QUESTION 1001
A live test of a mutual agreement for IT system recovery has been carried out, including a four-hour test of intensive usage by the business units. The test has been successful, but gives only partial assurance that the:

- system and the IT operations team can sustain operations in the emergency environment.
- Resources and the environment could sustain the transaction load.
- connectivity to the applications at the remote site meets response time requirements.
- workflow of actual business operations can use the emergency system in case of a disaster.

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The applications have been intensively operated, therefore choices B, C, and D have been actually tested. However, the capability of the system and the IT operations team to sustain and support this environment (ancillary operations, batch closing, error corrections, output distribution, etc.) is only partially tested.

QUESTION 1002
To address an organization's disaster recovery requirements, backup intervals should not exceed the:

- **service level objective (SLO).**
- **recovery time objective (RTO).**
- **recovery point objective (RPO).**
- **maximum acceptable outage (MAO).**

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The recovery point objective (RPO) defines the point in time to which data must be restored after a disaster to resume processing transactions. Backups should be performed in a way that the latest backup is no older than this maximum time frame. If service levels are not met, the usual consequences are penalty payments, not cessation of business. Organizations will try to set service level objectives (SLOs) to meet established targets. The recovery time objective (RTO) defines the time period after the disaster in which normal business functionality needs to be restored. The maximum acceptable outage (MAO) is the maximum amount of system downtime that is tolerable.

QUESTION 1003
Which of the following would have the HIGHEST priority in a business continuity plan (BCP)?

- **A. Resuming critical processes**
- **B. Recovering sensitive processes**
- **C. Restoring the site**
- **D. Relocating operations to an alternative site**

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The resumption of critical processes has the highest priority as it enables business processes to begin immediately after the interruption and not later than the declared mean time between failure (MTBF). Recovery of sensitive processes refers to recovering the vital and sensitive processes that can be performed manually at a tolerable cost for an extended period of time. Repairing and restoring the site to original status and resuming the business operations are time-consuming operations and are not the highest priority. Relocating operations to an alternative site, either temporarily or permanently, depending on the interruption, is also a time-consuming process and may not be required.

QUESTION 1004

After completing the business impact analysis (BIA), what is the next step in the business continuity planning process?

- Test and maintain the plan.
- Develop a specific plan.
- Develop recovery strategies.
- Implement the plan.

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The next phase in the continuity plan development is to identify the various recovery strategies and select the most appropriate strategy for recovering from a disaster. After selecting a strategy, a specific plan can be developed, tested, and implemented.

QUESTION 1005
Which of the following is an appropriate test method to apply to a business continuity plan (BCP)?

- Pilot
- Paper
- Unit
- System

Correct Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
A paper test is appropriate for testing a BCP. It is a walkthrough of the entire plan, or part of the plan, involving major players in the plan's execution, who reason out what may happen in a particular disaster. Choices A, C, and D are not appropriate for a BCP.

QUESTION 1006
An IS auditor has audited a business continuity plan (BCP). Which of the following findings is the MOST critical?

- Nonavailability of an alternate private branch exchange (PBX) system
- Absence of a backup for the network backbone
- Lack of backup systems for the users' PCs
- Failure of the access card system

Correct Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Failure of a network backbone will result in the failure of the complete network and impact the ability of all users to access information on the network. The nonavailability of an alternate PBX system will result in users not being able to make or receive telephone calls or faxes; however, users may have alternate means of communication, such as a mobile phone or email. Lack of backup systems for user PCs will impact only the specific users, not all users. Failure of the access card system impacts the ability to maintain records of the users who are entering the specified work areas; however, this could be mitigated by manual monitoring controls.

QUESTION 1007
As part of the business continuity planning process, which of the following should be identified FIRST in the business impact analysis?

- Organizational risks, such as single point-of-failure and infrastructure risk
- Threats to critical business processes
- Critical business processes for ascertaining the priority for recovery
- Resources required for resumption of business

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:
The identification of the priority for recovering critical business processes should be addressed first. Organizational risks should be identified next, followed by the identification of threats to critical business processes. Identification of resources for business resumption will occur after the tasks mentioned.

QUESTION 1008
Which of the following activities should the business continuity manager perform FIRST after the replacement of hardware at the primary information processing facility?

- Verify compatibility with the hot site.
- Review the implementation report.
- Perform a walk-through of the disaster recovery plan.
- Update the IS assets inventory.

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
An IS assets inventory is the basic input for the business continuity/disaster recovery plan, and the plan must be updated to reflect changes in the IS infrastructure. The other choices are procedures required to update the disaster recovery plan after updating the required assets inventory.

QUESTION 1009
Which of the following would contribute MOST to an effective business continuity plan (BCP)?

- Document is circulated to all interested parties
- Planning involves all user departments
- Approval by senior management
- Audit by an external IS auditor

Correct Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The involvement of user departments in the BCP is crucial for the identification of the business processing priorities. The BCP circulation will ensure that the BCP document is received by all users. Though essential, this does not contribute significantly to the success of the BCP. A BCP approved by senior management would not ensure the quality of the BCP, nor would an audit necessarily improve the quality of the BCP.

QUESTION 1010
To develop a successful business continuity plan, end user involvement is critical during which of the following phases?

- Business recovery strategy
- Detailed plan development
- Business impact analysis (BIA)
- Testing and maintenance

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
End user involvement is critical in the BIA phase. During this phase, the current operations of the business need to be understood, and the impact on the business of various disasters must be evaluated. End users are the appropriate persons to provide relevant information for these tasks. Inadequate end user involvement in this stage could result in an inadequate understanding of business priorities and the plan not meeting the requirements of the organization.

QUESTION 1011
Question: Which of the following would an IS auditor consider to be the MOST important to review

when conducting a business continuity audit?

Options:

- A. A hot site is contracted for and available as needed.
- B. A business continuity manual is available and current.
- C. Insurance coverage is adequate and premiums are current.
- D. Media backups are performed on a timely basis and stored offsite.

Answer: D

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

Without data to process, all other components of the recovery effort are in vain. Even in the absence of a plan, recovery efforts of any type would not be practical without data to process.

Additional Clarification:

Timely and offsite backups are essential in any disaster recovery scenario. If the data isn't backed up and stored in a secure, offsite location, the business cannot recover effectively, rendering other continuity measures such as a hot site or insurance irrelevant.

QUESTION 1012

Question: The PRIMARY objective of business continuity and disaster recovery plans should be to:

Options:

- A. Safeguard critical IS assets.
- B. Provide for continuity of operations.
- C. Minimize the loss to an organization.
- D. Protect human life.

Answer: D

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

Since human life is invaluable, the main priority of any business continuity and disaster recovery plan should be to protect people. All other priorities are important but are secondary objectives of a business continuity and disaster recovery plan.

Additional Clarification:

Protecting human life in disaster scenarios is always the first concern, as no business operation is worthwhile if people's safety is compromised. Once human life is safeguarded, other priorities like protecting IS assets and minimizing operational losses become the focus.

QUESTION 1013

After a full operational contingency test, an IS auditor performs a review of the recovery steps. The auditor concludes that the time it took for the technological environment and systems to return to full-functioning exceeded the required critical recovery time. Which of the following should the auditor recommend?

Options:

- A. Perform an integral review of the recovery tasks.
- B. Broaden the processing capacity to gain recovery time.
- C. Make improvements in the facility's circulation structure.
- D. Increase the amount of human resources involved in the recovery.

Answer: A

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

Performing an exhaustive review of the recovery tasks would be appropriate to identify how the tasks were performed, identify the time allocated to each step, and determine where adjustments can be made. Choices B, C, and D could be actions after the review.

Additional Clarification:

An integral review helps pinpoint bottlenecks or inefficiencies in the recovery process. Broader processing

capacity or additional human resources may be part of the solution, but a detailed review is necessary to understand the root cause of the delay.

QUESTION 1014
Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?
Options:
- A. Paper test.
- B. Post-test.
- C. Preparedness test.
- D. Walkthrough.

Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
A preparedness test is a localized version of a full test, simulating a system crash to gather evidence about the plan's effectiveness. It is a cost-effective method to gradually assess and improve the plan. A paper test is a walkthrough of the plan, usually performed before a preparedness test.
Additional Clarification:
The preparedness test allows you to test actual systems and processes without fully committing to a full-scale disaster recovery, making it a low-cost method for evaluating the effectiveness of the business continuity plan.

QUESTION 1015
While designing the business continuity plan (BCP) for an airline reservation system, the MOST appropriate method of data transfer/backup at an offsite location would be:
Options:
- A. Shadow file processing.
- B. Electronic vaulting.
- C. Hard-disk mirroring.
- D. Hot-site provisioning.

Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Shadow file processing involves maintaining exact duplicates of files, processed concurrently at the same or remote site. This is most appropriate for critical data, like airline booking systems. Other options are used for backup in different contexts but do not fit the needs of airline reservation data.
Additional Clarification:
Shadow file processing ensures that a real-time, identical copy of the data is maintained, which is crucial for high-availability systems like airline reservations, where data integrity and instant recovery are paramount.

QUESTION 1016
Depending on the complexity of an organization's business continuity plan (BCP), the plan may be developed as a set of more than one plan to address various aspects of business continuity and disaster recovery. In such an environment, it is essential that:
Options:
- A. Each plan is consistent with one another.
- B. All plans are integrated into a single plan.
- C. Each plan is dependent on one another.
- D. The sequence for implementation of all plans is defined.

Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:
In complex organizations, there may be more than one plan for various aspects of business continuity and disaster recovery. These plans need to be consistent with each other, ensuring that recovery efforts align effectively, even if the plans are not fully integrated into one document.
Additional Clarification:
Having multiple plans does not mean they should be integrated into a single plan, but consistency across them is crucial to avoid conflicts or gaps. This ensures a smooth, coordinated response during a crisis.

QUESTION 1017
During a business continuity audit, an IS auditor found that the business continuity plan (BCP) covered only critical processes. The IS auditor should:
Options:
- A. Recommend that the BCP cover all business processes.
- B. Assess the impact of the processes not covered.
- C. Report the findings to the IT manager.
- D. Redefine critical processes.

Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The auditor should assess the impact of the processes not covered by the BCP. It may not be cost-effective or necessary to include all processes, so an analysis of risk and cost should be conducted to make a decision.
Additional Clarification:
Not every process needs to be covered in the business continuity plan. By assessing the impact of missing processes, the auditor can determine whether the coverage is sufficient or whether adjustments are needed.

QUESTION 1018
An IS auditor noted that an organization had adequate business continuity plans (BCPs) for each individual process, but no comprehensive BCP. Which would be the BEST course of action for the IS auditor?
Options:
- A. Recommend that an additional comprehensive BCP be developed.
- B. Determine whether the BCPs are consistent.
- C. Accept the BCPs as written.
- D. Recommend the creation of a single BCP.

Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The IS auditor should check whether the individual BCPs are consistent. While it may not be necessary to have one comprehensive plan, all BCPs should align to form a coherent strategy that ensures the recovery of the business in a disaster.
Additional Clarification:
Multiple individual plans can be effective if they are consistent and work together seamlessly. The auditor should focus on ensuring alignment and integration rather than necessarily recommending the creation of a single plan.

QUESTION 1019
When developing a business continuity plan (BCP), which of the following tools should be used to gain an understanding of the organization's business processes?
Options:
- A. Business continuity self-audit.
- B. Resource recovery analysis.

- C. Risk assessment.
- D. Gap analysis.

Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
A risk assessment is crucial for understanding an organization's business processes as it helps identify potential threats and vulnerabilities to critical operations. The other options are tools for evaluating and improving plans once the business processes are understood.
Additional Clarification:
The risk assessment evaluates the organization's vulnerabilities, enabling the BCP team to prioritize and address the most critical risks, which is essential for effective continuity planning.

QUESTION 1020
During an audit of a business continuity plan (BCP), an IS auditor found that, although all departments were housed in the same building, each department had a separate BCP. The IS auditor recommended that the BCPs be reconciled. Which of the following areas should be reconciled FIRST?
Options:
- A. Evacuation plan.
- B. Recovery priorities.
- C. Backup storages.
- D. Call tree.

Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The first priority is to reconcile evacuation plans. In case of a disaster, conflicting evacuation plans across departments could jeopardize the safety of staff and clients. Other areas such as recovery priorities and backup storage should be reconciled after addressing safety concerns.
Additional Clarification:
Safety should always come first. Once the evacuation plans are aligned, it is safe to proceed with aligning recovery priorities, storage, and communication plans across departments.

QUESTION 1021
Management considered two projections for its business continuity plan; plan A with two months to recover and plan B with eight months to recover. The recovery objectives are the same in both plans. It is reasonable to expect that plan B projected higher:
Options:
- A. Downtime costs.
- B. Resumption costs.
- C. Recovery costs.
- D. Walkthrough costs.

Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Since the recovery time is longer in plan B, resumption and recovery costs can be expected to be lower. Walkthrough costs are not a part of disaster recovery.
Since the management considered a higher window for recovery in plan B, downtime costs included in the plan are likely to be higher.

QUESTION 1022
The optimum business continuity strategy for an entity is determined by the:
Options:

- A. Lowest downtime cost and highest recovery cost.
- B. Lowest sum of downtime cost and recovery cost.
- C. Lowest recovery cost and highest downtime cost.
- D. Average of the combined downtime and recovery cost.

Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Both costs have to be minimized, and the strategy for which the costs are lowest is the optimum strategy. The strategy with the highest recovery cost cannot be the optimum strategy. The strategy with the highest downtime cost cannot be the optimum strategy. The average of the combined downtime and recovery cost will be higher than the lowest combined cost of downtime and recovery.

QUESTION 1023
The PRIMARY objective of testing a business continuity plan is to:
Options:
- A. Familiarize employees with the business continuity plan.
- B. Ensure that all residual risks are addressed.
- C. Exercise all possible disaster scenarios.
- D. Identify limitations of the business continuity plan.

Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Testing the business continuity plan provides the best evidence of any limitations that may exist. Familiarizing employees with the business continuity plan is a secondary benefit of a test. It is not cost-effective to address residual risks in a business continuity plan, and it is not practical to test all possible disaster scenarios.

QUESTION 1024
In determining the acceptable time period for the resumption of critical business processes:
Options:
- A. Only downtime costs need to be considered.
- B. Recovery operations should be analyzed.
- C. Both downtime costs and recovery costs need to be evaluated.
- D. Indirect downtime costs should be ignored.

Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Both downtime costs and recovery costs need to be evaluated in determining the acceptable time period before the resumption of critical business processes. The outcome of the business impact analysis (BIA) should be a recovery strategy that represents the optimal balance. Downtime costs cannot be looked at in isolation. The quicker information assets can be restored and business processing resumed, the smaller the downtime costs. However, the expenditure needed to have the redundant capability required to recover information resources might be prohibitive for nonessential business processes. Recovery operations do not determine the acceptable time period for the resumption of critical business processes, and indirect downtime costs should be considered in addition to the direct cash outflows incurred due to business disruption. The indirect costs of a serious disruption to normal business activity, e.g., loss of customer and supplier goodwill and loss of market share, may actually be more significant than direct costs over time, thus reaching the point where business viability is threatened.

QUESTION 1025
In the event of a disruption or disaster, which of the following technologies provides for continuous operations?
Options:

- A. Load balancing
- B. Fault-tolerant hardware
- C. Distributed backups
- D. High-availability computing

Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Fault-tolerant hardware is the only technology that currently supports continuous, uninterrupted service. Load balancing is used to improve the performance of the server by splitting the work between several servers based on workloads. High-availability (HA) computing facilities provide a quick but not continuous recovery, while distributed backups require longer recovery times.

QUESTION 1026
Which of the following would be MOST important for an IS auditor to verify when conducting a business continuity audit?
Options:
- A. Data backups are performed on a timely basis
- B. A recovery site is contracted for and available as needed
- C. Human safety procedures are in place
- D. Insurance coverage is adequate and premiums are current

Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The most important element in any business continuity process is the protection of human life. This takes precedence over all other aspects of the plan.

QUESTION 1027
Which of the following insurance types provide for a loss arising from fraudulent acts by employees?
Options:
- A. Business interruption
- B. Fidelity coverage
- C. Errors and omissions
- D. Extra expense

Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Fidelity insurance covers the loss arising from dishonest or fraudulent acts by employees. Business interruption insurance covers the loss of profit due to the disruption in the operations of an organization. Errors and omissions insurance provides legal liability protection in the event that the professional practitioner commits an act that results in financial loss to a client. Extra expense insurance is designed to cover the extra costs of continuing operations following a disaster/ disruption within an organization.

QUESTION 1028
The BEST method for assessing the effectiveness of a business continuity plan is to review the:
Options:
- A. Plans and compare them to appropriate standards.
- B. Results from previous tests.
- C. Emergency procedures and employee training.
- D. Offsite storage and environmental controls.

Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Previous test results will provide evidence of the effectiveness of the business continuity plan.

Comparisons to standards will give some assurance that the plan addresses the critical aspects of a business continuity plan but will not reveal anything about its effectiveness. Reviewing emergency procedures, offsite storage and environmental controls would provide insight into some aspects of the plan but would fall short of providing assurance of the plan's overall effectiveness.

QUESTION 1029
With respect to business continuity strategies, an IS auditor interviews key stakeholders in an organization to determine whether they understand their roles and responsibilities. The IS auditor is attempting to evaluate the:
Options:
- A. Clarity and simplicity of the business continuity plans.
- B. Adequacy of the business continuity plans.
- C. Effectiveness of the business continuity plans.
- D. Ability of IS and end-user personnel to respond effectively in emergencies.

Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The IS auditor should interview key stakeholders to evaluate how well they understand their roles and responsibilities. When all stakeholders have a detailed understanding of their roles and responsibilities in the event of a disaster, an IS auditor can deem the business continuity plan to be clear and simple. To evaluate adequacy, the IS auditor should review the plans and compare them to appropriate standards. To evaluate effectiveness, the IS auditor should review the results from previous tests. This is the best determination for the evaluation of effectiveness. An understanding of roles and responsibilities by key stakeholders will assist in ensuring the business continuity plan is effective. To evaluate the response, the IS auditor should review results of continuity tests. This will provide the IS auditor with assurance that target and recovery times are met. Emergency procedures and employee training need to be reviewed to determine whether the organization had implemented plans to allow for the effective response.

QUESTION 1030
During the design of a business continuity plan, the business impact analysis (BIA) identifies critical processes and supporting applications. This will PRIMARILY influence the:
Options:
- A. Responsibility for maintaining the business continuity plan.
- B. Criteria for selecting a recovery site provider.
- C. Recovery strategy.
- D. Responsibilities of key personnel.

Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The most appropriate strategy is selected based on the relative risk level and criticality identified in the business impact analysis (BIA). The other choices are made after the selection or design of the appropriate recovery strategy.

QUESTION 1031
During a review of a business continuity plan, an IS auditor noticed that the point at which a situation is declared to be a crisis has not been defined. The MAJOR risk associated with this is that:
Options:
- A. Assessment of the situation may be delayed.
- B. Execution of the disaster recovery plan could be impacted.
- C. Notification of the teams might not occur.
- D. Potential crisis recognition might be ineffective.

Correct Answer: B

Topic: Risk of Undefined Crisis Declaration in Business Continuity Plan
Answer Explanation:
Execution of the business continuity plan would be impacted if the organization does not know when to declare a crisis. Choices A, C, and D are steps that must be performed to know whether to declare a crisis. Problem and severity assessment would provide information necessary in declaring a disaster. Once a potential crisis is recognized, the teams responsible for crisis management need to be notified. Delaying this step until a disaster has been declared would negate the effect of having response teams. Potential crisis recognition is the first step in responding to a disaster.

QUESTION 1032
An organization has just completed their annual risk assessment. Regarding the business continuity plan, what should an IS auditor recommend as the next step for the organization?
Options:
- A. Review and evaluate the business continuity plan for adequacy
- B. Perform a full simulation of the business continuity plan
- C. Train and educate employees regarding the business continuity plan
- D. Notify critical contacts in the business continuity plan

Correct Answer: A
Topic: Post-Risk Assessment Actions for Business Continuity Plan
Answer Explanation:
The business continuity plan should be reviewed every time a risk assessment is completed for the organization. Training of the employees and a simulation should be performed after the business continuity plan has been deemed adequate for the organization. There is no reason to notify the business continuity plan contacts at this time.

QUESTION 1033
Integrating business continuity planning (BCP) into an IT project aids in:
Options:
- A. The retrofitting of the business continuity requirements.
- B. The development of a more comprehensive set of requirements.
- C. The development of a transaction flowchart.
- D. Ensuring the application meets the user's needs.

Correct Answer: B
Topic: Benefits of Integrating BCP in IT Project Development
Answer Explanation:
Integrating business continuity planning (BCP) into the development process ensures complete coverage of the requirements through each phase of the project. Retrofitting of the business continuity plan's requirements occurs when BCP is not integrated into the development methodology. Transaction flowcharts aid in analyzing an application's controls. A business continuity plan will not directly address the detailed processing needs of the users.

QUESTION 1034
While observing a full simulation of the business continuity plan, an IS auditor notices that the notification systems within the organizational facilities could be severely impacted by infrastructural damage. The BEST recommendation the IS auditor can provide to the organization is to ensure:
Options:
- The salvage team is trained to use the notification system.
- The notification system provides for the recovery of the backup.
- Redundancies are built into the notification system.
- The notification systems are stored in a vault.

Correct Answer: C
Topic: Redundancy in Notification Systems for Business Continuity

Answer Explanation:
If the notification system has been severely impacted by damage, redundancy is the best control. The salvage team would not be able to use a severely damaged notification system even if they are trained to use it. Recovery of the backups is unrelated to the notification system, and storing the notification system in a vault would be ineffective if the building is damaged.

QUESTION 1035
The activation of an enterprise's business continuity plan should be based on predetermined criteria that address the:
Options:
- A. Duration of the outage.
- B. Type of outage.
- C. Probability of the outage.
- D. Cause of the outage.

Correct Answer: A
Topic: Criteria for Activating Business Continuity Plan
Answer Explanation:
The initiation of a business continuity plan should primarily be based on the maximum period a business function can be disrupted before threatening organizational objectives.

QUESTION 1036
An organization has outsourced its wide area network (WAN) to a third-party service provider. Under these circumstances, which of the following is the PRIMARY task the IS auditor should perform during an audit of business continuity (BCP) and disaster recovery planning (DRP)?
Options:
- A. Review whether the service provider's BCP process aligns with the organization's BCP and contractual obligations.
- B. Review whether the service level agreement (SLA) contains a penalty clause in case of failure to meet service levels during a disaster.
- C. Review the methodology adopted by the organization in choosing the service provider.
- D. Review the accreditation of the third-party service provider's staff.

Correct Answer: A
Topic: Ensuring Third-Party Alignment in Business Continuity and DRP
Answer Explanation:
The IS auditor should ensure that the service provider's BCP aligns with the organization’s BCP and contractual obligations, as disruptions to the provider directly impact the organization. Reviewing penalty clauses in the SLA and other choices are of secondary importance.

QUESTION 1037
An IS auditor can verify that an organization's business continuity plan (BCP) is effective by reviewing the:
Options:
- A. Alignment of the BCP with industry best practices.
- B. Results of business continuity tests performed by IS and end-user personnel.
- C. Off-site facility, its contents, security, and environmental controls.
- D. Annual financial cost of BCP activities versus expected benefits.

Correct Answer: B
Topic: Verifying Effectiveness of Business Continuity Plan
Answer Explanation:
The effectiveness of the BCP is best evaluated by reviewing results from previous tests for thoroughness

and accuracy in achieving objectives. Other choices do not provide adequate assurance of BCP effectiveness.

QUESTION 1038
To optimize an organization's business contingency plan (BCP), an IS auditor should recommend conducting a business impact analysis (BIA) to determine:
Options:
- A. Business processes generating the most financial value for recovery prioritization.
- B. Priorities and order for recovery to align with business strategy.
- C. Critical business processes to recover after a disaster to ensure survival.
- D. Priorities and recovery order for greatest system recovery in the shortest time.

Correct Answer: C
Topic: Conducting Business Impact Analysis for Critical Recovery Needs
Answer Explanation:
To ensure survival after a disaster, the BIA should focus on recovering critical business processes first, which is more urgent than focusing on financial value alone. Choices B and D emphasize strategy alignment and system recovery speed, which are secondary to the critical process recovery necessary for survival.

QUESTION 1039
A financial services organization is developing and documenting business continuity measures. In which of the following cases would an IS auditor MOST likely raise an issue?
Options:
- A. The organization uses good practice guidelines instead of industry standards and relies on external advisors to ensure the adequacy of the methodology.
- B. The business continuity capabilities are planned around a carefully selected set of scenarios which describe events that might happen with a reasonable probability.
- C. The recovery time objectives (RTOs) do not take IT disaster recovery constraints into account, such as personnel or system dependencies during the recovery phase.
- D. The organization plans to rent a shared alternate site with emergency workplaces which has only enough room for half of the normal staff.

Correct Answer: B
Topic: Scenario Planning in Business Continuity
Answer Explanation:
Using scenario planning for business continuity is risky because it is impractical to plan for every possible scenario. Planning around a few selected scenarios ignores the possibility of low-probability events that could significantly disrupt operations. Best practices focus on addressing four primary impact areas—premises, people, systems, and suppliers—rather than scenario-specific planning. Using good practice guidelines, considering IT constraints in RTOs, and having 50% capacity at an alternate site are generally acceptable practices in business continuity planning.

QUESTION 1040
A medium-sized organization, whose IT disaster recovery measures have been in place and regularly tested for years, has just developed a formal business continuity plan (BCP). A basic BCP tabletop exercise has been performed successfully. Which testing should an IS auditor recommend be performed NEXT to verify the adequacy of the new BCP?
Options:
- A. Full-scale test with relocation of all departments, including IT, to the contingency site.
- B. Walk-through test of a series of predefined scenarios with all critical personnel involved.
- C. IT disaster recovery test with business departments involved in testing the critical applications.
- D. Functional test of a scenario with limited IT involvement.

Correct Answer: D
Topic: Testing Stages for Business Continuity Plans

Answer Explanation:
After a successful tabletop exercise, the next step would be a functional test that includes mobilizing staff to exercise the administrative and organizational functions of recovery, with minimal IT involvement. Since the IT disaster recovery measures have been in place and tested, a full-scale test may waste resources. A walk-through test is too basic at this stage, and an IT disaster recovery test alone does not verify the non-IT components of the BCP.

QUESTION 1041
Question: Everything not explicitly permitted is forbidden has which of the following kinds of tradeoff?
Options:

- A. It improves security at a cost in functionality.
- B. It improves functionality at a cost in security.
- C. It improves security at a cost in system performance.
- D. It improves performance at a cost in functionality.
- E. None of the choices.

Correct Answer: A
Topic: Default Deny Approach
Answer Explanation:
The "default deny" approach ("everything not explicitly permitted is forbidden") enhances security by limiting functionality, only allowing necessary operations to proceed. This approach is ideal when there are significant security threats. Conversely, a "default permit" approach, which allows anything not explicitly forbidden, provides more functionality but less security.

QUESTION 1042
Default permit is only a good approach in an environment where:
Options:

- A. Security threats are non-existent or negligible.
- B. Security threats are non-negligible.
- C. Security threats are serious and severe.
- D. Users are trained.
- E. None of the choices.

Correct Answer: A
Topic: Default Permit Approach
Answer Explanation:
The "default permit" approach is suitable only in environments with minimal or no security threats, as it allows actions unless explicitly forbidden, potentially leaving the system vulnerable.

QUESTION 1043
Talking about the different approaches to security in computing, the principle of regarding the computer system itself as largely an untrusted system emphasizes:
Options:

- A. Most privilege
- B. Full privilege
- C. Least privilege
- D. Null privilege
- E. None of the choices.

Correct Answer: C
Topic: Least Privilege Principle
Answer Explanation:
Viewing the system as largely untrusted aligns with the principle of least privilege, where each user or process is given the minimum privileges necessary for their function, reducing the risk of internal threats.

QUESTION 1044
Which of the following refers to the proving of mathematical theorems by a computer program?
Options:
- A. Analytical theorem proving
- B. Automated technology proving
- C. Automated theorem processing
- D. Automated theorem proving
- E. None of the choices.

Correct Answer: D
Topic: Automated Theorem Proving
Answer Explanation:
Automated theorem proving (ATP) involves using computer programs to prove mathematical theorems. It has applications in integrated circuit design and verification, where logic and proofs are essential.

QUESTION 1045
Which of the following BEST describes the concept of "defense in depth"?
Options:
- A. More than one subsystem needs to be compromised to compromise the security of the system and the information it holds.
- B. Multiple firewalls are implemented.
- C. Multiple firewalls and multiple network OS are implemented.
- D. Intrusion detection and firewall filtering are required.
- E. None of the choices.

Correct Answer: A
Topic: Defense in Depth
Answer Explanation:
Defense in depth involves having multiple layers of security controls, meaning that compromising a single layer isn't enough to breach the overall security. This strategy ensures a more resilient and secure system.

QUESTION 1046
Under the concept of "defense in depth," subsystems should be designed to:
Options:
- A. "Fail insecure"
- B. "Fail secure"
- C. "React to attack"
- D. "React to failure"
- E. None of the choices.

Correct Answer: B
Topic: Fail-Secure Design
Answer Explanation:
Subsystems within a defense-in-depth strategy should be designed to "fail secure," ensuring that in case of a failure, the system remains in a secure state and does not expose vulnerabilities.

QUESTION 1047
Security should ALWAYS be an all or nothing issue.
Options:
- A. True
- B. True for trusted systems only
- C. True for untrusted systems only
- D. False
- E. None of the choices.

Correct Answer: D

Topic: Security Gradation
Answer Explanation:
Security should not be an all-or-nothing concept. Systems should maintain audit trails and assume that breaches are possible, allowing the extent and cause of a breach to be analyzed for future improvements.

QUESTION 1048
Question: The 'trusted systems' approach has been predominant in the design of:
Options:
- A. Many earlier Microsoft OS products
- B. The IBM AS/400 series
- C. The SUN Solaris series
- D. Most OS products in the market
- E. None of the choices.

Correct Answer: A
Topic: Trusted Systems Approach
Answer Explanation:
The trusted systems approach, focusing on functionality and ease of use, has been common in Microsoft OS products, often favoring usability over stringent security controls.

QUESTION 1049
Question: Which of the following terms generally refers to small programs designed to take advantage of a software flaw that has been discovered?
Options:
- A. Exploit
- B. Patch
- C. Quick fix
- D. Service pack
- E. Malware

Correct Answer: A
Topic: Exploit Programs
Answer Explanation:
An "exploit" is a small program that takes advantage of a discovered vulnerability. Exploits are frequently reused in malware like trojans and viruses to attack systems.

QUESTION 1050
Codes from exploit programs are frequently reused in:
Options:
- A. Trojan horses only
- B. Computer viruses only
- C. OS patchers
- D. Eavesdroppers
- E. Trojan horses and computer viruses

Correct Answer: E
Topic: Exploit Code Usage
Answer Explanation:
Exploit code is often reused in both trojan horses and computer viruses, as it provides a means to leverage vulnerabilities, making these types of malware more effective at compromising systems.

QUESTION 1051
Question: Machines that operate as a closed system can NEVER be eavesdropped.
Options:
- A. True
- B. False

Correct Answer: B
Topic: Closed System Security Risks
Answer Explanation:
Closed systems are not immune to eavesdropping. Even without direct network access, electromagnetic emissions from hardware (such as TEMPEST vulnerabilities) can be intercepted by attackers using specialized equipment, exposing the system to potential eavesdropping.

QUESTION 1052
Question: TEMPEST is a hardware for which of the following purposes?
Options:
- A. Eavesdropping
- B. Social engineering
- C. Virus scanning
- D. Firewalling
- E. None of the choices

Correct Answer: A
Topic: TEMPEST Technology
Answer Explanation:
TEMPEST technology is used to intercept and analyze the faint electromagnetic emissions from electronic devices to eavesdrop on information. This technique can capture data even from systems that are physically isolated from networks.

QUESTION 1053
Human error is being HEAVILY relied upon by which of the following types of attack?
Options:
- A. Eavesdropping
- B. DoS
- C. DDoS
- D. ATP
- E. Social Engineering
- F. None of the choices

Correct Answer: E
Topic: Social Engineering
Answer Explanation:
Social engineering attacks exploit human error by manipulating individuals into compromising security. This type of attack leverages trust or mistakes made by users rather than system vulnerabilities.

QUESTION 1054
Zombie computers are being HEAVILY relied upon by which of the following types of attack?
Options:
- A. Eavesdropping
- B. DoS
- C. DDoS
- D. ATP
- E. Social Engineering
- F. None of the choices

Correct Answer: C
Topic: Distributed Denial of Service (DDoS) Attacks
Answer Explanation:
DDoS attacks often use compromised computers, known as "zombies," to flood a target with traffic, overwhelming its resources. This coordinated attack can render a system unusable due to resource exhaustion.

QUESTION 1055
Attack amplifiers are often HEAVILY relied upon in which of the following types of attack?
Options:
- A. Packet dropping
- B. ToS
- C. DDoS
- D. ATP
- E. Wiretapping
- F. None of the choices

Correct Answer: C
Topic: Attack Amplifiers in DDoS Attacks
Answer Explanation:
DDoS attacks can leverage attack amplifiers, which exploit poorly designed protocols to significantly increase the volume of traffic directed at a target, further overwhelming its resources.

QUESTION 1056
Back Orifice is an example of:
Options:
- A. a virus
- B. a legitimate remote control software
- C. a backdoor that takes the form of an installed program
- D. an eavesdropper
- E. None of the choices

Correct Answer: C
Topic: Backdoors
Answer Explanation:
Back Orifice is a backdoor program that allows unauthorized remote control of a computer. It installs as a program to gain access to system resources, similar to other backdoor attacks that compromise security.

QUESTION 1057
Which of the following will replace system binaries and/or hook into the function calls of the operating system to hide the presence of other programs?
Options:
- A. Rootkits
- B. Virus
- C. Trojan
- D. Tripwire
- E. None of the choices

Correct Answer: A
Topic: Rootkits
Answer Explanation:
Rootkits modify system binaries or hook into OS functions to conceal malicious programs or processes. This stealth approach makes them difficult to detect by standard security measures.

QUESTION 1058
Question: Which of the following types of attack makes use of common consumer devices that can be used to transfer data surreptitiously?
Options:
- A. Direct access attacks
- B. Indirect access attacks
- C. Port attack
- D. Window attack
- E. Social attack

- F. None of the choices

Correct Answer: A
Topic: Direct Access Attacks
Answer Explanation:
Direct access attacks rely on consumer devices or physical access to transfer data covertly. Attackers may use devices like USB drives or keyloggers to steal data without detection.

QUESTION 1059
Question: Which of the following types of attack almost always requires physical access to the targets?
Options:
- A. Direct access attack
- B. Wireless attack
- C. Port attack
- D. Window attack
- E. System attack
- F. None of the choices

Correct Answer: A
Topic: Physical Access in Direct Attacks
Answer Explanation:
Direct access attacks require physical proximity to the system to install devices or modify hardware/software, making this type of attack heavily dependent on the attacker's physical presence.

QUESTION 1060
Question: Which of the following methods of encryption has been proven to be almost unbreakable when correctly used?
Options:
- A. Key pair
- B. Oakley
- C. Certificate
- D. 3-DES
- E. One-time pad
- F. None of the choices

Correct Answer: E
Topic: One-Time Pad Encryption
Answer Explanation:
A one-time pad is theoretically unbreakable if used correctly. It involves using a unique, random key for each message that is as long as the message itself, ensuring complete security.

QUESTION 1061
Question: Which of the following encryption methods uses a matching pair of key-codes, securely distributed, which are used once-and-only-once to encode and decode a single message?
Options:
- A. Blowfish
- B. Tripwire
- C. Certificate
- D. DES
- E. One-time pad
- F. None of the choices

Correct Answer: E
Topic: One-Time Pad Encryption
Answer Explanation:
The one-time pad encryption method uses a unique pair of keys for each message, distributed securely,

to ensure that the message can only be decoded with its corresponding key. This method is theoretically unbreakable if used correctly.

QUESTION 1062
Question: Why is the one-time pad not always preferable for encryption? (Choose all that apply)
Options:

- A. It is difficult to use securely.
- B. It is highly inconvenient to use.
- C. It requires a licensing fee.
- D. It requires internet connectivity.
- E. It is Microsoft-only.
- F. None of the choices

Correct Answer: A, B
Topic: One-Time Pad Encryption Limitations
Answer Explanation:
One-time pads are challenging to implement because they require secure distribution of unique keys for each message, and managing these keys is inconvenient. While highly secure, these factors make it impractical for widespread use.

QUESTION 1063
Question: You may reduce a cracker's chances of success by (choose all that apply):
Options:

- A. Keeping your systems up to date using a security scanner.
- B. Hiring competent people responsible for security to scan and update your systems.
- C. Using multiple firewalls.
- D. Using multiple firewalls and IDS.
- E. None of the choices

Correct Answer: A, B
Topic: Security Maintenance
Answer Explanation:
Keeping systems up to date and hiring skilled personnel can reduce the risk of successful attacks by identifying and fixing vulnerabilities promptly. Firewalls and IDS can add layers of protection but require knowledgeable management.

QUESTION 1064
Question: Which of the following measures can protect systems files and data, respectively?
Options:

- A. User account access controls and cryptography
- B. User account access controls and firewall
- C. User account access controls and IPS
- D. IDS and cryptography
- E. Firewall and cryptography
- F. None of the choices

Correct Answer: A
Topic: Security Measures
Answer Explanation:
User access controls limit who can access system files, and cryptography ensures that data remains confidential, even if intercepted.

QUESTION 1065
Question: Which of the following is by far the most common prevention system from a network security perspective?
Options:

- A. Firewall
- B. IDS
- C. IPS
- D. Hardened OS
- E. Tripwire
- F. None of the choices

Correct Answer: A
Topic: Network Security
Answer Explanation:
Firewalls are the most common prevention method for network security, acting as a barrier to control incoming and outgoing network traffic based on predetermined security rules.

QUESTION 1066
Question: Which of the following are designed to detect network attacks in progress and assist in post-attack forensics?
Options:

- A. Intrusion Detection Systems
- B. Audit trails
- C. System logs
- D. Tripwire
- E. None of the choices

Correct Answer: A
Topic: Intrusion Detection Systems
Answer Explanation:
Intrusion Detection Systems (IDS) monitor network traffic for suspicious activities, alerting administrators to possible attacks in real-time, and aiding in forensics after an attack.

QUESTION 1067
Question: "Nowadays, computer security comprises mainly 'preventive' measures."
Options:

- A. True
- B. True only for trusted networks
- C. True only for untrusted networks
- D. False
- E. None of the choices

Correct Answer: A
Topic: Computer Security
Answer Explanation:
Most modern computer security measures are preventive, focusing on stopping attacks before they happen through tools like firewalls, anti-virus software, and security protocols.

QUESTION 1068
Question: The majority of software vulnerabilities result from a few known kinds of coding defects, such as (choose all that apply):
Options:

- A. Buffer overflows
- B. Format string vulnerabilities
- C. Integer overflow
- D. Code injection
- E. Command injection
- F. None of the choices

Correct Answer: A, B, C, D, E
Topic: Common Coding Defects

Answer Explanation:
Most software vulnerabilities arise from common issues like buffer overflows, format string vulnerabilities, integer overflows, and both code and command injection, which expose software to various attacks.

QUESTION 1069
Question: ALL computer programming languages are vulnerable to command injection attacks.
Options:
- A. True
- B. False

Correct Answer: B
Topic: Command Injection Vulnerabilities
Answer Explanation:
Not all programming languages are equally vulnerable to command injection attacks. Languages like Java have built-in protections, though some still may be susceptible to certain types of injection vulnerabilities.

QUESTION 1070
Question: Which of the following refers to an anomalous condition where a process attempts to store data beyond the boundaries of a fixed-length buffer?
Options:
- A. Buffer overflow
- B. Format string vulnerabilities
- C. Integer misappropriation
- D. Code injection
- E. None of the choices

Correct Answer: A
Topic: Buffer Overflow
Answer Explanation:
A buffer overflow occurs when data exceeds the storage capacity of a buffer, causing data to overwrite adjacent memory locations. This can lead to unpredictable behavior or system crashes and is a common vulnerability.

QUESTION 1071
Buffer overflow aims primarily at corrupting:
- A. system processor
- B. network firewall
- **C. system memory**
- D. disk storage
- E. None of the choices

Answer: C
Topic: Buffer Overflow
Explanation:
A buffer overflow is an anomalous condition where a process attempts to store data beyond the boundaries of a fixed-length buffer. This causes the extra data to overwrite adjacent memory locations, potentially affecting other buffers, variables, and program flow data.

QUESTION 1072
Which of the following measures can effectively minimize the possibility of buffer overflows?
- **A. Sufficient bounds checking**
- B. Sufficient memory
- C. Sufficient processing capability
- D. Sufficient code injection
- E. None of the choices

Answer: A
Topic: Preventing Buffer Overflows
Explanation:
Buffer overflows can cause a program to crash or produce incorrect results. They are often exploited by inputs designed to execute malicious code or cause the program to behave unexpectedly. Sufficient bounds checking by the programmer or compiler is essential to prevent buffer overflows.

QUESTION 1073
Which of the following types of attack makes use of unfiltered user input as the format string parameter in the printf() function of the C language?

- A. buffer overflows
- **B. format string vulnerabilities**
- C. integer overflow
- D. code injection
- E. command injection
- F. None of the choices

Answer: B
Topic: Format String Vulnerabilities
Explanation:
Format string attacks exploit unfiltered user input as the format string parameter in C functions like printf(). A malicious user may use format tokens such as %s and %x to read data from memory or %n to write data, potentially executing harmful code.

QUESTION 1074
Which of the following kinds of function are particularly vulnerable to format string attacks?

- **A. C functions that perform output formatting**
- B. C functions that perform integer computation
- C. C functions that perform real number subtraction
- D. VB functions that perform integer conversion
- E. SQL functions that perform string conversion
- F. SQL functions that perform text conversion

Answer: A
Topic: Vulnerable Functions in C
Explanation:
Format string vulnerabilities occur in C functions that perform output formatting, such as printf(). These attacks can crash programs or execute malicious code by exploiting unfiltered user input as format string parameters.

QUESTION 1075
Integer overflow occurs primarily with:

- A. string formatting
- B. debug operations
- C. output formatting
- D. input verifications
- **E. arithmetic operations**
- F. None of the choices

Answer: E
Topic: Integer Overflow
Explanation:
An integer overflow happens when an arithmetic operation produces a value that exceeds the storage limit, leading to unexpected behavior or results.

QUESTION 1076
Which of the following types of attack works by taking advantage of the unenforced and unchecked assumptions the system makes about its inputs?

- A. format string vulnerabilities
- B. integer overflow
- **C. code injection**
- D. command injection
- E. None of the choices

Answer: C
Topic: Code Injection Attacks
Explanation:
Code injection attacks exploit assumptions about input that are not enforced or validated, allowing attackers to insert and execute malicious code.

QUESTION 1077
Which of the following terms refers to systems designed to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders?

- **A. ILD&P**
- B. ICT&P
- C. ILP&C
- D. ILR&D
- E. None of the choices

Answer: A
Topic: Information Leakage Detection and Prevention (ILD&P)
Explanation:
Information Leakage Detection and Prevention (ILD&P) systems are designed to detect and prevent the unauthorized transmission of information from an organization's computer systems to outsiders. These systems can be network-based or host-based. Network ILD&P are installed on the internet connection and monitor network traffic, while host-based systems run on workstations and monitor access to physical devices.

QUESTION 1078
Network ILD&P are typically installed:

- A. on the organization's internal network connection.
- **B. on the organization's internet network connection.**
- C. on each end-user station.
- D. on the firewall.
- E. None of the choices.

Answer: B
Topic: Network ILD&P
Explanation:
Network ILD&P are typically installed on an organization's internet network connection. They monitor and analyze network traffic to detect and prevent the unauthorized transmission of sensitive information outside the organization.

QUESTION 1079
Host Based ILD&P primarily addresses the issue of:

- A. information integrity
- B. information accuracy
- C. information validity
- **D. information leakage**
- E. None of the choices.

Answer: D
Topic: Host Based ILD&P
Explanation:
Host-based ILD&P systems run on end-user workstations. They focus on detecting and preventing information leakage, controlling access to physical devices, and monitoring data before encryption.

QUESTION 1080
Software is considered malware based on:

- **A. the intent of the creator.**
- B. its particular features.
- C. its location.
- D. its compatibility.
- E. None of the choices.

Answer: A
Topic: Malware Definition
Explanation:
Malware is defined based on the creator's intent, specifically designed to infiltrate or damage computer systems without the owner's consent. It includes viruses, worms, trojan horses, spyware, adware, and other malicious software.

QUESTION 1081
Which of the following are valid examples of Malware (choose all that apply):

- **A. viruses**
- **B. worms**
- **C. trojan horses**
- **D. spyware**
- **E. All of the above**

Answer: E
Topic: Examples of Malware
Explanation:
Malware includes various types of harmful software, such as viruses, worms, trojan horses, spyware, and adware, all designed to damage or infiltrate a system without the owner's consent.

QUESTION 1082
Which of the following refers to any program that invites the user to run it but conceals a harmful or malicious payload?

- A. virus
- B. worm
- **C. trojan horse**
- D. spyware
- E. rootkits
- F. None of the choices.

Answer: C
Topic: Trojan Horses
Explanation:
A Trojan horse is any program that invites the user to run it while concealing a harmful or malicious payload. Once executed, it may cause immediate damage or install further harmful software.

QUESTION 1083
Broadly speaking, a Trojan horse is any program that invites the user to run it, but conceals a harmful or malicious payload. The payload may take effect immediately and can lead to immediate yet undesirable effects, or more commonly it may install further harmful software into the user's system to serve the creator's longer-term goals.

- **A. True**
- **B. False**

Answer: B
Topic: Trojan Horse Behavior
Explanation:
While a Trojan horse may lead to immediate undesirable effects, it often installs additional harmful software or serves the creator's long-term goals. However, the payload may not always take effect immediately.

QUESTION 1084
Which of the following terms is used more generally for describing concealment routines in a malicious program?

- A. virus
- B. worm
- C. trojan horse
- D. spyware
- **E. rootkits**
- F. backdoor
- G. None of the choices

Answer: E
Topic: Rootkits
Explanation:
Rootkits are used to conceal malicious routines within a program. They can prevent a malicious process from being detected in the process table or hide files. Initially associated with Unix systems, the term now broadly refers to concealment routines in malicious software across various platforms.

QUESTION 1085
Which of the following refers to a method of bypassing normal system authentication procedures?

- A. virus
- B. worm
- C. trojan horse
- D. spyware
- E. rootkits
- **F. backdoor**
- G. None of the choices

Answer: F
Topic: Backdoors
Explanation:
A backdoor is a method that bypasses normal authentication procedures to access a system. Hackers often use backdoors to remotely access a system without detection. These backdoors can be installed through Trojan horses or worms.

QUESTION 1086
To install backdoors, hackers generally prefer to use:

- **A. either Trojan horse or computer worm.**
- B. either Tripwire or computer virus.
- C. either eavesdropper or computer worm.
- D. either Trojan horse or eavesdropper.
- E. None of the choices.

Answer: A
Topic: Installation of Backdoors
Explanation:

Hackers commonly use Trojan horses or worms to install backdoors. These malicious programs allow attackers to bypass system defenses and gain unauthorized access.

QUESTION 1087
In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as:

- A. wormnets
- B. trojannets
- C. spynets
- **D. botnets**
- E. rootnets
- F. backdoor

Answer: D
Topic: Botnets
Explanation:
Botnets are networks of infected computers controlled by attackers. These systems are used to execute coordinated attacks, with infected computers (bots) following commands sent through a central command-and-control system.

QUESTION 1088
In a botnet, malbot logs into a particular type of system for making coordinated attack attempts. What type of system is this?

- **A. Chat system**
- B. SMS system
- C. Email system
- D. Log system
- E. Kernel system
- F. None of the choices

Answer: A
Topic: Botnet Command-and-Control
Explanation:
In a botnet, the infected computer (malbot) typically connects to a chat system, such as an Internet Relay Chat (IRC) channel, to receive commands from the attacker. This enables the attacker to coordinate actions across many infected machines.

QUESTION 1089
Which of the following software tools is often used for stealing money from infected PC owners through taking control of the modem?

- A. System patcher
- **B. Porn dialer**
- C. War dialer
- D. T1 dialer
- E. T3 dialer
- F. None of the choices

Answer: B
Topic: Porn Dialer
Explanation:
A porn dialer is a type of software used by attackers to take control of an infected PC's modem and dial expensive premium-rate numbers, thereby stealing money from the PC owner. These dialers leave the phone line open, accruing charges on the victim's phone bill.

QUESTION 1090
Which of the following is an oft-cited cause of vulnerability of networks?

- **A. software monoculture**
- B. software diversification
- C. single line of defense
- D. multiple DMZ
- E. None of the choices

Answer: A
Topic: Software Monoculture
Explanation:
A common network vulnerability is software monoculture, where a large portion of systems use the same software. This increases the risk of widespread exploitation, as attackers can target the vulnerabilities of commonly used software, such as Microsoft Windows, to compromise many systems.

QUESTION 1091
Introducing inhomogeneity to your network for the sake of robustness would have which of the following drawbacks?

- A. poorer performance
- B. poor scalability
- C. weak infrastructure
- **D. high costs in terms of training and maintenance**
- E. None of the choices

Answer: D
Topic: Inhomogeneity in Networks
Explanation:
Introducing inhomogeneity, or diversity in software and hardware, can strengthen network robustness. However, it comes at the cost of increased training and maintenance expenses, as it requires support for a wider range of systems and solutions.

QUESTION 1092
Which of the following may be deployed in a network as lower-cost surveillance and early-warning tools?

- **A. Honeypots**
- B. Hardware IPSs
- C. Hardware IDSs
- D. Botnets
- E. Stateful inspection firewalls
- F. Stateful logging facilities
- G. None of the choices

Answer: A
Topic: Honeypots
Explanation:
Honeypots are decoy resources set up in a network to attract and monitor malicious activity. These can serve as early-warning tools and surveillance systems to detect attacks and help analyze new exploit techniques.

QUESTION 1093
All Social Engineering techniques are based on flaws in:

- **A. human logic**
- B. hardware logic
- C. software logic
- D. device logic
- E. group logic
- F. None of the choices

Answer: A
Topic: Social Engineering

Explanation:
Social engineering exploits cognitive biases and flaws in human logic to manipulate people into revealing confidential information or performing actions that benefit the attacker. These biases form the foundation of various social engineering techniques.

QUESTION 1094
Relatively speaking, firewalls operated at the application level of the seven-layer OSI model are:

- **A. almost always less efficient**
- B. almost always less effective
- C. almost always less secure
- D. almost always less costly to set up
- E. None of the choices

Answer: A
Topic: Application-Level Firewalls
Explanation:
Firewalls that operate at the application level of the OSI model require more CPU processing power since they inspect the content of each packet in detail. This makes them less efficient compared to lower-layer firewalls, like packet filters, that operate at the network layer.

QUESTION 1095
Relatively speaking, firewalls operated at the physical level of the seven-layer OSI model are:

- A. almost always less efficient
- B. almost always less effective
- C. almost always less secure
- D. almost always less costly to set up
- **E. None of the choices**

Answer: E
Topic: Firewalls at the Physical Layer
Explanation:
No firewalls operate at the physical level of the OSI model. Firewalls typically operate at higher layers, like the network or application layers, to inspect and filter traffic based on headers or content.

QUESTION 1096
Which of the following refers to the act of creating and using an invented scenario to persuade a target to perform an action?

- **A. Pretexting**
- B. Backgrounding
- C. Check making
- D. Bounce checking
- E. None of the choices

Answer: A
Topic: Pretexting
Explanation:
Pretexting is a social engineering tactic where an attacker creates a fabricated scenario to convince the target to disclose information or perform an action. It typically involves research and manipulation to appear legitimate.

QUESTION 1097
Pretexting is an act of:

- A. DoS
- **B. Social engineering**
- C. Eavesdropping
- D. Soft coding

- E. Hard coding
- F. None of the choices

Answer: B
Topic: Pretexting and Social Engineering
Explanation:
Pretexting is a form of social engineering, where attackers manipulate individuals into revealing confidential information by creating fake scenarios. It is not a denial-of-service attack or related to coding techniques.

QUESTION 1098
With Deep Packet Inspection, which of the following OSI layers are involved?

- **A. Layer 2 through Layer 7**
- B. Layer 3 through Layer 7
- C. Layer 2 through Layer 6
- D. Layer 3 through Layer 6
- E. Layer 2 through Layer 5
- F. None of the choices

Answer: A
Topic: Deep Packet Inspection (DPI)
Explanation:
Deep packet inspection (DPI) involves analyzing packets at all layers from Layer 2 (Data Link) through Layer 7 (Application). DPI examines the data part of packets for protocol violations or predefined criteria, offering more granular control than traditional packet filtering.

QUESTION 1099
Squid is an example of:

- A. IDS
- **B. Caching proxy**
- C. Security proxy
- D. Connection proxy
- E. Dialer
- F. None of the choices

Answer: B
Topic: Squid
Explanation:
Squid is a caching proxy server, primarily used to store copies of frequently accessed web content to reduce bandwidth usage. It is not specifically a security proxy, though it may help with network performance and content filtering.

QUESTION 1100
Which of the following types of firewall treats each network frame or packet in isolation?

- A. Stateful firewall
- B. Hardware firewall
- C. Combination firewall
- **D. Packet filtering firewall**
- E. Stateless firewall
- F. None of the choices

Answer: E
Topic: Stateless Firewalls
Explanation:
A stateless firewall treats each packet in isolation, without tracking the state of the connection. It does not differentiate between packets that are part of an ongoing session
trying to establish a new connection, or is just a rogue packet.