Free CISM Exam Prep Practice Test

Attempt CISM practice test questions and test your skills. This free CISM exam prep material simulates the actual certification exam.

200 Questions, 240 Minutes

Explanations

200	172	86
Questions	Correct Answers	%Correct Answers

1. As an IS Manager, you would like to lay down clearly-defined roles and responsibilities? What is the BEST benefit that you expect?

○ Ensure that all your team comply with policies.

○ Your team knows what to do and when.

● Every one is clear about their responsibilites and work that need to be done.

○ Your team is more accountable.

Explanation:

The correct option is D.Well-defined roles and responsibilities is a major requirement for accountability.

2. Who would you look to enforce access rights to application data?

○ Data owners

○ Business process owners

○ The security steering committee

● Security administrators

Explanation:

The correct option is D.As data custodians, security administrators are responsible for enforcing access rights to data. Data owners are responsible for approving these access rights. Business process owners are sometimes the data owners as well, and would not be

Call Us Chat Query?

3. You need to get approval form senior management to implement a warm site. How can you BEST achieve this?

○ Present periodic risk assessment reports

○ Present regulatory requirements as mandated by law

○ [✓ Present a business case with cost-benefit analyses.]

○ Present how the warm site would be measured.

Explanation:

The correct option is C.Business case development, including a cost-benefit analysis, is most ideal to win the support of the senior management. The remaining options cannot be used to garner support on their own and always must be accompanied by a business case. Keeping senior management informed of regulatory requirements may help gain support for initiatives, but it is well known that more than half of all organizations are not in compliance, so may not get senior management buy-in.

4. As an IS Manager you are developing IS Strategy for your organization. Which is the MOST important component of the strategy?

○ [✓ Well defined objectives]

○ Time frames for delivery

○ Adoption of a internation control framework like COBIT, ISO etc.

○ Complete policies

Explanation:

The correct option is A.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 have a successful information security strategy. Policies are developed subsequent to, and as a part of, implementing a strategy.

5. Which of the following is MOST important to understand when developing a meaningful information security strategy?

○ Regulatory environment

○ International security standards

○ Organizational risks

○ Organizational goals

Explanation:

Call Us Chat Query?

accomplish. The other choices are all elements that must be considered, but their importance is secondary and will vary depending on organizational goals.

6. You are implementing IS policy within your organization. There is a sense of discomfort from within the organization about certain components of the policy. What is the BEST approach to counter this?

○ Publish documentation about the IS Policy, so that all staff are aware.

○ Obtain strong management support

○ Get HR department involved to ensure strict compliance

○ Get internal audit to check whether there is compliance with the IS policy

Explanation:

The correct option is B.The best way to ensure the organization adopt the IS Policy is to get management support. Pressure from senior management will help to enforce the policy.

7. You have joined an organization recently as an IS Manager. You have requested a meeting with the senior management to discuss organization's network security to the senior managerment. What would you present FIRST?

○ Infrastructure layout of the organization which highlights all protective devices installed.

○ Present a a list of attacks that the organization may face on the network.

○ Present the first draft of your IS Policy.

○ Present the risk assessment report.

Explanation:

The correct option is D.A tool used to help the senior management to understand high level threats, probabilities and existing controls is a risk assessment. Others may follow the risk assessment presentation.

8. You are an IS Manager of an ecommerce portal. You have seen in the media about a new regulation that affects ecommerce transactions. What should you do FIRST?

○ Call for a meeting with all key stakeholders to discuss the regulation.

○ Inform the risk management team to analyze the regulation.

○ Check whether the controls in the existing ecommerce portal can address the regulation.

○ Inform you team of your plan to conduct a gap analysis.

Explanation:

taken only if the existing controls cannot address the regulation.

9. Which of the following would help to change an organization's security culture?

○ Develop procedures to enforce the information security policy

○ Obtain strong management support

○ Implement strict technical security controls

○ Periodically audit compliance with the information security policy

Explanation:

The correct option is B.Management support and pressure will help to change an organization's culture. Procedures will support an information security policy, but cannot change the culture of the organization. Technical controls will provide more security to an information system and staff; however, this does not mean the culture will be changed. Auditing will help to ensure the effectiveness of the information security policy; however, auditing is not effective in changing the culture of the company.

10. The PRIMARY goal in developing an information security strategy is to:

○ establish security metrics and performance monitoring.

○ educate business process owners regarding their duties

○ ensure that legal and regulatory requirements are met.

○ support the business objectives of the organization.

Explanation:

The correct option is D.The business objectives of the organization supersede all other factors. Establishing metrics and measuring performance, meeting legal and regulatory requirements, and educating business process owners are all subordinate to this overall goal.

11. The MOST important reason for aligning information security governance with corporate governance is to:

○ Provide cost-benefit to the organization.

○ Ensures all members of the IS Team understan corporate governance.

○ Ensure that all operations within the security team are consistent.

○ Ensure a faster response time for regulations.

Explanation:

The correct option is A.Non-alignment of corporate governance and security governance will result in potentially weak, duplicate or unneccessary controls. This can result in additional costs for the organization to rework and align security governance with corporate

12. A systems approach to managing information security can be a benefit PRIMARILY because it is:

○ able to provide a more integrated, holistic program.

○ an essential aspect of developing a security strategy.

○ a requirement for industry (ISO) certification.

○ a necessary component of organization governance.

Explanation:

The correct option is A.A holistic model based on a systems approach can help clarify complex relationships and their interdependencies within an organization, and thus provide a more effective integration of people, processes and technology. While a systems approach is useful for developing a security strategy and for understanding the relationship between people, processes and technology, a systems approach is not essential nor is it a requirement for industry (ISO) certification.

13. 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.

○ Determine likely areas of compliance.

○ Understand the threats to the business.

Explanation:

The correct option is A.Business operations are the main driver for security activities. IS Manager must ensure that all activities, carried out not only support the organizational objectives, but also preserves the organization.

14. Which of the following requirements would have the lowest level of priority in information security?

○ Technical

○ Regulatory

○ Privacy

○ Business

Explanation:

The correct option is A.Information security priorities may, at times, override technical specifications, which then must be rewritten to conform to minimum security standards. Regulatory and privacy requirements are government-mandated and, therefore, not subject to

Call Us Chat Query?

15. The MOST complete business case for procuring and implementing security solutions is one that:

○ [✓ includes appropriate justification.]

○ explains the current risk profile.

○ details regulatory requirements.

○ identifies incidents and losses.

Explanation:

The correct option is A.Management is primarily interested in security solutions that can address risks in the most cost-effective way. To address the needs of an organization, a business case should address appropriate security solutions in line with the organizational strategy.

16. Laws and regulations should be addressed by the information security manager:

○ [✓ to the extent that they impact the enterprise.]

○ by implementing international standards.

○ by developing policies that address the requirements.

○ to ensure that guidelines meet the requirements.

Explanation:

The correct option is A.Legal and regulatory requirements should be assessed based on the impact of noncompliance or partial compliance balanced against the costs of compliance, the risk tolerance defined by management, and the extent and nature of enforcement. International standards may not address the legal requirements in question. Policies should not address particular regulations because regulations are subject to change. Policies should only address the need to assess regulatory requirements and deal with them appropriately based on risk and impact. Guidelines would normally not address regulations, although standards may address regulations based on management's determination of the appropriate level of compliance.

17. 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:

Call Us Chat Query?

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.

18. An outcome of effective security governance is:

○ business dependency assessment.

○ strategic alignment.

○ risk assessment.

○ planning.

Explanation:

The correct option is B.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.

19. Which of the following is the PRIMARY reason to change policies during program development?

○ The policies must comply with new regulatory and legal mandates.

○ Appropriate security baselines are no longer set in the policies.

○ The policies no longer reflect management intent and direction.

○ Employees consistently ignore the policies.

Explanation:

The correct option is C.Policies must reflect management intent and direction. Policies should be changed only when management determines that there is a need to address new legal and regulatory requirements. Regulatory requirements typically are better addressed with standards and procedures than with high-level policies. Standards set security baselines, not policies. Employees not abiding by policies is a compliance and enforcement issue rather than a reason to change the policies.

20. Information security projects should be prioritized on the basis of:

○ time required for implementation.

○ impact on the organization.

○ total cost for implementation.

○ mix of resources required.

The correct option is B.Information security projects should be assessed on the basis of the positive impact that they will have on the organization. Time,cost and resource issues should be subordinate to this objective.

21. The MOST important component of a privacy policy is:

○ notifications.

○ warranties.

○ liabilities.

○ geographic coverage.

Explanation:

The correct option is A.Privacy policies must contain notifications and opt-out provisions; they are a high-level management statement of direction. They do not necessarily address warranties, liabilities or geographic coverage, which are more specific.

22. Which of the following is MOST likely to be discretionary?

○ Policies

○ Procedures

○ Guidelines

○ Standards

Explanation:

The correct option is C.Policies define security goals and expectations for an organization. These are defined in more specific terms within standards and procedures. Standards establish what is to be done while procedures describe how it is to be done. Guidelines provide recommendations that business management must consider in developing practices within their areas of control; as such, they are discretionary.

23. 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:

Call Us Chat Query?

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.

24. 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:

The correct option is C.As high-level statements, information security policies should be straightforward and easy to understand. They are 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.

25. Which person or group should have final approval of an organization's information security policies?

○ Business unit managers

○ Chief information security officer (CISO)

○ Senior management

○ Chief information officer (CIO)

Explanation:

The correct option is C.Senior management should have final approval of all organization policies, including information technology (IT) security policies.Business unit managers should have input into IT policies, but they should not have authority to give final approval. The CISO would more than likely be the primary author of the policies and therefore is not the appropriate individual to approve the policies. The CIO should provide input into the IT security policies, but should not have the authority to give final approval.

26. 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:

Call Us Chat Query?

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 groupwide 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.

27. When implementing effective security governance within the requirements of the company\'s security strategy, which of the following is the MOST important factor to consider?

○ Preserving the confidentiality of sensitive data

○ Establishing international security standards for data sharing

○ Adhering to corporate privacy standards

○ Establishing system manager responsibility for information security

Explanation:

The correct option is A.The goal of information security is to protect the organization's information assets. International security standards are situational, depending upon the company and its business. Adhering to corporate privacy standards is important, but those standards must be appropriate and adequate and are not the most important factor to consider. All employees are responsible for information security,but it is not the most important factor to consider.

28. Senior management commitment and support for information security will BEST be attained by an information security manager by emphasizing:

○ organizational risk.

○ organizationwide metrics.

○ security needs.

○ the responsibilities of organizational units.

Explanation:

The correct option is A.Information security exists to help the organization meet its objectives. The information security manager should identify information security needs based on organizational needs. Organizational or business risk should always take precedence. Involving each organizational unit in information security and establishing metrics to measure success will be viewed favorably by senior management after the overall organizational risk is identified.

29. Which of the following should drive the risk analysis for an organization?

○ Senior management

○ [✓ Security manager]

○ Quality manager

Call Us Chat Query?

Explanation:

The correct option is B.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.

30. Which of the following are seldom changed in response to technological changes?

○ Standards

○ Procedures

○ [✓ Policies]

○ Guidelines

Explanation:

The correct option is C.Policies are high-level statements of objectives. Because of their high-level nature and statement of broad operating principles, they are less subject to periodic change. Security standards and procedures as well as guidelines must be revised and updated based on the impact of technology changes.

31. Who is responsible for ensuring that information is categorized and that specific protective measures are taken?

○ The security officer

○ [✓ Senior management]

○ The end user

○ The custodian

Explanation:

The correct option is B.Routine administration of all aspects of security is delegated, but top management must retain overall responsibility. The security officer supports and implements information security for senior management. The end user does not perform categorization. The custodian supports and implements information security measures as directed.

32. Which of the following is the BEST approach to obtain senior management commitment to the information security program?

○ Describe the reduction of risk.

○ Present the emerging threat environment.

○ Benchmark against other enterprises.

○ Demonstrate the alignment of the program to business objectives.

Call Us Chat Query?

The correct option is D.A security program must be aligned to business objectives. Senior management will support the security program only when it helps achieve the business objectives. The security program will always try to reduce the risk; however, it has to be balanced against the cost and impact to the business. Reduction of risk alone cannot justify the security program from the senior management perspective. The security program monitors emerging threats; however, the threat environment itself cannot determine the mitigating activities. There are many ways to deal with threats. Senior management is primarily interested in how the security program can mitigate threats while supporting the ultimate business goals. While benchmarking against other enterprises can provide an approach, it does not necessarily mean that the approach is the best one for the enterprise.

33. 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:

The correct option is C.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.

34. The data access requirements for an application should be determined by the:

○ legal department.

○ compliance officer.

○ information security manager.

○ business owner.

Explanation:

The correct option is D.Business owners are ultimately responsible for their applications. The legal department, compliance officer and information security manager all can advise, but do not have final responsibility.

35. Which of the following is a key area of the ISO 27001 framework?

○ Operational risk assessment

○ Financial crime metrics

Call Us Chat Query?

○ Business continuity management

Explanation:

The correct option is D.Operational risk assessment, financial crime metrics and capacity management can complement the information security framework, but only business continuity management is a key component.

36. 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:

The correct option is C.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.

37. Which of the following is responsible for legal and regulatory liability?

○ Chief security officer (CSO)

○ Chief legal counsel (CLC)

○ Board and senior management

○ Information security steering group

Explanation:

The correct option is C.The board of directors and senior management are ultimately responsible for all that happens in the organization. The others are not individually liable for failures of security in the organization.

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

○ Consultation

○ Negotiation

○ Facilitation

Explanation:

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

39. Security technologies should be selected PRIMARILY on the basis of their:

○ ability to mitigate business risks.

○ evaluations in trade publications.

○ use of new and emerging technologies.

○ benefits in comparison to their costs.

Explanation:

The correct option is A.The most fundamental evaluation criterion for the appropriate selection of any security technology is its ability to reduce or eliminate business risks. Investments in security technologies should be based on their overall value in relation to their cost; the value can be demonstrated in terms of risk mitigation. This should take precedence over whether they use new or exotic technologies or how they are evaluated in trade publications.

40. An organization that has decided to implement a formal information security program 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:

The correct option is D.All four choices are valid steps in the process of implementing a formal information security program; however, defining high-level business security requirements should precede the others because the implementation should be based on those security requirements.

41. Which of the following would be the BEST approach to securing approval for information security expenditures?

○ Developing a business case

○ Conducting a cost-benefit analysis

○ Calculating return on investment (ROI)

○ Evaluating loss history

Call Us Chat Query?

The correct option is A.Justifying and obtaining approval for a security initiative is more likely to be successful if it is supported by a well-developed business case. Choices B, C and D will each be just one typical element of a business case.

42. The FIRST step in developing a business case is to:

○ determine the probability of success.

○ calculate the return on investment (ROI).

○ analyze the cost-effectiveness.

○ define the issues to be addressed.

Explanation:

The correct option is D.Without a clear definition of the issues to be addressed, the other components of a business case cannot be determined.

43. Which of the following would be MOST helpful to achieve alignment between information security and organization objectives?

○ Key control monitoring

○ A robust security awareness program

○ A security program that enables business activities

○ An effective security architecture

Explanation:

The correct option is C.A security program enabling business activities would be most helpful to achieve alignment between information security and organization objectives. All of the other choices are part of the security program and would not individually and directly help as much as the security program.

44. The MOST important requirement for gaining management commitment to the information security program is to:

○ benchmark a number of successful organizations.

○ demonstrate potential losses and other impacts that can result from a lack of support.

○ inform management of the legal requirements of due care.

○ demonstrate support for desired outcomes.

Explanation:

persuasively demonstrate how the program will help achieve the desired outcomes. This can be done by providing specific business support in areas of operational predictability and regulatory compliance, and by improving resource allocation and meaningful performance metrics. While benchmarking similar organizations can be helpful in some instances to make a case for management support of the information security program, benchmarking by itself is not sufficient. Requirements for the exercise of due care should also be covered by the desired outcomes.

45. While implementing information security governance an organization should FIRST:

○ adopt security standards.

○ determine security baselines.

○ [✓ define the security strategy.]

○ establish security policies.

Explanation:

The correct option is C.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.

46. 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:

The correct option is D.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.

47. A regulatory authority has just introduced a new regulation pertaining to the release of quarterly financial results. The FIRST task that the security officer should perform is to:

○ identify whether current controls are adequate.

○ communicate the new requirement to audit.

○ implement the requirements of the new regulation.

Call Us Chat Query?

Explanation:

The correct option is A.If current security practices and procedures already meet the new regulation, then there is no need to implement new controls.

48. Information security should be:

○ focused on eliminating all risks.

○ a balance between technical and business requirements.

○ driven by regulatory requirements.

○ defined by the board of directors.

Explanation:

The correct option is B.Information security should ensure that business objectives are met given available technical capabilities, resource constraints and compliance requirements. It is not practical or feasible to eliminate all risks. Regulatory requirements must be considered, but are inputs to the business considerations. The board of directors does not define information security, but provides direction in support of the business goals and objectives.

49. The MOST complete business case for security solutions is one that:

○ includes appropriate justification.

○ explains the current risk profile.

○ details regulatory requirements.

○ identifies incidents and losses.

Explanation:

The correct option is A.Management is primarily interested in security solutions that can address risks in the most cost-effective way. To address the needs of an organization, a business case should address appropriate security solutions in line with the organizational strategy.

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

○ change management.

○ privacy protection.

○ consent to data transfer.

○ encryption devices.

The correct option is B.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.

---

51. You are a IS Manager recently appointed. You now need to evaluate the data classification in the organization. Who would you talk to?

○ CEO of the company

○ Internal Auditor

○ Data owner

○ Chief Technology Officer

Explanation:

The correct option is C.The data owner is usually a member of management who has due care responsibility and will be held responsible for any neglect.The data custodian is responsible for preserving and protecting data confidentiality, integrity and availability based on the classification requirements assigned by the data owner.

---

52. What would be the BEST outcome for any risk management process?

○ The business operations exceed their performance every year.

○ Reduce risk to an acceptable level

○ External risks are completely removed

○ There are no balance risks

Explanation:

The correct option is B.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 risk. Ensuring business growth via risk management is not practical. Any risk external or internal cannot be completely removed, and there would be residual risk in any organization which must be acceptable to the business.

---

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

○ It used to identify gaps in information security tools.

○ It is used to identify and compare gaps in revenue allocation for information security

○ It is used to identify gaps between performance of your organization with the next best competitor.

○ It is used to measure current state vs. desired future state

Call Us Chat Query?

The correct option is D.A gap analysis is most useful in addressing the differences between the current state and an ideal future state. It is not appropriate for evaluating other choices listed.

54. As an IS Manager, which part of data classification would consider as MOST important?

○ Risk from external sources

○ Risk from internal sources

○ Level of impact from an exposure

○ Only infc ıation classified as confidential

Explanation:

The correct option is C.Level of impact that would occur as a result of exposure is the KEY element to consider for data classification.

55. You are an IS Manager discussing with the IT team of your organization, on implementation project plan of a new application to be rolled out. The IT team feels that as this is a technology based application, business managers or their team members need not be part of the project team. What should you do?

○ Discuss this with the business managers first.

○ Ask for the requirement document to check whether it is really a technology based application.

○ Take it up with the Security Steering committee in the next scheduled meeting.

○ Take this issue with the internal auditors.

Explanation:

The correct option is A.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. Other choices are not appropriate and may delay the project.

56. As an IS Manager, you are considering to upgrade and implement controls to establish a layered protection to your organization. Which is the MOST important consideration?

○ Controls that can be implemented by standard procedures.

○ Controls that can fail in different conditions.

○ Automated controls only

○ Controls that do not display critical messages when they fail.

Explanation:

The correct option is B.Common failure in existing controls must be considered by upgrading or adding controls so that they fail under

Call Us Chat Query?

57. What mechanisms are used to identify weakness or threats that can affect a business critical application?

○ Run an disaster recovery scenario on the affected network.

○ Carry out a comprehensive security gap analysis

○ Carry out a tool based vulnerability assessment

○ Audit the IT Service Desk function

Explanation:

The correct option is B.A security gap analysis can identify weakness of the security controls in place. Ideally this will cover not only the weakness of the technology but also of the process in place.

58. How, as an IS Manager would you test the effectiveness of a control you implemented.

○ The control is very reliable

○ Control has an in-built mechanism for sms facility

○ Control works as planned, and provided the intended results

○ Staff can be easily trained on implementing and using the control.

Explanation:

The correct option is C. Control effectiveness is achieved when control works as intended. Facility for notification does not determine control effectiveness. Reliability is also not an indication of control strength; weak controls can be highly reliable, even if they are ineffective controls.

59. What from the following is NOT true of transfer of risk?

○ Once the risk is transferred, it also removes the responsibility of the risk.

○ Risk is transferred from one party to another party.

○ Transfer of risk is a requirement that can be met by with an insurance contract.

○ Risk transfer is a risk response technique adopted by many organizations.

Explanation:

The correct option is A.Transferring risk is a risk response technique that reduces the impact, but does not eliminate responsibility. Please note that certain risk cannot be transferred.

Call Us Chat Query?

of the following requires your close attention?

○ The Local network is segregated into multiple virtual LANs (VLANs).

○ You are providing remote access to your staff as well as partners.

○ The CEO wants install wireless network in her conference room.

○ Your overseas business partner wants to use VOIP for connectivity

Explanation:

The correct option is C.Of the list, wireless poses the maximum risk if not configured properly. Even if misconfigured, the other choices generally pose less risk.

61. You have initiated a process to identify owners for information assets. Which of the follow would you consider? :

○ Analyze all business processes

○ Study the organization chart of your company.

○ Analyze past and present financial details of the organization and group it by department managers.

○ Analyze the procurement carried out for all information assets by departmental managers

Explanation:

The correct option is A.The starting point for identify asset owners is to study and analyze all business processes. Business process provide input, the process business logic and the corresponding output. It will also provide accountabilities and controls, and hence provides the most accurate picture to assign the ownership of information assets. Other choices does not provide information on asset owners.

62. What is the purpose of vulnerability assessment?

○ Identify all new vulnerabilities

○ Identify trojans and viruses

○ Identify protection mechanism against social engineering

○ Identify weakness in software

Explanation:

The correct option is D.A network vulnerability assessment intends to identify known weaknesses and vulnerabilities in software and tools based on common misconfigurations and missing updates.

Call Us Chat Query?

the organization?

○ Risk analysis process

○ Business impact analysis (BIA)

○ Risk management balanced scorecard

○ Risk-based audit program

Explanation:

The correct option is B.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.

64. You are in a meeting with CEO and the board and discussing implementation of a key control. One of the main agenda points is the investment for the control. What technique would you adopt to get their support?

○ Demonstrate cost-benefit analysis

○ Present reports from the penetration test carried out by an external party.

○ Present a report from Gartner indicating that the supplier of the control is on their niche player quadrant.

○ Present management features, deployment and operation features of the control

Explanation:

The correct option is A.In this scenario, presentation of the cost-benefit analysis can be used to justify investment in a specific control measure.

65. You have completed the risk assessment process of your organization and now are left with residual risks. However, the likelihood and impact of these risks are high. What is the BEST solution?

○ Mitigate the impact by purchasing insurance.

○ Transfer applications to a cloud provider.

○ Implement high end firewalls with redundancy

○ Implement state of the art intrusion detection system

Explanation:

The correct option is A.When residual risk are high, the only practical solution is to purchase insurance. Purchasing insurance is also known as risk transference.

Call Us Chat Query?

66. As an IS Manager you need to determine the criticality and sensitivity of information assets. What would you carry out?

○ Vulnerability assessment.

○ Security assessment which also includes social engineering tactics.

○ Gap analysis

○ Impact assessment.

Explanation:

The correct option is D.The criticality and sensitivity of information assets can be determined by the impact of the probability of the threats exploiting weaknesses in the asset. This also takes into account the asset value.

67. What is the purpose of carrying out a Business impact analysis?

○ Measure the criticality of the business function along with acceptable downtime and resources affected.

○ Calculate the cost of business outages caused by a impact.

○ List all the probable disaster recovery approaches for the organization

○ Prepare the disaster recovery team and its organization chart.

Explanation:

The correct option is A.The main purpose of a BIA is to measure the downtime tolerance, associated resources and criticality of a business function.

68. A business critical system has a requirement to have an account that cannot be automatically locked by the system. What would be the BEST countermeasure to prevent a hacker running a brute force attack on the account.

○ Disallow access to this account.

○ Create a long and a strong random password

○ Isolate the system on a DMZ

○ Enable account logging

Explanation:

The correct option is B.Creating a long and a strong random password is difficult to hack due to the long time it takes to break the account. Access to the account cannot be disallowed as it is business critical. Isolation the system to a DMZ or enabling logging will not prevent an brute force attack.

69. Which of the following would be of GREATEST importance to the security manager in determining whether to further mitigate 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:

The correct option is C.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.

70. 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:

The correct option is A.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 the 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.

71. Security risk assessments are MOST cost-effective to a software development organization when they are performed:

○ before system development begins.

○ at system deployment.

○ before developing a business case.

○ at each stage of the software development life cycle (SDLC).

Explanation:

The correct option is D.Performing risk assessments at each stage of the SDLC is the most cost-effective method because it ensures that vulnerabilities are discovered as soon as possible. A risk assessment performed before system development will not find vulnerabilities

risk. If performed prior to business case development, a risk assessment will not discover risk introduced during the SDLC.

72. What is the TYPICAL output of a risk assessment?

○ A list of appropriate controls for reducing or eliminating risk

○ Documented threats to the organization

○ Evaluation of the consequences to the entity

○ An inventory of risk that may impact the organization

Explanation:

The correct option is D.An inventory of risk is the output of a risk assessment. All other choices contribute to, or are subsequent to, the assessment.

73. Tightly integrated IT systems are MOST likely to be affected by:

○ aggregated risk.

○ systemic risk.

○ operational risk.

○ cascading risk.

Explanation:

74. 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:

The correct option is A.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

Call Us Chat Query?

75. Segregation of duties assists with:

○ employee monitoring.

○ reduced supervisory requirements.

○ fraud prevention.

○ enhanced compliance.

Explanation:

The correct option is C.Segregation of duties is primarily used to discourage fraudulent activities. Employee monitoring and enhanced compliance are secondary considerations. Supervision is not reduced, but facilitated.

76. 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:

The correct option is A.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.

77. An information security manager performing a security review determines that compliance with access control policies to the data center is inconsistent across employees. The FIRST step to address this issue should be to:

○ assess the risk of noncompliance.

○ initiate security awareness training.

○ prepare a status report for management.

○ increase compliance enforcement.

Explanation:

The correct option is A.Inconsistent compliance can be the result of different factors, but is often a lack of awareness. Assessing the risk of noncompliance will provide the information needed to determine the most effective remediation requirements. If awareness is adequate,

the issue that is normally a part of the information security manager's responsibilities. Increased enforcement is not warranted if the problem is a lack of effective communication about security policy.

78. Which of the following steps in conducting a risk assessment should be performed FIRST?

○ Identify business assets

○ Identify business risks

○ Assess vulnerabilities

○ Evaluate key controls

Explanation:

The correct option is A.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.

79. An enterprise is transferring its IT operations to an offshore location. An information security manager should be PRIMARILY concerned about:

○ reviewing new laws and regulations.

○ updating operational procedures.

○ validating staff qualifications.

○ conducting a risk assessment.

Explanation:

The correct option is D.A risk assessment should be conducted to determine new risks introduced by the outsourced processes. The other choices may or may not be identified as mitigating measures based on the risks determined by the assessment.

80. In controlling information leakage, management should FIRST establish:

○ a data leak prevention program.

○ user awareness training.

○ an information classification process.

○ a network intrusion detection system (IDS).

Explanation:

The correct option is C.Information classification must be conducted first. Only after data are determined critical to the organization can a

Call Us Chat Query?

81. 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:

The correct option is A.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.

82. During which phase of development is it MOST appropriate to begin assessing the risk of a new application system?

○ Feasibility

○ Design

○ Development

○ Testing

Explanation:

The correct option is A.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.

83. Which one of the following factors of a risk assessment typically involves the GREATEST amount of speculation?

○ Exposure

○ Impact

○ Vulnerability

○ Likelihood

The correct option is D.The likelihood of a threat encountering a susceptible vulnerability can only be estimated statistically. Exposure, impact and vulnerability can be determined within a range.

84. Which of the following is the MOST important reason to include an effective threat and vulnerability assessment in the change management process?

○ To reduce the need for periodic full risk assessments.

○ To ensure that information security is aware of changes.

○ To ensure that policies are changed to address new threats.

○ To maintain regulatory compliance.

Explanation:

The correct option is A.By assessing threats and vulnerabilities during the change management process, changes in risk can be determined and a risk assessment can be updated incrementally. This keeps the risk assessment current without the need to complete a full reassessment. Information security should have notification processes in place to ensure awareness of changes that might impact security. Policies should rarely require adjustment in response to changes in threats or vulnerabilities. While including an effective threat and vulnerability assessment may assist in maintaining compliance, it is not the primary reason for the change management process.

85. The goals of information security risk management inside an enterprise are BEST achieved if these risk management activities are:

○ treated as a distinct process.

○ conducted by the IT department.

○ integrated within business processes.

○ communicated to all employees.

Explanation:

The correct option is C.Risk management activities are more likely to be executed as part of a business process. The scope of information security risk management encompasses more than IT processes. Communication alone does not necessarily correlate with successful execution of the process.

86. Which of the following is the MOST important requirement for setting up an information security infrastructure for a new system?

○ Performing a business impact analysis (BIA)

○ Considering personal information devices as part of the security policy

○ Initiating IT security training and familiarization

Explanation:

The correct option is D.The information security infrastructure should be based on risk. While considering personal information devices as part of the security policy may be a consideration, it is not the most important requirement. A BIA is typically carried out to prioritize business processes as part of a business continuity plan. Initiating IT security training may not be important for the purpose of the information security infrastructure.

---

87. A permissive controls policy would be reflected in which one of the following implementations?

○ Allows access unless explicitly denied.

○ IT systems are configured to fail closed.

○ Specifies individuals can delegate privileges.

○ Permits control variations with defined limits.

Explanation:

The correct option is A.A permissive controls policy allows activities that are not explicitly denied.

---

88. 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:

The correct option is D.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.

---

89. Which of the following would be the BEST indicator of an asset's value to an organization?

○ Risk assessment

○ Security audit

○ Certification

○ Classification

The correct option is D.Classification is the process of determining criticality and sensitivity of information resources. Assessing the risk to resources will not determine their importance to the business; the classification of an item is needed to properly conduct a risk assessment. Security audits may provide an indication of the importance of particular resources, but will be more focused on risk, vulnerabilities and compliance. Certification is the process of assessing compliance with a standard.

---

90. In which phase of the development process should risk assessment be FIRST introduced?

○ Programming

○ Specification

○ User testing

○ Feasibility

Explanation:

The correct option is D.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.

---

91. 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:

The correct option is C.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.

---

92. Which is the BEST way to measure and prioritize aggregate risk deriving from a chain of linked system vulnerabilities?

○ Vulnerability scans

○ Penetration tests

○ Code reviews

Explanation:

The correct option is B.A penetration test is normally the only security assessment that can link vulnerabilities together by exploiting them sequentially. This gives a good measurement and prioritization of risks. Other security assessments such as vulnerability scans, code reviews and security audits can help give an extensive and thorough risk and vulnerability overview, but will not be able to test or demonstrate the final consequence of having several vulnerabilities linked together. Penetration testing can give risk a new perspective and prioritize based on the end result of a sequence of security problems.

93. 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:

The correct option is B.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.

94. Which of the following is the BEST quantitative indicator of an organization's current risk tolerance?

○ The number of incidents and the subsequent mitigation activities

○ The number, type and layering of deterrent control technologies

○ The extent of risk management requirements in policies and standards

○ The ratio of cost to insurance coverage for business interruption protection

Explanation:

The correct option is D.The cost of a business interruption can be accurately determined. The comparison of this expense (added to any deductible) with the total cost of premiums paid for a specific amount of insurance can serve as an accurate indicator of how much the organization will spend to protect against a defined loss. Incident history can provide only an approximation of the organization's efforts to mitigate further occurrences after consequences have been determined. Incident history may also indicate a lack of risk awareness. Controls deployment can provide a qualitative estimation of risk tolerance as long as technologies are tested and effectiveness is determined. Requirements set in policies and standards can only serve as a qualitative approximation of risk tolerance.

95. Which of the following is the MOST important element to consider when initiating asset classification?

Call Us Chat Query?

○ A comprehensive risk assessment and analysis

○ Business continuity and disaster recovery plans (BCPs/DRPs)

○ The consequences of losing system functionality

Explanation:

The correct option is D.Business criticality and sensitivity is the primary consideration for a classification scheme. This is determined by a business impact analysis (BIA), which will determine the consequences of losing or compromising various information systems. The type of hardware is typically not a classification issue, although it is a factor in incident recovery considerations. Classification is concerned with the loss or compromise of information systems, not the risk they are subject to. Classification is an element of BCP/DRP, but is not required for classification.

---

96. Legal and regulatory requirements pertaining to information security should be addressed by the information security manager:

○ as a mandate that requires organization compliance.

○ based on the level of risk they pose to the organization.

○ by developing policies that address the requirements.

○ to ensure that guidelines meet the requirements.

Explanation:

The correct option is B.Legal and regulatory requirements should be assessed for the risk and impact of non- or partial compliance compared to the cost of compliance and the organization's risk tolerance. There are potentially numerous regulations-including some that are still on the books but obsolete and not enforced or superseded. The result is they must be assessed as to current relevance and potential impact. Policies should not address particular regulations because regulations are subject to change. Policies should only address the need to assess regulatory requirements and deal with them appropriately based on risk, risk tolerance and impact. Guidelines would normally not address regulations, but standards might be based on management's determination of the appropriate level of compliance.

---

97. 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:

The correct option is B.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

Call Us Chat Query?

98. 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:

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.

99. The PRIMARY reason to consider information security during the first stage of a project life cycle is:

○ the cost of security is higher in later stages.

○ information security may affect project feasibility.

○ information security is essential to project approval.

○ it ensures proper project classification.

Explanation:

The correct option is B.Project feasibility can be directly impacted by information security requirements and is the primary reason to introduce information security requirements at this stage. The cost of security must be factored into any business case that will support project feasibility,and sometimes the cost of doing something securely exceeds the benefits that the project is anticipated to produce. Introducing security at later stages can cause projects to exceed budgets and can also create issues with project schedules and delivery dates,but this is generally avoided if security requirements are established in feasibility. Project approval is a business decision that may be influenced by information security considerations, but is not essential. Considering information security during the first stage will not ensure proper project classification. Classification levels are usually determined by the system owner or by the data owner. The levels will normally be influenced by information security, but are not decided by the information security manager.

100. The PRIMARY objective when selecting controls and countermeasures is to:

○ protect against all threats.

○ reduce costs.

○ optimize protection and usability.

○ restrict employee access.

Explanation:

Call Us Chat Query?

not feasible to protect against all threats. Business needs could require more expensive controls. Restriction of employee access may be part of a control, but it is not the objective of a control.

101. Which of the following is the MOST important consideration when developing a service level agreement (SLA) to mitigate the risk that outsourcing will result in a loss to the business?

○ The nature of the indemnity clause

○ Ensuring that the business objectives are defined and met

○ Alignment of information system security objectives with enterprise goals

○ Compliance with legal requirements

Explanation:

The correct option is B.An indemnity clause is not the most important consideration and may not be part of the SLA. An SLA should be designed to deliver and protect the business needs. The security objective is what is being sought by implementing the control. While important,compliance with legal requirements is not generally a primary consideration for SLAs and, in many cases, is not a factor.

102. 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 programmer's activity for review by their supervisor.

○ have the programmer sign a letter accepting full responsibility.

○ perform regular audits of the application.

Explanation:

The correct option is B.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 programmer's 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.

103. Which of the following is the MAIN objective in contracting with an external company to perform penetration testing?

○ To mitigate technical risks

○ To have an independent certification of network security

○ To receive an independent view of security exposures

○ To identify a complete list of vulnerabilities

Call Us Chat Query?

The correct option is C.Even though the organization may have the capability to perform penetration testing with internal resources, third-party penetration testing should be performed to gain an independent view of the security exposure. Mitigating technical risks is not a direct result of a penetration test. A penetration test would not provide certification of network security nor provide a complete list of vulnerabilities.

104. Which of the following is MOST effective in preventing weaknesses from being introduced into existing production systems?

○ Patch management

○ Change management

○ Security baselines

○ Virus detection

Explanation:

The correct option is B.Change management controls the process of introducing changes to systems. This is often the point at which a weakness will be introduced. Patch management involves the correction of software weaknesses and would necessarily follow change management procedures. Security baselines provide minimum recommended settings and do not prevent introduction of control weaknesses.Virus detection is an effective tool but primarily focuses on malicious code from external sources, and only for those applications that are online.

105. Which of the following should be done FIRST when making a decision to allow access to the information processing facility (IPF) of an enterprise to a new external party?

○ A contract language review

○ A risk assessment

○ The exposure factor

○ Vendor due diligence

Explanation:

The correct option is B.A risk assessment identifies the risks involved in allowing access to an external party and the required controls. The other choices could be part of the risk assessment.

106. 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.

Explanation:

The correct option is C.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.

---

107. An organization's information security manager is planning the structure of the Information Security Steering Committee. Which of the following groups should the manager invite?

○ External audit and network penetration testers

○ Board of directors and the organization's regulators

○ External trade union representatives and key security vendors

○ Leadership from IT, human resources and the sales department

Explanation:

The correct option is D.Leaders from IT, human resources and sales are key individuals who must support an information security program. External audit may assess and advise on the program, and testers may be used by the program, but they are not appropriate steering committee members. The steering committee needs to have practitioner-level representation. It may report to the board, but board members would not generally be part of the steering committee, except for its executive sponsor. Regulators would not participate on this committee. External trade union representatives and key security vendors are entities that may need to be consulted as part of program activities, but would not be members of the steering committee.

---

108. Which of the following is the BEST indicator that security awareness training has been effective?

○ Employees sign to acknowledge the security policy

○ More incidents are being reported

○ A majority of employees have completed training

○ No incidents have been reported in three months

Explanation:

The correct option is B.More incidents being reported could be an indicator that the staff is paying more attention to security. Employee signatures and training completion may or may not have anything to do with awareness levels. The number of individuals trained may not indicate they are more aware. No recent security incidents does not reflect awareness levels, but may prompt further research to confirm.

---

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

Call Us Chat Query?

○ Product documentation

○ Available support

○ System overhead

Explanation:

The correct option is D.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.

110. Which of the following would raise security awareness among an organization's employees?

○ Distributing industry statistics about security incidents

○ Monitoring the magnitude of incidents

○ Encouraging employees to behave in a more conscious manner

○ Continually reinforcing the security policy

Explanation:

The correct option is D.Employees must be continually made aware of the policy and expectations of their behavior. Choice A would have little relevant bearing on the employee's behavior. Choice B does not involve the employees. Choice C could be an aspect of continual reinforcement of the security policy.

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:

The correct option is B.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.

112. Which of the following security controls addresses availability?

○ Public key infrastructure

○ Role-based access

○ Contingency planning

Explanation:

The correct option is D.Contingency planning ensures that the system and data are available in the event of a problem. Choices A, B and C are not correct because least privilege is an access control that is concerned with confidentiality, public key infrastructure with confidentiality and integrity, and role-based access with integrity and confidentiality, not integrity alone.

113. Which of the following is an advantage of a centralized information security organizational structure?

○ It is easier to promote security awareness.

○ It is easier to manage and control.

○ It is more responsive to business unit needs.

○ It provides a faster turnaround for security requests.

Explanation:

The correct option is B.It is easier to manage and control a centralized structure. Promoting security awareness is an advantage of decentralization.Decentralization allows you to use field security personnel as security missionaries or ambassadors to spread the security awareness message. Decentralized operations allow security administrators to be more responsive. Being close to the business allows decentralized security administrators to achieve a faster turnaround than that achieved in a centralized operation.

114. Which of the following is the MOST appropriate individual to implement and maintain the level of information security needed for a specific business application?

○ System analyst

○ Quality control manager

○ Process owner

○ Information security manager

Explanation:

The correct option is C.Process owners implement information protection controls as determined by the business' needs. Process owners have the most knowledge about security requirements for the business application for which they are responsible. The system analyst, quality control manager, and information security manager do not possess the necessary knowledge or authority to implement and maintain the appropriate level of business security.

115. The MOST appropriate individual to determine the level of information security needed for a specific business application is the:

Call Us Chat Query?

○ system developer.

○ information security manager.

○ steering committee.

○ system data owner.

Explanation:

The correct option is D.Data owners are the most knowledgeable of the security needs of the business application for which they are responsible. The system developer, security manager and system custodian will have specific knowledge on limited areas but will not have full knowledge of the business issues that affect the level of security required. The steering committee does not perform at that level of detail on the operation.

116. What is the MOST important reason for conducting security awareness programs throughout an organization?

○ Create awareness among people about security implementation

○ Maintaining evidence of training records to ensure compliance

○ Informing business units about the security strategy

○ Training personnel in security incident response

Explanation:

The correct option is A.People are the weakest link in security implementation, and awareness would reduce this risk. Through security awareness and training programs, individual employees can be informed and sensitized on various security policies and other security topics, thus ensuring compliance from each individual. Laws and regulations also aim to reduce human risk. Informing business units about the security strategy is best done through steering committee meetings or other forums.

117. 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:

The correct option is A.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 contingency planning and not to system access. Third-party certification does not provide any assurance of controls over connectivity to maintain continuity.

118. 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:

The correct option is B.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.

119. Which of the following devices should be placed within a DMZ?

○ Router

○ Firewall

○ Mail relay

○ Authentication server

Explanation:

The correct option is C.A mail relay should normally be placed within a demilitarized zone (DMZ) to shield the internal network. An authentication server,due to its sensitivity, should always be placed on the internal network, never on a DMZ that is subject to compromise. Both routers and firewalls may bridge a DMZ to another network, but do not technically reside within the DMZ network segment.

120. 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:

The correct option is D.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 [illegible]

not to alert those responsible for monitoring (other than at the management level), so that the effectiveness of that monitoring can be accurately assessed.

---

121. 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:

The correct option is D.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 of users are all important but are not as effective in preventing this type of situation.

---

122. 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:

The correct option is C.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.

---

123. The effectiveness of virus detection software is MOST dependent on which of the following?

○ Packet filtering

○ Intrusion detection

○ Software upgrades

○ Definition files

Explanation:

The correct option is D.The effectiveness of virus detection software depends on virus signatures which are stored in virus definition files.

Call Us Chat Query?

124. Which of the following is the BEST way to erase confidential information stored on magnetic tapes?

○ Performing a low-level format

○ Rewriting with zeros

○ Burning them

○ Degaussing them

Explanation:

The correct option is D.Degaussing the magnetic tapes would best dispose of confidential information since information is completely destroyed due to the magnetic effect of the degaussing process. Performing a low-level format and rewriting with zeros may still help, but some forensic tools can be used to retrieve information. Rewriting with zeros is dependent on the procedure used. Burning destroys the tapes and does not allow their reuse.

125. The MOST effective technical approach to mitigate the risk of confidential information being disclosed in e-mail attachments is to implement:

○ content filtering.

○ data classification.

○ information security awareness.

○ encryption for all attachments.

Explanation:

The correct option is A.Content filtering provides the ability to examine the content of attachments and prevent information containing certain words or phrases, or of certain identifiable classifications, from being sent out of the enterprise. Data classification helps identify the material that should not be transmitted via e-mail attachments, but by itself will not prevent exposure. Information security awareness training also helps limit confidential material from being disclosed via e-mail as long as personnel are aware of what information should not be exposed and willingly comply with the requirements. Encrypting all attachments is not effective because it does not limit the content and may actually obscure confidential information contained in the e-mail.

126. At what point should a risk assessment of a new process occur to determine appropriate controls? It should occur:

○ only at the beginning and at the end of the new process.

○ during the entire life cycle of the process.

○ at the appropriate point since timing of assessments will differ for processes.

○ depending upon laws and regulations.

Call Us Chat Query?

The correct option is C.A risk assessment should be conducted during the entire life cycle of a new or a changed process. This allows an understanding of how implementation of an early control will affect control needs later on in a process.

---

127. What is the BEST policy for securing data on mobile universal serial bus (USB) drives?

○ Authentication

○ Encryption

○ Prohibit employees from copying data to USB devices

○ Limit the use of USB devices

Explanation:

The correct option is B.Encryption provides the most effective protection of data on mobile devices. Authentication on its own is not very secure. Prohibiting employees from copying data to USB devices and limiting the use of USB devices are after the fact.

---

128. Which of the following is the BEST approach to dealing with inadequate funding of the security program?

○ Eliminate low-priority security services.

○ Require management to accept the increased risk.

○ Prioritize risk mitigation and educate management.

○ Reduce monitoring and compliance enforcement activities.

Explanation:

The correct option is C.Allocating resources to the areas of highest risk and benefit and educating management on the potential consequences of underfunding is the best approach. Prioritizing security activities is always useful, but eliminating even low-priority security services should be a last resort. If budgets are seriously constrained, management is already addressing increases in other risks and is likely to be aware of the issue and a proactive approach to doing more with less will be well received. Reducing monitoring activities may unnecessarily increase risk when lower-cost options to perform those functions may be available.

---

129. 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?

○ Nondisclosure agreement

○ Proper firewall implementation

○ Right to audit

○ Dedicated security manager for monitoring compliance

The correct option is C.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.

---

130. The MOST effective way to ensure network users are aware of their responsibilities to comply with an organization's security requirements is:

○ messages displayed at every logon.

○ periodic security-related e-mail messages.

○ an intranet web site for information security.

○ circulating the information security policy.

Explanation:

The correct option is A.Logon banners would appear every time the user logs on, and the user would be required to read and agree to the same before using the resources. Also, as the message is conveyed in writing and appears consistently, it can be easily enforceable in any organization. Security-related e-mail messages are frequently considered as 'spam' by network users and do not, by themselves, ensure that the user agrees to comply with security requirements. The existence of an intranet web site does not force users to access it and read the information. Circulating the information security policy alone does not confirm that an individual user has read, understood and agreed to comply with its requirements unless it is associated with formal acknowledgment, such as a user's signature of acceptance.

---

131. An enterprise requires the use of Windows XP Service Pack 3 version on all desktops and Windows 2003 Service Pack 1 version on all servers. This is an example of a:

○ policy.

○ guideline.

○ standard.

○ procedure.

Explanation:

The correct option is C.A standard includes required hardware and software mechanisms without describing the settings used in that software. Required operating system software is an example of a standard. A standard sets the minimum requirements for required software or hardware. A guideline is not as mandatory as a standard requirement and is more like a recommendation. Procedures are usually detailed, step-by-step required actions.

---

132. The data backup policy will contain which of the following?

○ Criteria for data backup

○ Personnel responsible for backup

○ A data backup schedule

Call Us Chat Query?

Explanation:

The correct option is A.A policy is a high-level management intent and will essentially contain the criteria to be followed for backing up any data such as critical data, confidential data and project data, and the frequency of backup. Personnel responsible for backup, a data backup schedule and a list of systems to be backed up are procedural details and will not be included in the data backup policy.

133. 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:

The correct option is C.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.

134. 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:

The correct option is A.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.

135. When considering outsourcing services, at what point should information security become involved in the vendor management process?

Call Us Chat Query?

○ Upon request for assistance from the business unit

○ When requirements are being established

○ When a security incident occurs

Explanation:

The correct option is C.Information security should be involved in the vendor or third-party management process from the beginning of the selection process, when the business is defining what it needs. This will ensure that all bids for the service take into consideration, and reflect in bid prices, the security requirements. Waiting until later in the process can lead to vendors having to re-bid and can disrupt negotiations. Waiting until after the contract is signed can expose the enterprise to significant security risk, with little recourse to correct, because the contract has already been executed. There may be situations where information security involvement is not required, but those situations would be established by conducting an initial risk assessment.

136. Which of the following will BEST ensure that management takes ownership of the decision making process for information security?

○ Security policies and procedures

○ Annual self-assessment by management

○ Security steering committees

○ Security awareness campaigns

Explanation:

The correct option is C.Security steering committees provide a forum for management to express its opinion and take ownership in the decision making process. Security awareness campaigns, security policies and procedures, and self-assessment exercises are all good but do not exemplify the taking of ownership by management.

137. 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:

The correct option is B.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 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.

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

○ Tuning

○ Patching

○ Encryption

○ Packet filtering

Explanation:

The correct option is A.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.

139. An information security manager reviewing firewall rules will be MOST concerned if the firewall allows:

○ Expose internal IP

○ echo request on broadcast network

○ unregistered ports.

○ nonstandard protocols.

Explanation:

The correct option is A.If the firewall allows source routing, any outsider can carry out spoofing attacks by stealing the internal (private) IP addresses of the organization. Broadcast propagation, unregistered ports and nonstandard protocols do not create a significant security exposure.

140. 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:

The correct option is A.If there are many firewall rules, there is a chance that a particular rule may allow an external connection although

may occur.

141. Which item would be the BEST to include in the information security awareness training program for new general staff employees?

○ Review of various security models

○ Discussion of how to construct strong passwords

○ Review of roles that have privileged access

○ Discussion of vulnerability assessment results

Explanation:

The correct option is B.All new employees will need to understand techniques for the construction of strong passwords. The other choices would not be applicable to general staff employees.

142. 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:

The correct option is C.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.

143. 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:

The correct option is C.Procedures at the operational level must be developed by or with the involvement of operational units that will use

Call Us Chat Query?

144. 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:

The correct option is A.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 error denying access to a valid user or 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.

145. The BEST way to ensure that security settings on each platform are in compliance with information security policies and procedures is to:

○ perform penetration testing.

○ establish security baselines.

○ implement vendor default settings.

○ link policies to an independent standard.

Explanation:

The correct option is B.Security baselines will provide the best assurance that each platform meets minimum criteria. Penetration testing will not be as effective and can only be performed periodically. Vendor default settings will not necessarily meet the criteria set by the security policies, while linking policies to an independent standard will not provide assurance that the platforms meet these levels of security.

146. 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

Call Us Chat Query?

Explanation:

The correct option is D.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.

147. Several business units reported problems with their systems after multiple security patches were deployed. The FIRST step in handling this problem would be to:

○ assess the problems and institute rollback procedures, if needed.

○ disconnect the systems from the network until the problems are corrected.

○ immediately uninstall the patches from these systems.

○ immediately contact the vendor regarding the problems that occurred.

Explanation:

The correct option is A.Assessing the problems and instituting rollback procedures as needed would be the best course of action. Choices B and C would not identify where the problem was, and may in fact make the problem worse. Choice D is part of the assessment.

148. The organization has decided to outsource the majority of the IT department with a vendor that is hosting servers in a foreign country. Of the following, which is the MOST critical security consideration?

○ Laws and regulations of the country of origin may not be enforceable in the foreign country.

○ A security breach notification might get delayed due to the time difference.

○ Additional network intrusion detection sensors should be installed, resulting in an additional cost.

○ The company could lose physical control over the server and be unable to monitor the physical security posture of the servers.

Explanation:

The correct option is A.A company is held to the local laws and regulations of the country in which the company resides, even if the company decides to place servers with a vendor that hosts the servers in a foreign country. A potential violation of local laws applicable to the company might not be recognized or rectified (i.e., prosecuted) due to the lack of knowledge of the local laws that are applicable and the inability to enforce the laws. Choice B is not a problem. Time difference does not play a role in a 24/7 environment. Pagers, cellular phones, telephones, etc. are usually available to communicate notifications. Choice C is a manageable problem that requires additional funding, but can be addressed. Choice D is a problem that can be addressed. Most hosting providers have standardized the level of physical security that is in place. Regular physical audits or a SAS 70 report can address such concerns.

149. Which of the following is the BEST way to verify that all critical production servers are utilizing up-to-date virus signature files?

○ Use a recently identified benign virus to test if it is quarantined

○ Research the most recent signature file and compare to the console

○ Check a sample of servers that the signature files are current

Explanation:

The correct option is D.The only accurate way to check the signature files is to look at a sample of servers. The fact that an update was pushed out to a server does not guarantee that it was properly loaded onto that server. Checking the vendor information to the management console would still not be indicative as to whether the file was properly loaded on the server. Personnel should never release a virus, no matter how benign.

150. Which of the following is the MOST important element to ensure the successful recovery of a business during a disaster?

○ Detailed technical recovery plans are maintained offsite

○ Network redundancy is maintained through separate providers

○ Hot site equipment needs are recertified on a regular basis

○ Appropriate declaration criteria have been established

Explanation:

The correct option is A.In a major disaster, staff can be injured or can be prevented from traveling to the hot site, so technical skills and business knowledge can be lost. It is therefore critical to maintain an updated copy of the detailed recovery plan at an offsite location.Continuity of the business requires adequate network redundancy, hot site infrastructure that is certified as compatible, and clear criteria for declaring a disaster. Ideally, the business continuity program addresses all of these satisfactorily. However, in a disaster situation, where all these elements are present, but without the detailed technical plan, business recovery will be seriously impaired.

151. 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:

The correct option is C.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.

Call Us Chat Query?

152. Which of the following application systems should have the shortest recovery time objective (RTO)?

○ Contractor payroll

○ Change management

○ E-commerce web site

○ Fixed asset system

Explanation:

The correct option is C.In most businesses where an e-commerce site is in place, it would need to be restored in a matter of hours, if not minutes.Contractor payroll, change management and fixed assets would not require as rapid a recovery time.

153. 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

○ Postincident review

Explanation:

The correct option is D.Postevent 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.

154. The BEST time to determine who should be responsible for declaring a disaster is:

○ during the establishment of the plan.

○ once an incident has been confirmed by operations staff.

○ after fully testing the incident management plan.

○ after the implementation details of the plan have been approved.

Explanation:

The correct option is A.Roles and responsibilities for all involved in incident response should be established when the incident response plan is established. Determining roles and responsibilities during a disaster is not the best time to make such decisions, unless it is absolutely necessary. While testing the plan may drive some changes in roles based on test results, roles (including who declares the disaster) should have been established before testing and plan approval.

○ conducting a business impact assessment.

○ conducting a table-top business continuity test.

○ [✓ selecting an alternate recovery site.]

○ developing disaster recovery metrics.

Explanation:

The correct option is C.Proximity to the primary site, the scope of potential hazards, and their possible impact on the recovery site are important considerations when selecting the location of a recovery site. Proximity to hazards is not a primary consideration in the other choices.

156. Which of the following recovery strategies has the GREATEST chance of failure?

○ Hot site

○ Redundant site

○ [✓ Reciprocal arrangement]

○ Cold site

Explanation:

The correct option is C.A reciprocal arrangement is an agreement that allows two organizations to back up each other during a disaster. This approach sounds desirable, but has the greatest chance of failure due to problems in keeping agreements and plans up to date. A hot site is incorrect because it is a site kept fully equipped with processing capabilities and other services by the vendor. A redundant site is incorrect because it is a site equipped and configured exactly like the primary site. A cold site is incorrect because it is a building having a basic environment such as electrical wiring, air conditioning, flooring, etc. and is ready to receive equipment in order to operate.

157. An organization keeps backup tapes of its servers at a warm site. To ensure that the tapes are properly maintained and usable during a system crash, the MOST appropriate measure the organization should perform is to:

○ use the test equipment in the warm site facility to read the tapes.

○ [✓ periodically retrieve the tapes from the warm site and test them.]

○ have duplicate equipment available at the warm site.

○ inspect the facility and inventory the tapes on a quarterly basis.

Explanation:

The correct option is B.A warm site is not fully equipped with the company's main systems; therefore, the tapes should be periodically tested using the company's production systems. Inspecting the facility and checking the tape inventory does not guarantee that the tapes

Call Us Chat Query?

158. Which of the following is the MOST important element to ensure the success of a disaster recovery test at a vendor-provided hot

○ Tests are scheduled on weekends

○ Network IP addresses are predefined

○ Equipment at the hot site is identical

○ Business management actively participates

Explanation:

The correct option is D.Disaster recovery testing requires the allocation of sufficient resources to be successful. Without the support of management, these resources will not be available, and testing will suffer as a result. Testing on weekends can be advantageous but this is not the most important choice. As vendor-provided hot sites are in a state of constant change, it is not always possible to have network addresses defined in advance. Although it would be ideal to provide for identical equipment at the hot site, this is not always practical as multiple customers must be served and equipment specifications will therefore vary.

159. Which of the following is MOST important when deciding whether to build an alternate facility or subscribe to a third-party hot site?

○ Cost to build a redundant processing facility and invocation

○ Daily cost of losing critical systems and recovery time objectives (RTOs)

○ Infrastructure complexity and system sensitivity

○ Criticality results from the business impact analysis (BIA)

Explanation:

The correct option is C.The complexity and business sensitivity of the processing infrastructure and operations largely determines the viability of such an option; the concern is whether the recovery site meets the operational and security needs of the organization. The cost to build a redundant facility is not relevant since only a fraction of the total processing capacity is considered critical at the time of the disaster and recurring contract costs would accrue over time. Invocation costs are not a factor because they will be the same regardless.The incremental daily cost of losing different systems and the recovery time objectives (RTOs) do not distinguish whether a commercial facility is chosen. Resulting criticality from the business impact analysis (BIA) will determine the scope and timeline of the recovery efforts, regardless of the recovery location.

160. Three employees reported the theft or loss of their laptops while on business trips. The FIRST course of action for the security manager is to:

○ assess the impact of the loss and determine mitigating steps.

○ communicate the best practices in protecting laptops to all laptop users.

○ instruct the erring employees to pay a penalty for the lost laptops.

Call Us Chat Query?

Explanation:

The correct option is A.The first step when addressing theft or loss is to determine what was actually lost and the appropriate response. Choice B may occur after the impact is assessed. Choices C and D depend upon company policy.

161. Which of the following actions should take place immediately after a security breach is reported to an information security manager?

○ Confirm the incident

○ Determine impact

○ Notify affected stakeholders

○ Isolate the incident

Explanation:

The correct option is A.Before performing analysis of impact, resolution, notification or isolation of an incident, it must be validated as a real security incident.

162. At the conclusion of a disaster recovery test, which of the following should ALWAYS be performed prior to leaving the vendor's hot site facility?

○ Erase data and software from devices

○ Conduct a meeting to evaluate the test

○ Complete an assessment of the hot site provider

○ Evaluate the results from all test scripts

Explanation:

The correct option is A.For security and privacy reasons, all organizational data and software should be erased prior to departure. Evaluations can occur back at the office after everyone is rested, and the overall results can be discussed and compared objectively.

163. 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

Call Us Chat Query?

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

164. Which of the following is the MOST effective method to ensure that a business continuity plan (BCP) meets an organization's needs?

○ Require quarterly updating of the BCP.

○ Automate the survey of plan owners to obtain input to the plan.

○ Periodically test the cross-departmental plan with varied scenarios.

○ None of the above.

Explanation:

The correct option is B.Cross-departmental testing of a plan with varied scenarios is most effective in determining the validity of a BCP. Quarterly updates do not establish that a plan meets the organization's needs. Face-to-face meetings and automated surveys are methods that could be used during testing, but on their own are not sufficient.

165. An organization has been experiencing a number of network-based security attacks that all appear to originate internally. The BEST course of action is to:

○ require the use of strong passwords.

○ assign static IP addresses.

○ implement centralized logging software.

○ install an intrusion detection system (IDS).

Explanation:

The correct option is D.Installing an intrusion detection system (IDS) will allow the information security manager to better pinpoint the source of the attack so that countermeasures may then be taken. An IDS is not limited to detection of attacks originating externally. Proper placement of agents on the internal network can be effectively used to detect an internally based attack. Requiring the use of strong passwords will not be sufficiently effective against a network-based attack. Assigning IP addresses would not be effective since these can be spoofed. Implementing centralized logging software will not necessarily provide information on the source of the attack.

166. Which of the following should be performed FIRST in the aftermath of a denial-of-service attack?

○ Restore servers from backup media stored offsite

○ Conduct an assessment to determine system status

○ Perform an impact analysis of the outage

○ Isolate the screened subnet

The correct option is B.An assessment should be conducted to determine whether any permanent damage occurred and the overall system status. It is not necessary at this point to rebuild any servers. An impact analysis of the outage or isolating the demilitarized zone (DMZ) or screen subnet will not provide any immediate benefit.

167. 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:

The correct option is B.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.

168. Establishing severity criteria should be based PRIMARILY on:

○ standards.

○ impact.

○ policies.

○ risk.

Explanation:

The correct option is B.The potential business impact as the result of a specific type of incident should be the primary basis for determining severity criteria.Standards and policies may define some requirements for severity levels, but are not the primary basis for establishing them. Risk associated with particular incidents may affect severity levels, but only insofar as potential impact is concerned.

169. An intrusion detection system (IDS) should:

○ run continuously.

○ ignore anomalies.

○ require a stable, rarely changed environment.

○ be located on the network.

Explanation:

detect, not ignore,anomalies. An IDS should be flexible enough to cope with a changing environment. Both host- and network-based IDSs are recommended for adequate detection.

170. During the recovery process following a natural disaster, a server that hosts an important new customer-facing web service was among the last systems restored, resulting in significant lost sales. Which of the following is the BEST approach to prevent this from happening again?

○ Regularly review and update the business impact analysis (BIA).

○ Improve incident identification methods.

○ Ensure that the sales department has representation on the recovery team.

○ Establish a warm site for recovery purposes.

Explanation:

The correct option is A.The purpose of a BIA is to help stakeholders understand the impact of system downtime to key business processes. This process will help to prioritize the sequence of recovery for primary and supporting systems to meet the most important needs of the business first. Better incident identification would not resolve the issue because incident response without a BIA to reference would not address prioritization. Representation of the sales department on the recovery team does not ensure that the appropriate systems will be restored first, and could actually hinder the process. The establishment of a warm site would ensure that there is a site for recovery purposes, but would not necessarily result in systems being restored in the proper sequence.

171. When electronically stored information is requested during a fraud investigation, which of the following should be the FIRST priority?

○ Assigning responsibility for acquiring the data

○ Locating the data and preserving the integrity of the data

○ Creating a forensically sound image

○ Issuing a litigation hold to all affected parties

Explanation:

The correct option is B.Locating the data and preserving data integrity is the only correct answer because it represents the primary responsibility of an investigator and is a complete and accurate statement of the first priority. While assigning responsibility for acquiring the data is a step that should be taken, it is not the first step or the highest priority. Creating a forensically sound image may or may not be a necessary step, depending on the type of investigation, but it would never be the first priority. Issuing a litigation hold to all affected parties might be a necessary step early on in an investigation of certain types, but not the first priority.

172. The PRIMARY consideration when defining recovery time objectives (RTOs) for information assets is:

○ regulatory requirements.

○ business requirements.

Call Us Chat Query?

○ IT resource availability.

Explanation:

The correct option is B.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.

---

173. When performing a business impact analysis (BIA), which of the following should calculate the recovery time and cost estimates?

○ Business continuity coordinator

○ Information security manager

○ Business process owners

○ IT management

Explanation:

The correct option is C.Business process owners are in the best position to understand the true impact on the business that a system outage would create.The business continuity coordinator, IT management and even the information security manager will not be able to provide that level of detailed knowledge.

---

174. Which of the following is the BEST way to verify that all critical production servers are utilizing up-to-date virus signature files?

○ Verify the date that signature files were last pushed out

○ Use a recently identified benign virus to test if it is quarantined

○ Research the most recent signature file and compare to the console

○ Check a sample of servers that the signature files are current

Explanation:

The correct option is D.The only accurate way to check the signature files is to look at a sample of servers. The fact that an update was pushed out to a server does not guarantee that it was properly loaded onto that server. Checking the vendor information to the management console would still not be indicative as to whether the file was properly loaded on the server. Personnel should never release a virus, no matter how benign.

---

175. The typical requirement for security incidents to be resolved quickly and service restored is:

○ often in conflict with effective problem management.

○ the basis for enterprise risk management (ERM) activities.

○ a component of forensics training.

Explanation:

The correct option is B.Problem management is focused on investigating and uncovering the root cause of incidents, which will often be a problem when restoring service compromises the evidence needed. Quickly restoring service will not always be the best option such as in cases of criminal activity, which requires preservation of evidence precluding use of the systems involved. Managing risk goes beyond the quick restoration of services, e.g., if doing so increased some other risk disproportionately. Forensics is concerned with legally adequate collection and preservation of evidence, not with service continuity.

176. 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:

The correct option is A.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.

177. Which of the following is the MOST important to ensure a successful recovery?

○ Backup media is stored offsite

○ Recovery location is secure and accessible

○ More than one hot site is available

○ Network alternate links are regularly tested

Explanation:

The correct option is A.Unless backup media are available, all other preparations become meaningless. Recovery site location and security are important,but would not prevent recovery in a disaster situation. Having a secondary hot site is also important, but not as important as having backup media available. Similarly, alternate data communication lines should be tested regularly and successfully but, again, this is not as critical.

178. Which of the following is the MOST important aspect of forensic investigations that will potentially

○ The independence of the investigator

○ Timely intervention

○ Identifying the perpetrator

○ Chain of custody

Explanation:

The correct option is D.Establishing the chain of custody is one of the most important steps in conducting forensic investigations since it preserves the evidence in a manner that is admissible in court. The independence of the investigator may be important, but is not the most important aspect. Timely intervention is important for containing incidents, but not as important for forensic investigation. Identifying the perpetrator is important, but maintaining the chain of custody is more important in order to have the perpetrator convicted in court.

179. In a large organization, effective management of security incidents will be MOST dependent on:

○ clear policies detailing incident severity levels.

○ broadly dispersed intrusion detection capabilities.

○ training employees to recognize security incidents.

○ effective communication and reporting processes.

Explanation:

The correct option is D.Timely communication and reporting is most likely to ensure that the information security manager receives the information necessary to effectively manage a security incident. Effective communication will also help ensure that the correct resources are engaged at the appropriate time. Understanding severity levels is important, but on its own is not sufficient to ensure that the information security manager is able to manage the incident effectively. Intrusion detection is useful for detecting potential network security incidents, but without robust communication and reporting processes, the tool is less effective. Conducting awareness training so individuals can recognize potential incidents is important, but not effective unless the information is communicated to the right people in a timely manner.

180. Which of the following is MOST closely associated with a business continuity program?

○ Confirming that detailed technical recovery plans exist

○ Periodically testing network redundancy

○ Updating the hot site equipment configuration every quarter

○ Developing recovery time objectives (RTOs) for critical functions

Explanation:

The correct option is D.Technical recovery plans, network redundancy and equipment needs are all associated with infrastructure disaster recovery. Only recovery time objectives (RTOs) directly relate to business continuity.

181. A new e-mail virus that uses an attachment disguised as a picture file is spreading rapidly over the Internet. Which of the following should be performed FIRST in response to this threat?

○ Quarantine all picture files stored on file servers

○ Block all e-mails containing picture file attachments

○ Quarantine all mail servers connected to the Internet

○ Block incoming Internet mail, but permit outgoing mail

Explanation:

The correct option is B.Until signature files can be updated, incoming e-mail containing picture file attachments should be blocked. Quarantining picture files already stored on file servers is not effective since these files must be intercepted before they are opened. Quarantine of all mail servers or blocking all incoming mail is unnecessary overkill since only those e-mails containing attached picture files are in question.

182. 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:

The correct option is C.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.

183. 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:

The correct option is D.The original media should be used since one can never be sure of all the changes a super-user may have made nor the timeline in which these changes were made. Rebuilding from the last known verified backup is incorrect since the verified backup

Call Us Chat Query?

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.

184. Which of the following should be the PRIMARY basis for making a decision to establish an alternate site for disaster recovery?

○ A business impact analysis (BIA), which identifies the requirements for continuous availability of critical business processes

○ Adequate distance between the primary site and the alternate site so that the same disaster does not simultaneously impact both sites

○ A benchmarking analysis of similarly situated enterprises in the same geographic region to demonstrate due diligence

○ Differences between the regulatory requirements applicable at the primary site and those at the alternate site

Explanation:

The correct option is A.The BIA will help determine the recovery time objective (RTO) and recovery point objective (RPO) for the enterprise. This information will drive the decision on the appropriate level of protection for its assets. Natural disasters and regulatory requirements are just two of many factors that an enterprise must consider when it decides whether to pursue an alternate site for disaster recovery. While a benchmark could provide useful information, the decision should be based on a BIA, which considers factors specific to the enterprise.

185. Why is 'slack space' of value to an information security manager as part 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:

The correct option is A.'Slack space' is the unused space between where the file 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.

186. Which of the following MOST effectively reduces false-positive alerts generated by a security information and event management (SIEM) process?

○ Building use cases

○ Conducting a network traffic analysis

○ Performing an asset-based risk assessment

○ The quality of the logs

The correct option is A.Implementing an SIEM process helps ensure that incidents are correctly identified and handled appropriately. Since an SIEM process depends on log analysis based on predefined rules, the most effective way to reduce false-positive alerts is to develop use cases for known threats to identified critical systems. The use cases would then be used to develop appropriate rules for the SIEM solution. Although security monitoring requires traffic analysis, risk assessment, and quality logs, only properly defined use cases can ensure that the rules are accurately defined and that events are properly identified, thereby reducing false-positive alerts.

187. 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:

The correct option is B.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.

188. When performing a business impact analysis (BIA), which of the following would be the MOST appropriate to calculate the recovery time and cost estimates?

○ Information security manager

○ Information owners

○ Business continuity coordinator

○ Information technology (IT) operations manager

Explanation:

The correct option is B.Information owners are in the best position to understand the true business impact that a specific system outage would create. The other roles listed cannot provide that level of detailed knowledge unless they happen to be the owners of a particular information set.

189. The BEST approach in managing a security incident involving a successful penetration should be to:

○ allow business processes to continue during the response.

○ allow the security team to assess the attack profile.

○ permit the incident to continue to trace the source.

Call Us Chat Query?

Explanation:

The correct option is A.Since information security objectives should always be linked to the objectives of the business, it is imperative that business processes be allowed to continue whenever possible. Only when there is no alternative should these processes be interrupted.Although it is important to allow the security team to assess the characteristics of an attack, this is subordinate to the needs of the business. Permitting an incident to continue may expose the organization to additional damage. Evaluating the incident management process for deficiencies is valuable but it, too, is subordinate to allowing business processes to continue.

190. The PRIMARY purpose of installing an intrusion detection system (IDS) is to identify:

○ weaknesses in network security.

○ patterns of suspicious access.

○ how an attack was launched on the network.

○ potential attacks on the internal network.

Explanation:

The most important function of an intrusion detection system (IDS) is to identify potential attacks on the network. Identifying how the attack was launched is secondary. It is not designed specifically to identify weaknesses in network security or to identify patterns of suspicious logon attempts.

191. Which of the following terms and conditions represent a significant deficiency if included in a commercial hot site contract?

○ A hot site facility will be shared in multiple disaster declarations

○ All equipment is provided 'at time of disaster, not on floor'

○ The facility is subject to a 'first-come, first-served' policy

○ Equipment may be substituted with equivalent models

Explanation:

The correct option is B.Equipment provided 'at time of disaster (ATOD), not on floor' means that the equipment is not available but will be acquired by the commercial hot site provider on a best effort basis. This leaves the customer at the mercy of the marketplace. If equipment is not immediately available, the recovery will be delayed. Many commercial providers do require sharing facilities in cases where there are multiple simultaneous declarations, and that priority may be established on a first-come, first-served basis. It is also common for the provider to substitute equivalent or better equipment, as they are frequently upgrading and changing equipment.

192. A serious vulnerability is reported in the firewall software used by an organization. Which of the following should be the immediate action of the information security manager?

Call Us Chat Query?

○ Block inbound traffic until a suitable solution is found

○ Obtain guidance from the firewall manufacturer

○ Commission a penetration test

Explanation:

The correct option is C.The best source of information is the firewall manufacturer since the manufacturer may have a patch to fix the vulnerability or a workaround solution. Ensuring that all OS patches are up-to-date is a best practice, in general, but will not necessarily address the reported vulnerability. Blocking inbound traffic may not be practical or effective from a business perspective. Commissioning a penetration test will take too much time and will not necessarily provide a solution for corrective actions.

193. The business continuity policy should contain which of the following?

○ Emergency call trees

○ Recovery criteria

○ Business impact assessment (BIA)

○ Critical backups inventory

Explanation:

The correct option is B.Recovery criteria, indicating the circumstances under which specific actions are undertaken, should be contained within a business continuity policy. Telephone trees, business impact assessments (BIAs) and listings of critical backup files are too detailed to include in a policy document.

194. Observations made by staff during a disaster recovery test are PRIMARILY reviewed to:

○ identify people who have not followed the process.

○ determine lessons learned.

○ identify equipment that is needed.

○ maintain evidence of review.

Explanation:

The correct option is B.After a test, results should be reviewed to ensure that lessons learned are applied. It is not the aim of observation to identify people who have not followed the process. Identifying equipment that is needed may be part of the lessons learned, but is not the sole reason for the review. Review is conducted not only to maintain evidence, but to make improvements.

195. When an organization is using an automated tool to manage and house its business continuity plans, which of the following is the PRIMARY concern?,1,

Call Us Chat Query?

○ Versioning control as plans are modified

○ Broken hyperlinks to resources stored elsewhere

○ Tracking changes in personnel and plan assets

Explanation:

The correct option is A.If all of the plans exist only in electronic form, this presents a serious weakness if the electronic version is dependent on restoration of the intranet or other systems that are no longer available. Versioning control and tracking changes in personnel and plan assets is actually easier with an automated system. Broken hyperlinks are a concern, but less serious than plan accessibility.

196. Which of the following should be determined FIRST when establishing a business continuity program?

○ Cost to rebuild information processing facilities

○ Incremental daily cost of the unavailability of systems

○ Location and cost of offsite recovery facilities

○ Composition and mission of individual recovery teams

Explanation:

The correct option is A.If all of the plans exist only in electronic form, this presents a serious weakness if the electronic version is dependent on restoration of the intranet or other systems that are no longer available. Versioning control and tracking changes in personnel and plan assets is actually easier with an automated system. Broken hyperlinks are a concern, but less serious than plan accessibility.

197. The factor that is MOST likely to result in identification of security incidents is:

○ clear policies detailing incident severity levels.

○ intrusion detection system (IDS) capabilities.

○ security awareness training.

Explanation:

The correct option is C.Ensuring that employees have the knowledge to recognize and report a suspected incident is most likely to result in identification of security incidents. Timely communication and reporting is only useful once identification of an incident has occurred. Understanding how to establish severity levels is important, but not the essential element of ensuring that the information security manager is aware of anomalous events that might signal an incident. IDSs are useful for detecting IT-related incidents, but not useful in identifying other types of incidents such as social engineering or physical intrusion.

198. A company has a network of branch offices with local file/print and mail servers; each branch individually contracts a hot site. Which of the following would be the GREATEST weakness in recovery

○ Exclusive use of the hot site is limited to six weeks

○ The hot site may have to be shared with other customers

○ The time of declaration determines site access priority

○ The provider services all major companies in the area

Explanation:

The correct option is D.Sharing a hot site facility is sometimes necessary in the case of a major disaster. Also, first come, first served usually determines priority of access based on general industry practice. Access to a hot site is not indefinite; the recovery plan should address a long-term outage. In case of a disaster affecting a localized geographical area, the vendor's facility and capabilities could be insufficient for all of its clients, which will all be competing for the same resource. Preference will likely be given to the larger corporations, possibly delaying the recovery of a branch that will likely be smaller than other clients based locally.

199. A password hacking tool was used to capture detailed bank account information and personal identification numbers (PINs). Upon confirming the incident, the NEXT step is to:

○ notify law enforcement.

○ start containment.

○ make an image copy of the media.

○ isolate affected servers.

Explanation:

The correct option is B.Once an incident has been confirmed, containment is the first priority of incident response, because it will generally mitigate further impact. Notifying law enforcement, making an image copy of the media and isolating the system should be performed after the containment plan has been executed.

200. Which of the following is the MOST significant risk of using reciprocal agreements for disaster recovery?

○ Both entities are vulnerable to the same threat.

○ The contract contains legal inadequacies.

○ The cultures of the organizations are not compatible.

○ One party has more frequent disruptions.

Explanation:

The correct option is A.The use of reciprocal disaster recovery is based on the hope that both organizations will not suffer a disaster at the same time-which is not always a safe assumption. Inadequate contracts can be a risk, but generally a lesser one. While incompatible cultures can create problems, this is less of a risk than the scenario of both enterprises being impacted by a disaster simultaneously. While one party may utilize the other's resources more frequently, this can be addressed by contractual provisions and is not a major risk.

Call Us Chat Query?

Follow us!

Refer and Earn

Company

About us

Our team

Careers

In the media

Alumni speak

Contact us

Help & support

Work with us

Become an instructor

Blog as guest

Become an affiliate

Discover

Resources

Simplilearn community

Career data labs

RSS feed

For Businesses

Corporate training

Authorised training partner

Learn On the Go!

Get the Android App

Get the iOS App

Terms of Use Privacy Policy Refund Policy Reschedule Policy

Disclaimer

Call Us Chat Query?