒ Entitlement changes
- ☐ Intrusion detection
- ☐ Antivirus controls

Explanation:

Explanation:

Data owners are responsible for assigning user entitlements and approving access to the systems for which they are responsible. Platform security, intrusion detection and antivirus controls are all within the responsibility of the information security manager.

Question 355

An information security manager wishing to establish security baselines would:

- ☐ include appropriate measurements in the system development life cycle.
- ☒ implement the security baselines to establish information security best practices.
- ☐ implement the security baselines to fulfill laws and applicable regulations in different jurisdictions.
- ☐ leverage information security as a competitive advantage.

Explanation:

Explanation:

While including appropriate measurements in the system development life cycle may indicate a security baseline practice; these are wider in scope and, thus, implementing security baselines to establish information security best practices is the appropriate answer. Implementing security baselines to fulfill laws and applicable regulations in different jurisdictions, and leveraging information security as a competitive advantage may be supplementary benefits of using security baselines.

Licensed to Berend Post berend.post@it-university.nl

Question 356

A successful risk management program should lead to:

- ☒ optimization of risk reduction efforts against cost.
- ☐ containment of losses to an annual budgeted amount.
- ☐ identification and removal of all man-made threats.
- ☐ elimination or transference of all organizational risks.

Explanation:

Explanation:

Successful risk management should lead to a breakeven point of risk reduction and cost. The other options listed are not achievable. Threats cannot be totally removed or transferred, while losses cannot be budgeted in advance with absolute certainty.

Question 357

When configuring a biometric access control system that protects a high-security data center, the system's sensitivity level should be set:

- ☒ to a higher false reject rate (FRR).
- ☐ to a lower crossover error rate.
- ☐ to a higher false acceptance rate (FAR).
- ☐ exactly to the crossover error rate.

Explanation:

Explanation:

Biometric access control systems are not infallible. When tuning the solution, one has to adjust the sensitivity level to give preference either to false reject rate (type I error rate) where the system will be more prone to err denying access to a valid user or erring and allowing access to an invalid user. As the sensitivity of the biometric system is adjusted, these values change inversely. At one point, the two values intersect and are equal. This condition creates the crossover error rate, which is a measure of the system accuracy. In systems where the possibility of false rejects is a problem, it may be necessary' to reduce sensitivity and thereby increase the number of false accepts. This is sometimes referred to as equal error rate (EER). In a very sensitive system, it may be desirable to minimize the number of false accepts — the number of unauthorized persons allowed access. To do this, the system is tuned to be more sensitive, which causes the false rejects the number of authorized persons disallowed access to increase.

Licensed to Berend Post berend.post@it-university.nl

Question 358

A risk assessment study carried out by an organization noted that there is no segmentation of the local area network (LAN). Network segmentation would reduce the potential impact of which of the following?

- ☐ Denial of service (DoS) attacks
- ☒ Traffic sniffing
- ☐ Virus infections
- ☐ IP address spoofing

Explanation:

Explanation:

Network segmentation reduces the impact of traffic sniffing by limiting the amount of traffic that may be visible on any one network segment. Network segmentation would not mitigate the risk posed by denial of service (DoS) attacks, virus infections or IP address spoofing since each of these would be able to traverse network segments.

Question 359

An information security manager must understand the relationship between information security and business operations in order to:

- ☒ support organizational objectives.
- ☐ determine likely areas of noncompliance.
- ☐ assess the possible impacts of compromise.
- ☐ understand the threats to the business.

Explanation:

Explanation:

Security exists to provide a level of predictability for operations, support for the activities of the organization and to ensure preservation of the organization. Business operations must be the driver for security activities in order to set meaningful objectives, determine and manage the risks to those activities, and provide a basis to measure the effectiveness of and provide guidance to the security program. Regulatory compliance may or may not be an organizational requirement. If compliance is a requirement, some level of compliance must be supported but compliance is only one aspect. It is necessary to understand the business goals in order to assess potential impacts and evaluate threats. These are some of the ways in which security supports organizational objectives, but they are not the only ways.

Licensed to Berend Post berend.post@it-university.nl

Question 360

Which of the following situations would MOST inhibit the effective implementation of security governance?

- ☐ The complexity of technology
- ☐ Budgetary constraints
- ☐ Conflicting business priorities
- ☒ High-level sponsorship

Explanation:

Explanation:

The need for senior management involvement and support is a key success factor for the implementation of appropriate security governance. Complexity of technology, budgetary constraints and conflicting business priorities are realities that should be factored into the governance model of the organization, and should not be regarded as inhibitors.

Question 361

Which of the following are the MOST important individuals to include as members of an information security steering committee?

- ☐ Direct reports to the chief information officer
- ☒ IT management and key business process owners
- ☐ Cross-section of end users and IT professionals
- ☐ Internal audit and corporate legal departments

Explanation:

Explanation:

Security steering committees provide a forum for management to express its opinion and take some ownership in the decision making process. It is imperative that business process owners be included in this process. None of the other choices includes input by business process owners.

Question 362

Which of the following steps in conducting a risk assessment should be performed FIRST?

- ☒ Identity business assets
- ☐ Identify business risks
- ☐ Assess vulnerabilities
- ☐ Evaluate key controls

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Risk assessment first requires one to identify the business assets that need to be protected before identifying the threats. The next step is to establish whether those threats represent business risk by identifying the likelihood and effect of occurrence, followed by assessing the vulnerabilities that may affect the security of the asset. This process establishes the control objectives against which key controls can be evaluated.

Question 363

The MOST effective approach to address issues that arise between IT management, business units and security management when implementing a new security strategy is for the information security manager to:

- ☐ escalate issues to an external third party for resolution.
- ☐ ensure that senior management provides authority for security to address the issues.
- ☐ insist that managers or units not in agreement with the security solution accept the risk.
- ☒ refer the issues to senior management along with any security recommendations.

Explanation:

Explanation:

Senior management is in the best position to arbitrate since they will look at the overall needs of the business in reaching a decision. The authority may be delegated to others by senior management after their review of the issues and security recommendations. Units should not be asked to accept the risk without first receiving input from senior management.

Question 364

What does a network vulnerability assessment intend to identify?

- ☐ 0-day vulnerabilities
- ☐ Malicious software and spyware
- ☐ Security design flaws
- ☒ Misconfiguration and missing updates

Explanation:

Explanation:

A network vulnerability assessment intends to identify known vulnerabilities based on common misconfigurations and missing updates. 0-day vulnerabilities by definition are not previously known and therefore are undetectable. Malicious software and spyware are normally addressed through antivirus and antispyware policies. Security design flaws require a deeper level of analysis.

Licensed to Berend Post berend.post@it-university.nl

Question 365

To prevent computers on the corporate network from being used as part of a distributed denial of service attack, the information security manager should use:

- ☐ incoming traffic filtering
- ☒ outgoing traffic filtering
- ☐ IT security policy dissemination
- ☐ rate limiting

Question 366

To reduce the possibility of service interruptions, an entity enters into contracts with multiple Internet service providers (ISPs). Which of the following would be the MOST important item to include?

- ☒ Service level agreements (SLAs)
- ☐ Right to audit clause
- ☐ Intrusion detection system (IDS) services
- ☐ Spam filtering services

Explanation:

Explanation:

Service level agreements (SLA) will be most effective in ensuring that Internet service providers (ISPs) comply with expectations for service availability. Intrusion detection system (IDS) and spam filtering services would not mitigate (as directly) the potential for service interruptions. A right-to-audit clause would not be effective in mitigating the likelihood of a service interruption.

Question 367

To determine the selection of controls required to meet business objectives, an information security manager should:

- ☐ prioritize the use of role-based access controls.
- ☒ focus on key controls.
- ☐ restrict controls to only critical applications.
- ☐ focus on automated controls.

Explanation:

Explanation:

Key controls primarily reduce risk and are most effective for the protection of information assets. The other choices could be examples of possible key controls.

Licensed to Berend Post berend.post@it-university.nl

Question 368

On a company's e-commerce web site, a good legal statement regarding data privacy should include:

- ☒ a statement regarding what the company will do with the information it collects.
- ☐ a disclaimer regarding the accuracy of information on its web site.
- ☐ technical information regarding how information is protected.
- ☐ a statement regarding where the information is being hosted.

Explanation:

Explanation:

Most privacy laws and regulations require disclosure on how information will be used. A disclaimer is not necessary since it does not refer to data privacy. Technical details regarding how information is protected are not mandatory to publish on the web site and in fact would not be desirable. It is not mandatory to say where information is being hosted.

Question 369

Which of the following has the highest priority when defining an emergency response plan?

- ☐ Critical data
- ☐ Critical infrastructure
- ☒ Safety of personnel
- ☐ Vital records

Explanation:

Explanation:

The safety of an organization's employees should be the most important consideration given human safety laws. Human safety is considered first in any process or management practice. All of the other choices are secondary.

Question 370

Which two components PRIMARILY must be assessed in an effective risk analysis?

- ☐ Visibility and duration
- ☒ Likelihood and impact
- ☐ Probability and frequency
- ☐ Financial impact and duration

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The probability or likelihood of the event and the financial impact or magnitude of the event must be assessed first. Duration refers to the length of the event; it is important in order to assess impact but is secondary. Once the likelihood is determined, the frequency is also important to determine overall impact.

Question 371

What is the MOST appropriate change management procedure for the handling of emergency program changes?

- ☐ Formal documentation does not need to be completed before the change
- ☐ Business management approval must be obtained prior to the change
- ☒ Documentation is completed with approval soon after the change
- ☐ All changes must follow the same process

Explanation:

Explanation:

Even in the case of an emergency change, all change management procedure steps should be completed as in the case of normal changes. The difference lies in the timing of certain events. With an emergency change, it is permissible to obtain certain approvals and other documentation on "the morning after" once the emergency has been satisfactorily resolved. Obtaining business approval prior to the change is ideal but not always possible.

Question 372

Documented standards/procedures for the use of cryptography across the enterprise should PRIMARILY:

- ☒ define the circumstances where cryptography should be used.
- ☐ define cryptographic algorithms and key lengths.
- ☐ describe handling procedures of cryptographic keys.
- ☐ establish the use of cryptographic solutions.

Explanation:

Explanation:

There should be documented standards-procedures for the use of cryptography across the enterprise; they should define the circumstances where cryptography should be used. They should cover the selection of cryptographic algorithms and key lengths, but not define them precisely, and they should address the handling of cryptographic keys. However, this is secondary to how and when cryptography should be used. The use of cryptographic solutions should be addressed but, again, this is a secondary consideration.

Licensed to Berend Post berend.post@it-university.nl

Question 373

Which of the following is the BEST approach to reduce unnecessary duplication of compliance activities?

- ☐ Automation of controls
- ☐ Documentation of control procedures
- ☐ Integration of assurance efforts
- ☒ Standardization of compliance requirements

Question 374

Good information security procedures should:

- ☐ define the allowable limits of behavior.
- ☐ underline the importance of security governance.
- ☐ describe security baselines for each platform.
- ☒ be updated frequently as new software is released.

Explanation:

Explanation:

Security procedures often have to change frequently to keep up with changes in software. Since a procedure is a how-to document, it must be kept up-to-date with frequent changes in software. A security standard such as platform baselines — defines behavioral limits, not the how-to process; it should not change frequently. High-level objectives of an organization, such as security governance, would normally be addressed in a security policy.

Question 375

Identification and prioritization of business risk enables project managers to:

- ☐ establish implementation milestones.
- ☐ reduce the overall amount of slack time.
- ☒ address areas with most significance.
- ☐ accelerate completion of critical paths.

Explanation:

Explanation:

Identification and prioritization of risk allows project managers to focus more attention on areas of greater importance and impact. It will not reduce the overall amount of slack time, facilitate establishing implementation milestones or allow a critical path to be completed any sooner.

Licensed to Berend Post berend.post@it-university.nl

Question 376

The MOST important success factor to design an effective IT security awareness program is to:

- ☒ customize the content to the target audience.
- ☐ ensure senior management is represented.
- ☐ ensure that all the staff is trained.
- ☐ avoid technical content but give concrete examples.

Explanation:

Explanation:

Awareness training can only be effective if it is customized to the expectations and needs of attendees. Needs will be quite different depending on the target audience and will vary between business managers, end users and IT staff; program content and the level of detail communicated will therefore be different. Other criteria are also important; however, the customization of content is the most important factor.

Question 377

Which of the following is the MOST usable deliverable of an information security risk analysis?

- ☐ Business impact analysis (BIA) report
- ☒ List of action items to mitigate risk
- ☐ Assignment of risks to process owners
- ☐ Quantification of organizational risk

Explanation:

Explanation:

Although all of these are important, the list of action items is used to reduce or transfer the current level of risk. The other options materially contribute to the way the actions are implemented.

Question 378

When an organization is setting up a relationship with a third-party IT service provider, which of the following is one of the MOST important topics to include in the contract from a security standpoint?

- ☐ Compliance with international security standards.
- ☐ Use of a two-factor authentication system.
- ☐ Existence of an alternate hot site in case of business disruption.
- ☒ Compliance with the organization's information security requirements.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Prom a security standpoint, compliance with the organization's information security requirements is one of the most important topics that should be included in the contract with third-party service provider. The scope of implemented controls in any ISO 27001-compliant organization depends on the security requirements established by each organization. Requiring compliance only with this security standard does not guarantee that a service provider complies with the organization's security requirements. The requirement to use a specific kind of control methodology is not usually stated in the contract with third- party service providers.

Question 379

When developing incident response procedures involving servers hosting critical applications, which of the following should be the FIRST to be notified?

- ☐ Business management
- ☐ Operations manager
- ☒ Information security manager
- ☐ System users

Explanation:

Explanation:

The escalation process in critical situations should involve the information security manager as the first contact so that appropriate escalation steps are invoked as necessary. Choices A, B and D would be notified accordingly.

Question 380

In an organization that has undergone an expansion through an acquisition which of the following would BEST secure the enterprise network?

- ☒ Using security groups
- ☐ Log analysis od system access
- ☐ Business or role-based segmentation
- ☐ Encryption of data traversing networks

Question 381

Good information security standards should:

- ☒ define precise and unambiguous allowable limits.
- ☐ describe the process for communicating violations.
- ☐ address high-level objectives of the organization.
- ☐ be updated frequently as new software is released.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

A security standard should clearly state what is allowable; it should not change frequently. The process for communicating violations would be addressed by a security procedure, not a standard. High-level objectives of an organization would normally be addressed in a security policy.

Question 382

In performing a risk assessment on the impact of losing a server, the value of the server should be calculated using the:

- ☐ original cost to acquire.
- ☐ cost of the software stored.
- ☐ annualized loss expectancy (ALE).
- ☒ cost to obtain a replacement.

Explanation:

Explanation:

The value of the server should be based on its cost of replacement. The original cost may be significantly different from the current cost and, therefore, not as relevant. The value of the software is not at issue because it can be restored from backup media. The ALE for all risks related to the server does not represent the server's value.

Question 383

An information security manager has been assigned to implement more restrictive preventive controls. By doing so, the net effect will be to PRIMARILY reduce the:

- ☐ threat.
- ☐ loss.
- ☒ vulnerability.
- ☐ probability.

Explanation:

Explanation:

Implementing more restrictive preventive controls mitigates vulnerabilities but not the threats. Losses and probability of occurrence may not be primarily or directly affected.

Licensed to Berend Post berend.post@it-university.nl

Question 384

The BEST protocol to ensure confidentiality of transmissions in a business-to-customer (B2C) financial web application is:

- ☒ Secure Sockets Layer (SSL).
- ☐ Secure Shell (SSH).
- ☐ IP Security (IPSec).
- ☐ Secure/Multipurpose Internet Mail Extensions (S/MIME).

Explanation:

Explanation:

Secure Sockets Layer (SSL) is a cryptographic protocol that provides secure communications providing end point authentication and communications privacy over the Internet. In typical use, all data transmitted between the customer and the business are, therefore, encrypted by the business's web server and remain confidential. SSH File Transfer Protocol (SFTP) is a network protocol that provides file transfer and manipulation functionality over any reliable data stream. It is typically used with the SSH-2 protocol to provide secure file transfer. IP Security (IPSec) is a standardized framework for securing Internet Protocol (IP) communications by encrypting and/or authenticating each IP packet in a data stream. There are two modes of IPSec operation: transport mode and tunnel mode. Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for public key encryption and signing of e-mail encapsulated in MIME; it is not a web transaction protocol.

Question 385

The MOST important characteristic of good security policies is that they:

- ☐ state expectations of IT management.
- ☐ state only one general security mandate.
- ☒ are aligned with organizational goals.
- ☐ govern the creation of procedures and guidelines.

Explanation:

Explanation:

The most important characteristic of good security policies is that they be aligned with organizational goals. Failure to align policies and goals significantly reduces the value provided by the policies. Stating expectations of IT management omits addressing overall organizational goals and objectives. Stating only one general security mandate is the next best option since policies should be clear; otherwise, policies may be confusing and difficult to understand. Governing the creation of procedures and guidelines is most relevant to information security standards.

Licensed to Berend Post berend.post@it-university.nl

Question 386

An information security program should be sponsored by:

- ☐ infrastructure management.
- ☐ the corporate audit department.
- ☒ key business process owners.
- ☐ information security management.

Explanation:

Explanation:

The information security program should ideally be sponsored by business managers, as represented by key business process owners. Infrastructure management is not sufficiently independent and lacks the necessary knowledge regarding specific business requirements. A corporate audit department is not in as good a position to fully understand how an information security program needs to meet the needs of the business. Audit independence and objectivity will be lost, impeding traditional audit functions. Information security implements and executes the program. Although it should promote it at all levels, it cannot sponsor the effort due to insufficient operational knowledge and lack of proper authority.

Question 387

Which of the following is the PRIMARY reason for implementing a risk management program?

- ☐ Allows the organization to eliminate risk
- ☒ Is a necessary part of management's due diligence
- ☐ Satisfies audit and regulatory requirements
- ☐ Assists in incrementing the return on investment (ROD

Explanation:

Explanation:

The key reason for performing risk management is that it is part of management's due diligence. The elimination of all risk is not possible. Satisfying audit and regulatory requirements is of secondary importance. A risk management program may or may not increase the return on investment (ROD.

Licensed to Berend Post berend.post@it-university.nl

Question 388

Without prior approval, a training department enrolled the company in a free cloud-based collaboration site and invited employees to use it. Which of the following is the BEST response of the information security manager?

- ☐ Conduct a risk assessment and develop an impact analysis.
- ☐ Update the risk register and review the information security strategy.
- ☒ Report the activity to senior management.
- ☐ Allow temporary use of the site and monitor for data leakage.

Question 389

Which of the following is the MAIN reason for performing risk assessment on a continuous basis'?

- ☐ Justification of the security budget must be continually made.
- ☐ New vulnerabilities are discovered every day.
- ☒ The risk environment is constantly changing.
- ☐ Management needs to be continually informed about emerging risks.

Explanation:

Explanation:

The risk environment is impacted by factors such as changes in technology, and business strategy. These changes introduce new threats and vulnerabilities to the organization. As a result, risk assessment should be performed continuously. Justification of a budget should never be the main reason for performing a risk assessment. New vulnerabilities should be managed through a patch management process. Informing management about emerging risks is important, but is not the main driver for determining when a risk assessment should be performed.

Question 390

Risk acceptance is a component of which of the following?

- ☐ Assessment
- ☒ Mitigation
- ☐ Evaluation
- ☐ Monitoring

Explanation:

Explanation:

Risk acceptance is one of the alternatives to be considered in the risk mitigation process. Assessment and evaluation are components of the risk analysis process. Risk acceptance is not a component of monitoring.

Licensed to Berend Post berend.post@it-university.nl

Question 391

Data owners are normally responsible for which of the following?

- ☐ Applying emergency changes to application data
- ☐ Administering security over database records
- ☐ Migrating application code changes to production
- ☒ Determining the level of application security required

Explanation:

Explanation:

Data owners approve access to data and determine the degree of protection that should be applied (data classification). Administering database security, making emergency changes to data and migrating code to production are infrastructure tasks performed by custodians of the data.

Question 392

An organization's senior management is encouraging employees to use social media for promotional purposes. Which of the following should be the information security manager's FIRST step to support this strategy?

- ☐ Incorporate social media into the security awareness program.
- ☒ Develop a guideline on the acceptable use of social media.
- ☐ Develop a business case for a data loss prevention solution.
- ☐ Employ the use of a web content filtering solution.

Question 393

After logging in to a web application, further password credentials are required at various application points. Which of the following is the PRIMARY reason for such an approach?

- ☒ To ensure access is granted to the authorized person
- ☐ To enforce strong two-factor authentication
- ☐ To ensure session management variables are secure
- ☐ To implement single sign-on

Question 394

When developing an incident response plan, the information security manager should:

- ☐ include response scenarios that have been approved previously by business management.
- ☒ determine recovery time objectives (RTOs).
- ☐ allow IT to decide which systems can be removed from the infrastructure.
- ☐ require IT to invoke the business continuity plan.

Licensed to Berend Post berend.post@it-university.nl

Question 395

Secure customer use of an e-commerce application can BEST be accomplished through:

- ☒ data encryption.
- ☐ digital signatures.
- ☐ strong passwords.
- ☐ two-factor authentication.

Explanation:

Explanation:

Encryption would be the preferred method of ensuring confidentiality in customer communications with an e-commerce application. Strong passwords, by themselves, would not be sufficient since the data could still be intercepted, while two-factor authentication would be impractical. Digital signatures would not provide a secure means of communication. In most business-to-customer (B-to-C) web applications, a digital signature is also not a practical solution.

Question 396

Which of the following would a security manager establish to determine the target for restoration of normal processing?

- ☒ Recover time objective (RTO)
- ☐ Maximum tolerable outage (MTO)
- ☐ Recovery point objectives (RPOs)
- ☐ Services delivery objectives (SDOs)

Explanation:

Explanation:

Recovery time objective (RTO) is the length of time from the moment of an interruption until the time the process must be functioning at a service level sufficient to limit financial and operational impacts to an acceptable level. Maximum tolerable outage (MTO) is the maximum time for which an organization can operate in a reduced mode. Recovery point objectives (RPOs) relate to the age of the data required for recovery. Services delivery objectives (SDOs) are the levels of service required in reduced mode.

Licensed to Berend Post berend.post@it-university.nl

Question 397

The MOST useful way to describe the objectives in the information security strategy is through:

- ☒ attributes and characteristics of the 'desired state."
- ☐ overall control objectives of the security program.
- ☐ mapping the IT systems to key business processes.
- ☐ calculation of annual loss expectations.

Explanation:

Explanation:

Security strategy will typically cover a wide variety of issues, processes, technologies and outcomes that can best be described by a set of characteristics and attributes that are desired. Control objectives are developed after strategy and policy development. Mapping IT systems to key business processes does not address strategy issues. Calculation of annual loss expectations would not describe the objectives in the information security strategy.

Question 398

Which of the following change management procedures is MOST likely to cause concern to the information security manager?

- ☐ Fallback processes are tested the weekend before changes are made.
- ☒ The development manager migrates programs into production.
- ☐ A manual rather than an automated process is used to compare program versions.
- ☐ Users are not notified of scheduled system changes.

Question 399

Who is ultimately responsible for ensuring that information is categorized and that protective measures are taken?

- ☐ Information security officer
- ☒ Security steering committee
- ☐ Data owner
- ☐ Data custodian

Explanation:

Explanation:

Routine administration of all aspects of security is delegated, but senior management must retain overall responsibility. The information security officer supports and implements information security for senior management. The data owner is responsible for categorizing data security requirements. The data custodian supports and implements information security as directed.

Licensed to Berend Post berend.post@it-university.nl

Question 400

Which of the following is the BEST indicator that an effective security control is built into an organization?

- ☒ The monthly service level statistics indicate a minimal impact from security issues.
- ☐ The cost of implementing a security control is less than the value of the assets.
- ☐ The percentage of systems that is compliant with security standards.
- ☐ The audit reports do not reflect any significant findings on security.

Explanation:

Explanation:

The best indicator of effective security control is the evidence of little disruption to business operations. Choices B, C and D can support this evidence, but are supplemental to choice A.

Question 401

Which of the following is the MOST important to keep in mind when assessing the value of information?

- ☒ The potential financial loss
- ☐ The cost of recreating the information
- ☐ The cost of insurance coverage
- ☐ Regulatory requirement

Explanation:

Explanation:

The potential for financial loss is always a key factor when assessing the value of information. Choices B, C and D may be contributors, but not the key factor.

Question 402

The recovery time objective (RTO) is reached at which of the following milestones?

- ☐ Disaster declaration
- ☐ Recovery of the backups
- ☒ Restoration of the system
- ☐ Return to business as usual processing

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The recovery time objective (RTO) is based on the amount of time required to restore a system; disaster declaration occurs at the beginning of this period. Recovery of the backups occurs shortly after the beginning of this period. Return to business as usual processing occurs significantly later than the RTO. RTO is an "objective," and full restoration may or may not coincide with the RTO. RTO can be the minimum acceptable operational level, far short of normal operations.

Question 403

After obtaining commitment from senior management, which of the following should be completed NEXT when establishing an information security program?

- ☐ Define security metrics
- ☒ Conduct a risk assessment
- ☐ Perform a gap analysis
- ☐ Procure security tools

Explanation:

Explanation:

When establishing an information security program, conducting a risk assessment is key to identifying the needs of the organization and developing a security strategy. Defining security metrics, performing a gap analysis and procuring security tools are all subsequent considerations.

Question 404

What should be an organization's MAIN concern when evaluating an Infrastructure as a Service (IaaS) cloud computing model for an e-Commerce application?

- ☒ Availability of provider's services
- ☐ Internal about requirements
- ☐ Where the application resides
- ☐ Application ownership

Question 405

Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:

- ☒ it implies compliance risks.
- ☐ short-term impact cannot be determined.
- ☐ it violates industry security practices.
- ☐ changes in the roles matrix cannot be detected.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Monitoring processes are also required to guarantee fulfillment of laws and regulations of the organization and, therefore, the information security manager will be obligated to comply with the law. Choices B and C are evaluated as part of the operational risk. Choice D is unlikely to be as critical a breach of regulatory legislation. The acceptance of operational risks overrides choices B, C and D.

Question 406

A border router should be placed on which of the following?

- ☐ Web server
- ☐ IDS server
- ☐ Screened subnet
- ☒ Domain boundary

Explanation:

Explanation:

A border router should be placed on a (security) domain boundary. Placing it on a web server or screened subnet, which is a demilitarized zone (DMZ) would not provide any protection. Border routers are positioned on the boundary of the network, but do not reside on a server.

Question 407

The MOST appropriate owner of customer data stored in a central database, used only by an organization's sales department, would be the:

- ☐ sales department.
- ☐ database administrator.
- ☐ chief information officer (CIO).
- ☒ head of the sales department.

Explanation:

Explanation:

The owner of the information asset should be the person with the decision-making power in the department deriving the most benefit from the asset. In this case, it would be the head of the sales department. The organizational unit cannot be the owner of the asset because that removes personal responsibility. The database administrator is a custodian. The chief information officer (CIO) would not be an owner of this database because the CIO is less likely to be knowledgeable about the specific needs of sales operations and security concerns.

Licensed to Berend Post berend.post@it-university.nl

Question 408

Who is ultimately responsible for the organization's information?

- ☐ Data custodian
- ☐ Chief information security officer (CISO)
- ☒ Board of directors
- ☐ Chief information officer (CIO)

Explanation:

Explanation:

The board of directors is ultimately responsible for the organization's information and is tasked with responding to issues that affect its protection. The data custodian is responsible for the maintenance and protection of data. This role is usually filled by the IT department. The chief information security officer (CISO) is responsible for security and carrying out senior management's directives. The chief information officer (CIO) is responsible for information technology within the organization and is not ultimately responsible for the organization's information.

Question 409

When performing a quantitative risk analysis, which of the following is MOST important to estimate the potential loss?

- ☐ Evaluate productivity losses
- ☐ Assess the impact of confidential data disclosure
- ☒ Calculate the value of the information or asset
- ☐ Measure the probability of occurrence of each threat

Explanation:

Explanation:

Calculating the value of the information or asset is the first step in a risk analysis process to determine the impact to the organization, which is the ultimate goal. Determining how much productivity could be lost and how much it would cost is a step in the estimation of potential risk process. Knowing the impact if confidential information is disclosed is also a step in the estimation of potential risk. Measuring the probability of occurrence for each threat identified is a step in performing a threat analysis and therefore a partial answer.

Licensed to Berend Post berend.post@it-university.nl

Question 410

To implement a security framework, an information security manager must FIRST develop:

- ☐ security standards.
- ☐ security procedures.
- ☐ a security policy.
- ☒ security guidelines.

Question 411

Which of the following characteristics is MOST important to a bank in a high-value online financial transaction system?

- ☐ Identification
- ☒ Confidentiality
- ☐ Authentication
- ☐ Audit monitoring

Question 412

When developing a tabletop test plan for incident response testing, the PRIMARY purpose of the scenario should be to:

- ☐ give the business a measure of the organization's overall readiness
- ☐ provide participants with situations to ensure understanding of their roles
- ☒ measure management engagement as part of an incident response team
- ☐ challenge the incident response team to solve the problem under pressure

Explanation:

Explanations

Tabletop scenarios that need to be completed with one hour per scenario using full escalation as per decision trees to accurately simulate and evaluate responses of each team member and the processes within the playbooks.

Question 413

Which of the following controls is MOST effective in providing reasonable assurance of physical access compliance to an unmanned server room controlled with biometric devices?

- ☒ Regular review of access control lists
- ☐ Security guard escort of visitors
- ☐ Visitor registry log at the door
- ☐ A biometric coupled with a PIN

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

A review of access control lists is a detective control that will enable an information security manager to ensure that authorized persons are entering in compliance with corporate policy. Visitors accompanied by a guard will also provide assurance but may not be cost effective. A visitor registry is the next cost-effective control. A biometric coupled with a PIN will strengthen the access control; however, compliance assurance logs will still have to be reviewed.

Question 414

Which of the following is the MOST important process that an information security manager needs to negotiate with an outsource service provider?

- ☒ The right to conduct independent security reviews
- ☐ A legally binding data protection agreement
- ☐ Encryption between the organization and the provider
- ☐ A joint risk assessment of the system

Explanation:

Explanation:

A key requirement of an outsource contract involving critical business systems is the establishment of the organization's right to conduct independent security reviews of the provider's security controls. A legally binding data protection agreement is also critical, but secondary to choice A, which permits examination of the actual security controls prevailing over the system and. as such, is the more effective risk management tool. Network encryption of the link between the organization and the provider may well be a requirement, but is not as critical since it would also be included in choice A. A joint risk assessment of the system in conjunction with the outsource provider may be a compromise solution, should the right to conduct independent security reviews of the controls related to the system prove contractually difficult.

Question 415

A security manager meeting the requirements for the international flow of personal data will need to ensure:

- ☐ a data processing agreement.
- ☐ a data protection registration.
- ☒ the agreement of the data subjects.
- ☐ subject access procedures.

Explanation:

Explanation:

Whenever personal data are transferred across national boundaries, the awareness and agreement of the data subjects are required. Choices A, B and D are supplementary data protection requirements that are not key for international data transfer.

Licensed to Berend Post berend.post@it-university.nl

Question 416

A mission-critical system has been identified as having an administrative system account with attributes that prevent locking and change of privileges and name. Which would be the BEST approach to prevent successful brute forcing of the account?

- ☐ Prevent the system from being accessed remotely
- ☒ Create a strong random password
- ☐ Ask for a vendor patch
- ☐ Track usage of the account by audit trails

Explanation:

Explanation:

Creating a strong random password reduces the risk of a successful brute force attack by exponentially increasing the time required. Preventing the system from being accessed remotely is not always an option in mission-critical systems and still leaves local access risks. Vendor patches are not always available, tracking usage is a detective control and will not prevent an attack.

Question 417

The FIRST step in an incident response plan is to:

- ☐ notify- the appropriate individuals.
- ☐ contain the effects of the incident to limit damage.
- ☐ develop response strategies for systematic attacks.
- ☒ validate the incident.

Explanation:

Explanation:

Appropriate people need to be notified; however, one must first validate the incident. Containing the effects of the incident would be completed after validating the incident. Developing response strategies for systematic attacks should have already been developed prior to the occurrence of an incident.

Licensed to Berend Post berend.post@it-university.nl

Question 418

Following a risk assessment, new countermeasures have been approved by management. Which of the following should be performed NEXT?

- ☒ Develop an implementation strategy.
- ☐ Schedule the target end date for implementation activities.
- ☐ Budget the total cost of implementation activities.
- ☐ Calculate the residual risk for each countermeasure.

Question 419

A new regulation for safeguarding information processed by a specific type of transaction has come to the attention of an information security officer. The officer should FIRST:

- ☐ meet with stakeholders to decide how to comply.
- ☐ analyze key risks in the compliance process.
- ☒ assess whether existing controls meet the regulation.
- ☐ update the existing security/privacy policy.

Explanation:

Explanation:

If the organization is in compliance through existing controls, the need to perform other work related to the regulation is not a priority. The other choices are appropriate and important; however, they are actions that are subsequent and will depend on whether there is an existing control gap.

Question 420

To mitigate a situation where one of the programmers of an application requires access to production data, the information security manager could BEST recommend to.

- ☐ create a separate account for the programmer as a power user.
- ☒ log all of the programmers' activity for review by supervisor.
- ☐ have the programmer sign a letter accepting full responsibility.
- ☐ perform regular audits of the application.

Explanation:

Explanation:

It is not always possible to provide adequate segregation of duties between programming and operations in order to meet certain business requirements. A mitigating control is to record all of the programmers' actions for later review by their supervisor, which would reduce the likelihood of any inappropriate action on the part of the programmer. Choices A, C and D do not solve the problem.

Licensed to Berend Post berend.post@it-university.nl

Question 421

When the computer incident response team (CIRT) finds clear evidence that a hacker has penetrated the corporate network and modified customer information, an information security manager should FIRST notify:

- ☐ the information security steering committee.
- ☐ customers who may be impacted.
- ☒ data owners who may be impacted.
- ☐ regulatory- agencies overseeing privacy.

Explanation:

Explanation:

The data owners should be notified first so they can take steps to determine the extent of the damage and coordinate a plan for corrective action with the computer incident response team. Other parties will be notified later as required by corporate policy and regulatory requirements.

Question 422

An organization without any formal information security program that has decided to implement information security best practices should FIRST:

- ☐ invite an external consultant to create the security strategy.
- ☐ allocate budget based on best practices.
- ☐ benchmark similar organizations.
- ☒ define high-level business security requirements.

Explanation:

Explanation:

All four options are valid steps in the process of implementing information security best practices; however, defining high-level business security requirements should precede the others because the implementation should be based on those security requirements.

Question 423

Which of the following risks would BEST be assessed using quantitative risk assessment techniques?

- ☐ Customer data stolen
- ☒ An electrical power outage
- ☐ A web site defaced by hackers
- ☐ Loss of the software development team

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The effect of the theft of customer data or web site defacement by hackers could lead to a permanent decline in customer confidence, which does not lend itself to measurement by quantitative techniques. Loss of a majority of the software development team could have similar unpredictable repercussions. However, the loss of electrical power for a short duration is more easily measurable and can be quantified into monetary amounts that can be assessed with quantitative techniques.

Question 424

An organization's information security processes are currently defined as ad hoc. In seeking to improve their performance level, the next step for the organization should be to:

- ☒ ensure that security processes are consistent across the organization.
- ☐ enforce baseline security levels across the organization.
- ☐ ensure that security processes are fully documented.
- ☐ implement monitoring of key performance indicators for security processes.

Explanation:

Explanation:

The organization first needs to move from ad hoc to repeatable processes. The organization then needs to document the processes and implement process monitoring and measurement. Baselining security levels will not necessarily assist in process improvement since baselining focuses primarily on control improvement. The organization needs to standardize processes both before documentation, and before monitoring and measurement.

Question 425

Which of the following security mechanisms is MOST effective in protecting classified data that have been encrypted to prevent disclosure and transmission outside the organization's network?

- ☐ Configuration of firewalls
- ☐ Strength of encryption algorithms
- ☐ Authentication within application
- ☒ Safeguards over keys

Explanation:

Explanation:

If keys are in the wrong hands, documents will be able to be read regardless of where they are on the network. Choice A is incorrect because firewalls can be perfectly configured, but if the keys make it to the other side, they will not prevent the document from being decrypted. Choice B is incorrect because even easy encryption algorithms require adequate resources to break, whereas encryption keys can be easily used. Choice C is incorrect because the application "front door" controls may be bypassed by accessing data directly.

Licensed to Berend Post berend.post@it-university.nl

Question 426

Which of the following measures would be MOST effective against insider threats to confidential information?

- ☒ Role-based access control
- ☐ Audit trail monitoring
- ☐ Privacy policy
- ☐ Defense-in-depth

Explanation:

Explanation:

Role-based access control provides access according to business needs; therefore, it reduces unnecessary- access rights and enforces accountability. Audit trail monitoring is a detective control, which is 'after the fact.' Privacy policy is not relevant to this risk. Defense-in-depth primarily focuses on external threats

Question 427

The main mail server of a financial institution has been compromised at the superuser level; the only way to ensure the system is secure would be to:

- ☐ change the root password of the system.
- ☐ implement multifactor authentication.
- ☒ rebuild the system from the original installation medium.
- ☐ disconnect the mail server from the network.

Explanation:

Explanation:

Rebuilding the system from the original installation medium is the only way to ensure all security vulnerabilities and potential stealth malicious programs have been destroyed. Changing the root password of the system does not ensure the integrity of the mail server. Implementing multifactor authentication is an aftermeasure and does not clear existing security threats. Disconnecting the mail server from the network is an initial step, but does not guarantee security.

Licensed to Berend Post berend.post@it-university.nl

Question 428

What is the BEST way to ensure users comply with organizational security requirements for password complexity?

- ☐ Include password construction requirements in the security standards
- ☐ Require each user to acknowledge the password requirements
- ☐ Implement strict penalties for user noncompliance
- ☒ Enable system-enforced password configuration

Explanation:

Explanation:

Automated controls are generally more effective in preventing improper actions. Policies and standards provide some deterrence, but are not as effective as automated controls.

Question 429

What is the MOST important item to be included in an information security policy?

- ☐ The definition of roles and responsibilities
- ☐ The scope of the security program
- ☒ The key objectives of the security program
- ☐ Reference to procedures and standards of the security program

Explanation:

Explanation:

Stating the objectives of the security program is the most important element to ensure alignment with business goals. The other choices are part of the security policy, but they are not as important.

Question 430

Which of the following is the BEST approach to make strategic information security decisions?

- ☐ Establish an information security steering committee.
- ☐ Establish periodic senior management meetings.
- ☐ Establish regular information security status reporting.
- ☒ Establish business unit security working groups.

Licensed to Berend Post berend.post@it-university.nl

Question 431

As part of an international expansion plan, an organization has acquired a company located in another jurisdiction. Which of the following would be the BEST way to maintain any effective information security program?

- ☐ Ensure information security is included in any change control efforts
- ☐ Merge the two information security programs to establish continuity
- ☒ Determine new factors that could influence the information security strategy
- ☐ Implement the current information security program in the acquired company

Question 432

When developing an information security program, what is the MOST useful source of information for determining available resources?

- ☐ Proficiency test
- ☐ Job descriptions
- ☐ Organization chart
- ☒ Skills inventory

Explanation:

Explanation:

A skills inventory would help identify- the available resources, any gaps and the training requirements for developing resources. Proficiency testing is useful but only with regard to specific technical skills. Job descriptions would not be as useful since they may be out of date or not sufficiently detailed. An organization chart would not provide the details necessary to determine the resources required for this activity.

Question 433

A business partner of a factory has remote read-only access to material inventory to forecast future acquisition orders. An information security manager should PRIMARILY ensure that there is:

- ☒ an effective control over connectivity and continuity.
- ☐ a service level agreement (SLA) including code escrow.
- ☐ a business impact analysis (BIA).
- ☐ a third-party certification.

Explanation:

Explanation:

The principal risk focus is the connection procedures to maintain continuity in case of any contingency. Although an information security manager may be interested in the service level agreement (SLA), code escrow is not a concern. A business impact analysis (BIA) refers to

Licensed to Berend Post berend.post@it-university.nl

contingency planning and not to system access. Third-party certification does not provide any assurance of controls over connectivity to maintain continuity.

Question 434

After completing a full IT risk assessment, who can BEST decide which mitigating controls should be implemented?

- ☐ Senior management
- ☒ Business manager
- ☐ IT audit manager
- ☐ Information security officer (ISO)

Explanation:

Explanation:

The business manager will be in the best position, based on the risk assessment and mitigation proposals. to decide which controls should/could be implemented, in line with the business strategy and with budget. Senior management will have to ensure that the business manager has a clear understanding of the risk assessed but in no case will be in a position to decide on specific controls. The IT audit manager will take part in the process to identify threats and vulnerabilities, and to make recommendations for mitigations. The information security officer (ISO) could make some decisions regarding implementation of controls. However, the business manager will have a broader business view and full control over the budget and, therefore, will be in a better position to make strategic decisions.

Question 435

What is the GREATEST advantage of documented guidelines and operating procedures from a security perspective?

- ☐ Provide detailed instructions on how to carry out different types of tasks
- ☒ Ensure consistency of activities to provide a more stable environment
- ☐ Ensure compliance to security standards and regulatory requirements
- ☐ Ensure reusability to meet compliance to quality requirements

Explanation:

Explanation:

Developing procedures and guidelines to ensure that business processes address information security risk is critical to the management of an information security program. Developing procedures and guidelines establishes a baseline for security program performance and consistency of security activities.

Licensed to Berend Post berend.post@it-university.nl

Question 436

Which of the following roles is PRIMARILY responsible for determining the information classification levels for a given information asset?

- ☐ Manager
- ☐ Custodian
- ☐ User
- ☒ Owner

Explanation:

Explanation:

Although the information owner may be in a management position and is also considered a user, the information owner role has the responsibility for determining information classification levels. Management is responsible for higher-level issues such as providing and approving budget, supporting activities, etc. The information custodian is responsible for day-to-day security tasks such as protecting information, backing up information, etc. Users are the lowest level. They use the data, but do not classify the data. The owner classifies the data.

Question 437

What is the MAIN drawback of e-mailing password-protected zip files across the Internet? They:

- ☐ all use weak encryption.
- ☐ are decrypted by the firewall.
- ☒ may be quarantined by mail filters.
- ☐ may be corrupted by the receiving mail server.

Explanation:

Explanation:

Often, mail filters will quarantine zip files that are password-protected since the filter (or the firewall) is unable to determine if the file contains malicious code. Many zip file products are capable of using strong encryption. Such files are not normally corrupted by the sending mail server.

Question 438

Which of the following is the BEST defense against distributed denial of service (DDoS) attacks?

- ☐ Multiple and redundant paths
- ☒ Well-configured routers and firewalls
- ☐ Regular patching
- ☐ Intruder-detection lockout

Licensed to Berend Post berend.post@it-university.nl

Question 439

Which of (lie following would be the MOST relevant factor when defining the information classification policy?

- ☐ Quantity of information
- ☐ Available IT infrastructure
- ☐ Benchmarking
- ☒ Requirements of data owners

Explanation:

Explanation:

When defining the information classification policy, the requirements of the data owners need to be identified. The quantity of information, availability of IT infrastructure and benchmarking may be part of the scheme after the fact and would be less relevant.

Question 440

Executive management is considering outsourcing all IT operations. Which of the following functions should remain internal?

- ☒ Data ownership
- ☐ Data monitoring
- ☐ Data custodian
- ☐ Data encryption

Question 441

The MOST effective way to incorporate risk management practices into existing production systems is through:

- ☐ policy development.
- ☒ change management.
- ☐ awareness training.
- ☐ regular monitoring.

Explanation:

Explanation:

Change is a process in which new risks can be introduced into business processes and systems. For this reason, risk management should be an integral component of the change management process. Policy development, awareness training and regular monitoring, although all worthwhile activities, are not as effective as change management.

Licensed to Berend Post berend.post@it-university.nl

Question 442

Which of the following should be PRIMARILY included in a security training program for business process owners?

- ☒ Impact of security risks
- ☐ Application vulnerabilities
- ☐ Application recovery time
- ☐ List of security incidents reported

Question 443

When a significant security breach occurs, what should be reported FIRST to senior management?

- ☐ A summary of the security logs that illustrates the sequence of events
- ☒ An explanation of the incident and corrective action taken
- ☐ An analysis of the impact of similar attacks at other organizations
- ☐ A business case for implementing stronger logical access controls

Explanation:

Explanation:

When reporting an incident to senior management, the initial information to be communicated should include an explanation of what happened and how the breach was resolved. A summary of security logs would be too technical to report to senior management. An analysis of the impact of similar attacks and a business case for improving controls would be desirable; however, these would be communicated later in the process.

Question 444

Which of the following practices is BEST to remove system access for contractors and other temporary users when it is no longer required?

- ☐ Log all account usage and send it to their manager
- ☒ Establish predetermined automatic expiration dates
- ☐ Require managers to e-mail security when the user leaves
- ☐ Ensure each individual has signed a security acknowledgement

Explanation:

Explanation:

Predetermined expiration dates are the most effective means of removing systems access for temporary users. Reliance on managers to promptly send in termination notices cannot always be counted on, while requiring each individual to sign a security acknowledgement would have little effect in this case.

Licensed to Berend Post berend.post@it-university.nl

Question 445

Which of the following is MOST important for an information security manager to regularly report to senior management?

- ☐ Results of penetration tests
- ☐ Audit reports
- ☒ Impact of unremediated risks
- ☐ Threat analysis reports

Question 446

In the process of deploying a new e-mail system, an information security manager would like to ensure the confidentiality of messages while in transit. Which of the following is the MOST appropriate method to ensure data confidentiality in a new e-mail system implementation?

- ☒ Encryption
- ☐ Digital certificate
- ☐ Digital signature
- ☐ I lashing algorithm

Explanation:

Explanation:

To preserve confidentiality of a message while in transit, encryption should be implemented. Choices B and C only help authenticate the sender and the receiver. Choice D ensures integrity.

Question 447

The valuation of IT assets should be performed by:

- ☐ an IT security manager.
- ☐ an independent security consultant.
- ☐ the chief financial officer (CFO).
- ☒ the information owner.

Explanation:

Explanation:

Information asset owners are in the best position to evaluate the value added by the IT asset under review within a business process, thanks to their deep knowledge of the business processes and of the functional IT requirements. An IT security manager is an expert of the IT risk assessment methodology and IT asset valuation mechanisms. However, the manager could not have a deep understanding of all the business processes of the firm. An IT security subject matter expert will take part of the process to identify threats and vulnerabilities and will collaborate with the business

Licensed to Berend Post berend.post@it-university.nl

information asset owner to define the risk profile of the asset. A chief financial officer (CFO) will have an overall costs picture but not detailed enough to evaluate the value of each IT asset.

Question 448

The PRIMARY reason for using information security metrics is to:

- ☐ achieve senior management commitment.
- ☐ ensure alignment with corporate requirements.
- ☐ adhere to legal and regulatory requirements.
- ☒ monitor the effectiveness of controls.

Question 449

Which of the following is the BEST justification to convince management to invest in an information security program?

- ☐ Cost reduction
- ☐ Compliance with company policies
- ☐ Protection of business assets
- ☒ Increased business value

Explanation:

Explanation:

Investing in an information security program should increase business value and confidence. Cost reduction by itself is rarely the motivator for implementing an information security program. Compliance is secondary to business value. Increasing business value may include protection of business assets.

Question 450

In an organization, information systems security is the responsibility of:

- ☒ all personnel.
- ☐ information systems personnel.
- ☐ information systems security personnel.
- ☐ functional personnel.

Explanation:

Explanation:

All personnel of the organization have the responsibility of ensuring information systems security- this can include indirect personnel such as physical security personnel. Information systems security cannot be the responsibility of information systems personnel alone since they cannot ensure

Licensed to Berend Post berend.post@it-university.nl

security. Information systems security cannot be the responsibility of information systems security personnel alone since they cannot ensure security. Information systems security cannot be the responsibility of functional personnel alone since they cannot ensure security.

Question 451

An information security manager is recommending an investment in a new security initiative to address recently published threats. Which of the following would be MOST important to include in the business case?

- ☒ Business impact if threats materialize
- ☐ Availability of unused funds in the security budget
- ☐ Threat information from reputable sources
- ☐ Alignment of the new initiative with the approved business strategy

Question 452

Which of the following would BEST assist an information security manager in measuring the existing level of development of security processes against their desired state?

- ☐ Security audit reports
- ☐ Balanced scorecard
- ☒ Capability maturity model (CMM)
- ☐ Systems and business security architecture

Explanation:

Explanation:

The capability maturity model (CMM) grades each defined area of security processes on a scale of 0 to 5 based on their maturity, and is commonly used by entities to measure their existing state and then determine the desired one. Security audit reports offer a limited view of the current state of security. Balanced scorecard is a document that enables management to measure the implementation of their strategy and assists in its translation into action. Systems and business security architecture explain the security architecture of an entity in terms of business strategy, objectives, relationships, risks, constraints and enablers, and provides a business-driven and business-focused view of security architecture.

Licensed to Berend Post berend.post@it-university.nl

Question 453

What is the BEST way to alleviate security team understaffing while retaining the capability in-house?

- ☐ Hire a contractor that would not be included in the permanent headcount
- ☐ Outsource with a security services provider while retaining the control internally
- ☒ Establish a virtual security team from competent employees across the company
- ☐ Provide cross training to minimize the existing resources gap

Explanation:

Explanation:

While hiring an indirect resource that will not be part of headcount will help to add an extra resource, it usually costs more than a direct employee; thus, it is not cost efficient. Outsourcing may be a more expensive option and can add complexities to the service delivery. Competent security staff can be recruited from other departments e.g., IT. product development, research and development (R&D). By leveraging existing resources, there is a nominal additional cost. It is also a strategic option since the staff may join the team as full members in the future (internal transfer). Development of staff is often a budget drain and, if not managed carefully, these resources may move away from the company and leave the team with a bigger resource gap.

Question 454

Which of the following is MOST important for measuring the effectiveness of a security awareness program?

- ☐ Reduced number of security violation reports
- ☒ A quantitative evaluation to ensure user comprehension
- ☐ Increased interest in focus groups on security issues
- ☐ Increased number of security violation reports

Explanation:

Explanation:

To truly judge the effectiveness of security awareness training, some means of measurable testing is necessary to confirm user comprehension. Focus groups may or may not provide meaningful feedback but, in and of themselves, do not provide metrics. An increase or reduction in the number of violation reports may not be indicative of a high level of security awareness.

Licensed to Berend Post berend.post@it-university.nl

Question 455

The MAIN reason for deploying a public key infrastructure (PKI) when implementing an information security program is to:

- ☐ ensure the confidentiality of sensitive material.
- ☒ provide a high assurance of identity.
- ☐ allow deployment of the active directory.
- ☐ implement secure sockets layer (SSL) encryption.

Explanation:

Explanation:

The primary purpose of a public key infrastructure (PKI) is to provide strong authentication. Confidentiality is a function of the session keys distributed by the PKI. An active directory can use PKI for authentication as well as using other means. Even though secure sockets layer (SSL) encryption requires keys to authenticate, it is not the main reason for deploying PKI.

Question 456

When residual risk is minimized:

- ☒ acceptable risk is probable.
- ☐ transferred risk is acceptable.
- ☐ control risk is reduced.
- ☐ risk is transferable.

Explanation:

Explanation:

Since residual risk is the risk that remains after putting into place an effective risk management program, it is probable that the organization will decide that it is an acceptable risk if sufficiently minimized. Transferred risk is risk that has been assumed by a third party, therefore its magnitude is not relevant. Accordingly, choices B and D are incorrect since transferred risk does not necessarily indicate whether risk is at an acceptable level. Minimizing residual risk will not reduce control risk.

Question 457

Which would be the BEST recommendation to protect against phishing attacks?

- ☐ Install an antispam system
- ☒ Publish security guidance for customers
- ☐ Provide security awareness to the organization's staff
- ☐ Install an application-level firewall

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Customers of the organization are the target of phishing attacks. Installing security software or training the organization's staff will be useless. The effort should be put on the customer side.

Question 458

The BEST way to mitirate the risk associated with a social engineering attack is to:

- ☐ deploy an effective intrusion detection system (IDS).
- ☐ perform a business risk assessment of the email filtering system.
- ☐ implement multi-factor authentication on critical business systems.
- ☒ perform a user-knowledge gap assessment of information security practices.

Question 459

A global organization has developed a strategy to share a customer information database between offices in two countries. In this situation, it is MOST important to ensure:

- ☒ data sharing complies with local laws and regulations at both locations.
- ☐ data is encrypted in transit and at rest.
- ☐ a nondisclosure agreement is signed.
- ☐ risk coverage is split between the two locations sharing data.

Question 460

Which of the following is MOST likely to reduce the effectiveness of a signature-based intrusion detection system (IDS)?

- ☐ The activities being monitored deviate from what is considered normal.
- ☐ The information regarding monitored activities becomes stale.
- ☐ The pattern of normal behavior changes quickly and dramatically.
- ☒ The environment is complex.

Question 461

Which of the following tasks should be performed once a disaster recovery plan has been developed?

- ☐ Analyze the business impact
- ☒ Define response team roles
- ☐ Develop the test plan
- ☐ Identify recovery time objectives

Licensed to Berend Post berend.post@it-university.nl

Question 462

Which of the following is the MOST relevant metric to include in an information security quarterly report to the executive committee?

- ☒ Security compliant servers trend report
- ☐ Percentage of security compliant servers
- ☐ Number of security patches applied
- ☐ Security patches applied trend report

Explanation:

Explanation:

The percentage of compliant servers will be a relevant indicator of the risk exposure of the infrastructure. However, the percentage is less relevant than the overall trend, which would provide a measurement of the efficiency of the IT security program. The number of patches applied would be less relevant, as this would depend on the number of vulnerabilities identified and patches provided by vendors.

Question 463

Which of the following is MOST effective in protecting against the attack technique known as phishing?

- ☐ Firewall blocking rules
- ☐ Up-to-date signature files
- ☒ Security awareness training
- ☐ Intrusion detection monitoring

Explanation:

Explanation:

Phishing relies on social engineering techniques. Providing good security awareness training will best reduce the likelihood of such an attack being successful. Firewall rules, signature files and intrusion detection system (IDS) monitoring will be largely unsuccessful at blocking this kind of attack.

Question 464

What would be the MOST significant security risks when using wireless local area network (LAN) technology?

- ☐ Man-in-the-middle attack
- ☐ Spoofing of data packets
- ☒ Rogue access point
- ☐ Session hijacking

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

A rogue access point masquerades as a legitimate access point The risk is that legitimate users may connect through this access point and have their traffic monitored. All other choices are not dependent on the use of a wireless local area network (LAN) technology.

Question 465

Which of the following would be MOST effective in successfully implementing restrictive password policies?

- ☐ Regular password audits
- ☐ Single sign-on system
- ☒ Security awareness program
- ☐ Penalties for noncompliance

Explanation:

Explanation:

To be successful in implementing restrictive password policies, it is necessary to obtain the buy-in of the end users. The best way to accomplish this is through a security awareness program. Regular password audits and penalties for noncompliance would not be as effective on their own; people would go around them unless forced by the system. Single sign-on is a technology solution that would enforce password complexity but would not promote user compliance. For the effort to be more effective, user buy-in is important.

Question 466

The MOST important objective of a post incident review is to:

- ☒ capture lessons learned to improve the process.
- ☐ develop a process for continuous improvement.
- ☐ develop a business case for the security program budget.
- ☐ identify new incident management tools.

Explanation:

Explanation:

The main purpose of a post incident review is to identify areas of improvement in the process. Developing a process for continuous improvement is not true in every case. Developing a business case for the security program budget and identifying new incident management tools may come from the analysis of the incident, but are not the key objectives.

Licensed to Berend Post berend.post@it-university.nl

Question 467

For virtual private network (VPN) access to the corporate network, the information security manager is requiring strong authentication. Which of the following is the strongest method to ensure that logging onto the network is secure?

- ☐ Biometrics
- ☐ Symmetric encryption keys
- ☐ Secure Sockets Layer (SSL)-based authentication
- ☒ Two-factor authentication

Explanation:

Explanation:

Two-factor authentication requires more than one type of user authentication. While biometrics provides unique authentication, it is not strong by itself, unless a PIN or some other authentication factor is used with it. Biometric authentication by itself is also subject to replay attacks. A symmetric encryption method that uses the same secret key to encrypt and decrypt data is not a typical authentication mechanism for end users. This private key could still be compromised. SSL is the standard security technology for establishing an encrypted link between a web server and a browser. SSL is not an authentication mechanism. If SSL is used with a client certificate and a password, it would be a two-factor authentication.

Question 468

An organization has adopted a practice of regular staff rotation to minimize the risk of fraud and encourage cross training. Which type of authorization policy would BEST address this practice?

- ☐ Multilevel
- ☒ Role-based
- ☐ Discretionary
- ☐ Attribute-based

Explanation:

Explanation:

A role-based policy will associate data access with the role performed by an individual, thus restricting access to data required to perform the individual's tasks. Multilevel policies are based on classifications and clearances. Discretionary policies leave access decisions up to information resource managers.

Licensed to Berend Post berend.post@it-university.nl

Question 469

Which of the following, using public key cryptography, ensures authentication, confidentiality and nonrepudiation of a message?

- ☐ Encrypting first by receiver's private key and second by sender's public key
- ☒ Encrypting first by sender's private key and second by receiver's public key
- ☐ Encrypting first by sender's private key and second decrypting by sender's public key
- ☐ Encrypting first by sender's public key and second by receiver's private key

Explanation:

Explanation:

Encrypting by the sender's private key ensures authentication. By being able to decrypt with the sender's public key, the receiver would know that the message is sent by the sender only and the sender cannot deny/repudiate the message. By encrypting with the sender's public key secondly, only the sender will be able to decrypt the message and confidentiality is assured. The receiver's private key is private to the receiver and the sender cannot have it for encryption. Similarly, the receiver will not have the private key of the sender to decrypt the second-level encryption. In the case of encrypting first by the sender's private key and. second, decrypting by the sender's public key, confidentiality is not ensured since the message can be decrypted by anyone using the sender's public key. The receiver's private key would not be available to the sender for second-level encryption. Similarly, the sender's private key would not be available to the receiver for decrypting the message.

Licensed to Berend Post berend.post@it-university.nl