DES-9131.VCEplus.premium.exam.60q

Number: DES-9131
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

DES-9131

Specialist - Infrastructure Security Exam

Version 1.0

Exam A

QUESTION 1

What are the four tiers of integration within the NIST Cybersecurity Framework?

A. Selective, Repeatable, Partial, and Adaptive
B. Partial, Risk Informed, Repeatable, and Adaptive
C. Corrective, Risk Informed, Repeatable. and Adaptive
D. Risk Informed, Selective, Repeatable, and Partial

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.nist.gov/cyberframework/online-learning/components-framework

QUESTION 2
What procedure is designed to enable security personnel to detect, analyze, contain, eradicate, respond, and recover from malicious computer incidents such as a denial-of-service attack?

A. Disaster Recovery Plan
B. Emergency Analysis Plan
C. Crisis Communication Plan
D. Incident Response Plan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

QUESTION 3
What determines the technical controls used to restrict access to USB devices and help prevent their use within a company?

A. Block use of the USB devices for all employees
B. Written security policy prohibiting the use of the USB devices
C. Acceptable use policy in the employee HR on-boarding training
D. Detect use of the USB devices and report users

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4 Concerning a risk management strategy, what should the executive level be responsible for communicating?

A. Risk mitigation
B. Risk profile
C. Risk tolerance
D. Asset risk

Correct Answer: B
Section: (none)

Explanation
Explanation/Reference:

QUESTION 5 What process is used to identify an organization's physical, digital, and human resource, as required in their Business Impact Analysis?

A. Risk Management Strategy
B. Risk Assessment
C. Risk Treatment
D. Asset Inventory

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6 What supports an organization in making risk management decisions to address their security posture in real time?

A. Baseline reporting
B. Continuous monitoring
C. User access reviews
D. Video surveillance

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7 When should event analysis be performed?

A. Only when requested by an auditor
B. Routinely for all events collected on a mission critical system
C. Only at the discretion of an authorized security analyst
D. After an event is triggered by the detection system

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8 What type of system processes information, the loss of which would have a debilitating impact to an organization?

A. Mission critical
B. Security critical
C. Business criticalD. Safety critical

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 9 Which mechanism within the NIST Cybersecurity Framework describes a method to capture the current state and define the target state for understanding gaps, exposure, and prioritize changes to mitigate risk?

A. Functions
B. Profiles
C. Tiers
D. Categories

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
The CSF recommends that the Communication Plan for an IRP include audience, method of communication, frequency, and what other element?

A. Incident category
B. Message criteria
C. Incident severity
D. Templates to use

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.utc.edu/information-technology/pdfs/it-comm-plan-master-2017.pdf (p.4)

QUESTION 11 What is the main goal of a gap analysis in the Identify function?

A. Determine security controls to improve security measures
B. Determine actions required to get from the current profile state to the target profile state
C. Identify gaps between Cybersecurity Framework and Cyber Resilient Lifecycle pertaining to that functionD. Identify business process gaps to improve business efficiency

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
DRAG DROP

Rank order the relative severity of impact to an organization of each plan, where “1” signifies the most impact and “4” signifies the least impact.

Select and Place:

Backup Plan	1
Disaster Recovery Plan	2
Recovery Plan	3
Business Continuity Plan	4

Correct Answer:

Backup Plan	Disaster Recovery Plan
Disaster Recovery Plan	Business Continuity Plan
Recovery Plan	Disaster Recovery Plan
Business Continuity Plan	Backup Plan

Section: (none)
Explanation

Explanation/Reference:

QUESTION 13 What does a security benchmark help define?

A. Whether or not the organization should implement ISCM
B. The Baseline, or “as is” state
C. Which step of the DRP to execute first
D. What parts of the Baseline are appropriate

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14 In which function is the SDLC implemented?

A. Respond
B. Protect
C. Detect
D. Recover

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15 Which category addresses the detection of unauthorized code in software?

A. PR.DS
B. DE.DP
C. PR.AT
D. DE.CM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://vufind.carli.illinois.edu/vf-rou/Record/rou_346654/TOC

QUESTION 16 What database is used to record and manage assets?

A. Configuration Management Database
B. Asset Inventory Management Database
C. High Availability Mirrored Database
D. Patch Management Inventory Database

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Configuration_management_database

QUESTION 17
The CSIRT team is following the existing recovery plans on non-production systems in a PRE-BREACH scenario. This action is being executed in which function?

A. Protect
B. Recover
C. Identify
D. Respond

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18 What is a consideration when performing data collection in Information Security Continuous Monitoring?

A. Data collection efficiency is increased through automation.
B. The more data collected, the better chances to catch an anomaly.
C. Collection is used only for compliance requirements.
D. Data is best captured as it traverses the network.

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 19
An organization has a policy to respond “ASAP” to security incidents. The security team is having a difficult time prioritizing events because they are responding to all of them, in order of receipt.

Which part of the IRP does the team need to implement or update?

A. Scheduling of incident responses
B. ‘Post mortem’ documentation
C. Classification of incidents
D. Containment of incidents

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Your firewall blocked several machines on your network from connecting to a malicious IP address. After reviewing the logs, the CSIRT discovers all Microsoft Windows machines on the network have been affected based on a newly published CVE.

Based on the IRP, what should be done immediately?

A. Update the asset inventory
B. Contain the breach
C. Eradicate the breach
D. Revise the IRP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which document provides an implementation plan to recover business functions and processes during and after an event?

A. Business Continuity Plan
B. Disaster Recovery Plan
C. Risk Assessment Strategy
D. Business Impact Analysis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.bmc.com/blogs/disaster-recovery-planning/

QUESTION 22 Which NIST Cybersecurity Framework function should be executed before any others?

A. Respond
B. Protect
C. Recover
D. Identify

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.nist.gov/cyberframework/online-learning/five-functions

QUESTION 23 What is part of the Pre-Recovery phase?

A. Backup validation
B. Validate functionality
C. Restore assets
D. Monitor assets

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Refer to the exhibit.

ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev.4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev.4** CP-8, PE-9, PE-11, PM-8. SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev.4** CP-2, CP-11, SA-14

What type of item appears in the second column of the table?

A. Subcategory
B. Informative Reference
C. Function
D. Tier

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
What must be included in the CMDB?

A. Inventory of uninstalled software
B. Software End User Licensing AgreementsC. Dependencies of installed components
D. Known vulnerabilities of installed software

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

Reference: https://docs.servicenow.com/bundle/london-servicenow-platform/page/product/configuration-management/concept/cnfig-mgmt-and-cmdb.html

QUESTION 26
What should an organization use to effectively mitigate against password sharing to prevent unauthorized access to systems?

A. Access through a ticketing system
B. Frequent password resets
C. Strong password requirements
D. Two factor authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
You have been tasked with documenting mission critical procedures of an organization that need to be sustained through a significant disruption.

What document would you develop?

A. Business Continuity Plan
B. Business Impact Assessment
C. Risk Analysis Report
D. Regression Test Plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28 What contains a predefined set of efforts that describes an organization's mission/business critical processes, and defines how they will be sustained during and after a significant disruption?

A. Disaster Recovery Plan
B. Risk Assessment Strategy
C. Business Continuity Plan
D. Business Impact Analysis

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
An Internet-connected file server compromised by a threat that leaked all data. The data was destroyed to cover all tracks. The file server has high availability capabilities to handle critical workloads. The operations team took only 15 minutes to restore workload routing to a different node.

What part(s) of the CIA Triad was affected?

A. A only
B. C, I
C. C, A

D. A, I

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30 Your organization was breached. You informed the CSIRT and they contained the breach and eradicated the threat.

What is the next step required to ensure that you have an effective CSRL and a more robust cybersecurity posture in the future?

A. Determine change agent
B. Update the BIA
C. Conduct a gap analysis
D. Update the BCP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Your organization has tasked you with collecting information on all the data, personnel, devices, systems, and facilities that enable the organization to achieve its business purposes. Which part of the NIST Cybersecurity Framework would you consult first?

A. ID.SC
B. DE.DPC. PR.AC
D. ID.AM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.phe.gov/Preparedness/planning/405d/Documents/resources-templates-508.pdf (27)

QUESTION 32 What is concerned with availability, reliability, and recoverability of business processes and functions?

A. Business Impact Analysis
B. Business Continuity Plan
C. Recovery Strategy
D. Disaster Recovery Plan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
A security engineer is responsible for monitoring company software, firmware, system OS, and applications for known vulnerabilities. How should they stay current on exploits and information security?

A. Implement security awareness training
B. Update company policies and procedures
C. Revise vulnerability management plan
D. Subscribe to security mailing lists

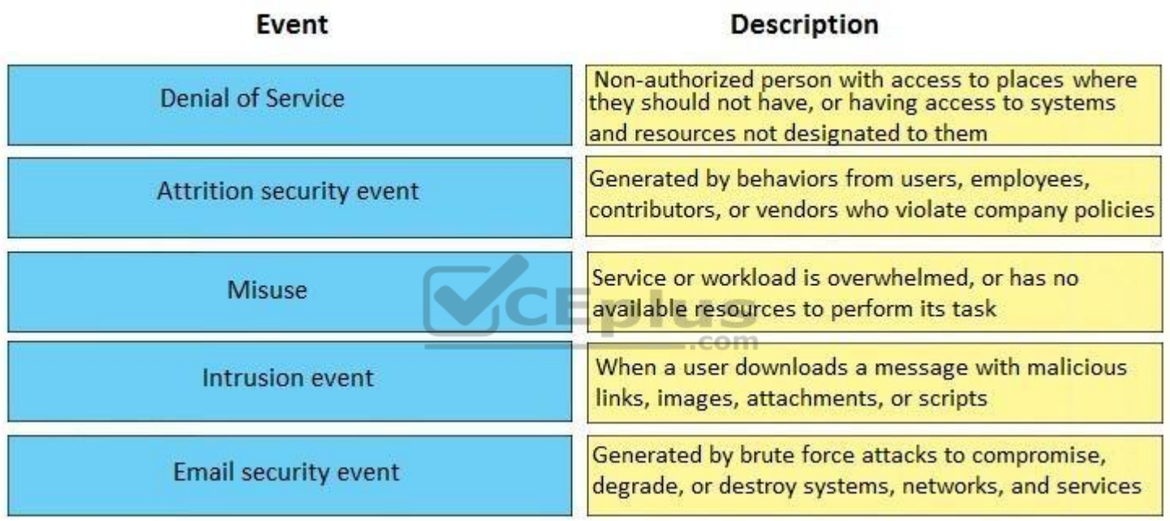
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

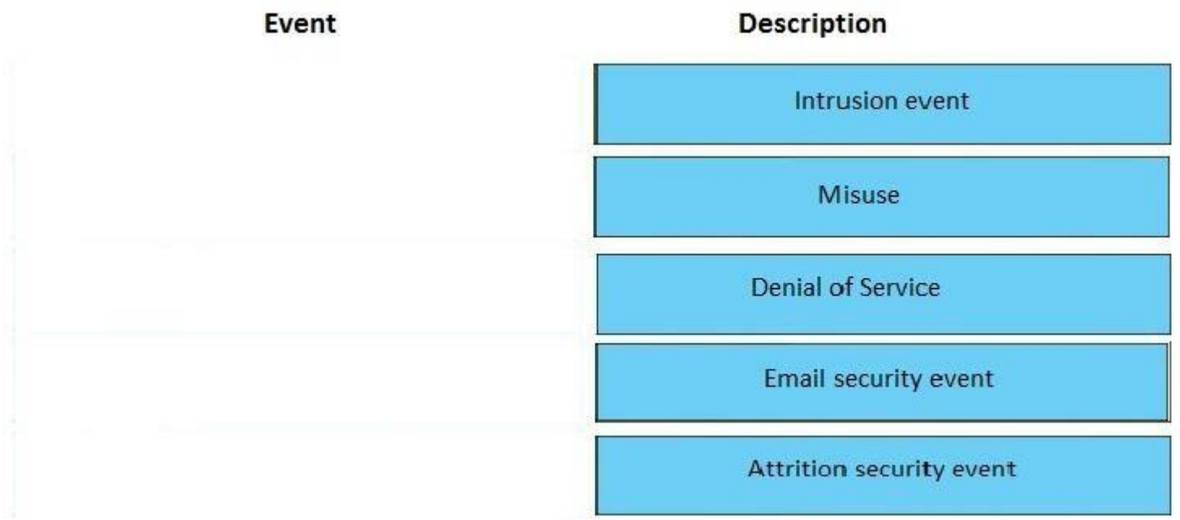
QUESTION 34
DRAG DROP

Match the security event to its description.

Select and Place:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
The project manager of a data center has a budget of $1,500,000 to install critical infrastructure systems. The project will take 24 months to complete.

The project manager is working with the project management team, security experts, and stakeholders to identify cyber risks. After reviewing the project plan, the CIO wants to know why so many risk identification meetings are requested.

What a valid reason for the repeated risk identification meetings?

A. Identify new risks
B. Update the company risk register
C. Transfer risk to other project team members
D. Prevent all risk

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
A company suffers a data breach and determines that the threat actors stole or compromised 10,000 user profiles. The company had planned for such a breach and determined the loss would be around $2 million. Soon after restoration, the company stock suffered a 30% drop and the loss was nearly $20 million. In addition, the company received negative press.

Which area of risk did the business forget to account for?

A. Litigation or Legal Risk
B. Reputational Risk
C. Vulnerability risk
D. Business Operational Risk

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 37 A company implemented an intrusion detection system. They notice the system generates a very large number of false alarms.

What steps should the company take to rectify this situation?

A. Re-evaluate the Baseline and make necessary adjustments to the detection rules
B. Replace the intrusion detection system with an intrusion protection system
C. Define how to identify and disregard the false alarms
D. Consider evaluating a system from another vendor

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38 Assume that a DDoS attack has been occurring for 72 minutes. What determines who talks to external stakeholders?

A. Business Continuity Plan
B. Communication Plan
C. Business Impact Analysis
D. Incident Response Plan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39 What is considered outside the scope of a BIA?

A. Estimated probability of the identified threats actually occurring
B. Selection of full, incremental, or differential backups
C. Efficiency and effectiveness of existing risk mitigation controls
D. Determination of capacity requirements for backups

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40 What are the five functions of the NIST Framework Core?

A. Identify, Protect, Detect, Respond, and Recover
B. Governance, Identify, Recover, Respond, and Recover
C. Protect, Detect, Respond, Governance, and Recover

D. Identify, Respond, Protect, Detect, and Governance

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference https://www.nist.gov/cyberframework/online-learning/five-functions

QUESTION 41 Which NIST Cybersecurity Framework category ensures that organizational communication and data flows are mapped?

A. ID.AM
B. ID.GV
C. ID.RAD. ID.SC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference https://1path.com/blog/overview-of-the-nist-cybersecurity-framework/

QUESTION 42 The Backup Recovery Plan is dependent on what effort?

A. PR.DS
B. RTO
C. BIA
D. SDLC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf

QUESTION 43 What must be done before returning a compromised laptop to normal operations in the environment?

A. Perform a virus scan
B. Eliminate the root cause of the compromise
C. Re-image the device
D. Device cannot be returned to the environment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
An incident has occurred. You restore backups onto mission/business critical assets. After restoration of the backups your services are still inaccessible on numerous assets.

What could be the cause of the issue?
A. Unverified backups

B. Incorrect backup strategy
C. Hardware failure
D. Network failure

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45 A new employee is starting work at your company. When should they be informed of the company's security policy?

A. Based on human resource policy
B. After the first security infraction
C. Annual security policy review
D. During regular security awareness sessions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46 A continuously updated CMDB is an output of which NIST function and category?

A. ID.RM
B. ID.SC
C. ID.BE
D. ID.AM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
What contains a predefined set of instructions or processes that describes the management policy, procedures, and written plan defining recovery of information systems?

A. RAS
B. DRP
C. BIA
D. BCP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.drj.com/downloads/drj_glossary.pdf

QUESTION 48

Your data center uses a diesel generator as backup for two different power grids provided by your regional power company. During a period of unprecedented heat, you experience brown-outs on both grids simultaneously. The diesel generator starts up but only runs for two minutes before it also shuts down, leaving your entire data center down until grid power can be restored. Further inspection reveals a clogged fuel filter.

Failing to schedule preventive service for the backup generator is a failure in which function?

A. Recover
B. Respond
C. Detect
D. Protect

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://1path.com/blog/overview-of-the-nist-cybersecurity-framework/

QUESTION 49 What is the purpose of separation of duties?

A. Internal control to prevent fraud
B. Enhance exposure to functional areas
C. Encourage collaboration
D. Mitigate collusion and prevent theft

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.marsdd.com/mars-library/internal-controls-accounting-key-benefits/

QUESTION 50
What common process conducted by organizations when protecting digital assets is outside the scope of the NIST Cybersecurity Framework?

A. Recover
B. Identify
C. Protect
D. Investigate

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://1path.com/blog/overview-of-the-nist-cybersecurity-framework/

QUESTION 51
What defines who is accountable for contacting operational teams, managers, and others affected by a localized, safety critical event?

A. Asset Management Plan
B. Business Impact Analysis
C. Business Continuity Plan
D. Incident Response Plan

Correct Answer: D
Section: (none)

Explanation
Explanation/Reference:

QUESTION 52
The network security team in your company has discovered a threat that leaked partial data on a compromised file server that handles sensitive information. Containment must be initiated and addresses by the CSIRT.

Service disruption is not a concern because this server is used only to store files and does not hold any critical workload. Your company security policy required that all forensic information must be preserved.

Which actions should you take to stop data leakage and comply with requirements of the company security policy?

A. Disconnect the file server from the network to stop data leakage and keep it powered on for further analysis.
B. Shut down the server to stop the data leakage and power it up only for further forensic analysis.
C. Restart the server to purge all malicious connections and keep it powered on for further analysis.
D. Create a firewall rule to block all external connections for this file server and keep it powered on for further analysis.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53 You need to review your current security baseline policy for your company and determine which security controls need to be applied to the baseline and what changes have occurred since the last update.

Which category addresses this need?

A. ID.AM
B. PR.IP
C. PR.MA
D. ID.SC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjjw_fHytHgAhWvyqYKHXaVAWcQFjAAegQICRAC&url=https%3A%2F%2Fwww.nist.gov%2Fdocument%2Fdraft-cybersecurity-frameworkv11-corexlsx&usg=AOvVaw2wFipKqwxx2QnhlcVB2A7g

QUESTION 54
A CISO is looking for a solution to lower costs, enhance overall efficiency, and improve the reliability of monitoring security related information.

Which ISCM feature is recommended?

A. Reporting
B. Provisioning
C. Automation
D. Collection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf (19)

QUESTION 55 What is the primary objective of establishing governance and risk management processes for an organization?

A. Manage assets effectively in accordance with local laws
B. Minimize cybersecurity risks in conjunction with compliance processes
C. Determine compliance controls in accordance with national laws
D. Establish recovery time objectives for critical infrastructure

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
During what activity does an organization identify and prioritize technical, organizational, procedural, administrative, and physical security weaknesses?

A. Table top exercise
B. Penetration testing
C. Vulnerability assessment
D. White box testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Refer to the exhibit.

Action	Category	System	Risk Rank		Maturity		Priority	Cost
			SRC	TGT	SRC	TGT		
Detection Processes	A	ENG, FIN, Sales	3	8	4	6	7	4
		HR, EXEC	7	8	9	9	3	4
Security Continuous Monitoring	B	ENG, FIN, SALES, HR, EXEC	5	8	5	6	4	3
Anomalies and Events	C	ENG, FIN, SALES, HR, EXEC	6	8	5	7	6	6

Your organization's security team has been working with various business units to understand their business requirements, risk tolerance, and resources used to create a Framework Profile.

Based on the Profile provided, what entries correspond to labels A, B, and C?

A: PR.IP
B: DE.CM
C: DE.AE

A: PR.DS
B: DE.AE
C: DE.CM

A: DE.AE
B: PR.DS
C: RS.CO

A.

B.

C.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58 Which document is designed to limit damage, reduce recovery time, and reduce costs where possible to the organization?

A. Business Impact Analysis
B. Business Continuity Plan
C. Risk Assessment Strategy
D. Incident Response Plan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
A security audit of the systems on a network must be performed to determine their compliance with security policies. Which control should be used for the audit?

A. PR.DS

B. DE.CM
C. RS.MID. ID.AM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
In accordance with PR.MA, an organization has just truncated all log files that are more than 12 months old. This has freed up 25 TB per logging server.

What must be updated once the truncation is verified?
A. SDLC
B. IRP
C. Baseline
D. ISCM

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: