Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

D-CSF-SC-23 Dumps
D-CSF-SC-23 Braindumps
D-CSF-SC-23 Real Questions
D-CSF-SC-23 Practice Test
D-CSF-SC-23 Actual Questions

killexams.com

DELL-EMC

D-CSF-SC-23

NIST Cybersecurity Framework 2023 Certification

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/D-CSF-SC-23

Question: 1

What could be considered a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors and align to five concurrent and continuous functions?

A. Baseline
B. Core
C. Profile
D. Governance

Answer: B

Question: 2

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

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

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

A. Option A
B. Option B

C. Option C

Answer: A

Question: 3

What term refers to a partially equipped, environmentally conditioned work space used to relocate operations in the event of a significant disruption?

A. Hot site
B. Warm site
C. Mirror site
D. Secondary site

Answer: B

Question: 4

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

Answer: D

Question: 5

What are the main components of the NIST Cybersecurity Framework?

A. Core, Categories, and Tiers
B. Functions, Profiles, and Tiers
C. Categories, Tiers, and Profiles
D. Core, Tiers, and Profiles

Answer: D

Question: 6

The Disaster Recovery Plan must document what effort in order to address unrecoverable assets?

A. RTO savings
B. Recovery priority
C. Recovery resources
D. Recovery resources

Answer: D

Question: 7

To generate an accurate risk assessment, organizations need to gather information in what areas?

A. Assets, Threats, Vulnerabilities, and Impact
B. Assets, Vulnerabilities, Security, and Response
C. Inventory, Security, Response, and Impact
D. Inventory, Threats, Security, and Impact

Answer: A

Question: 8

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. I
B. AM
C. P
D. IP
E. P
F. MA
G. I
H. SC

Answer: B

Question: 9

What specifically addresses cyber-attacks against an organization's IT systems?

A. Continuity of Support Plan
B. Business Continuity Plan
C. Continuity of Operations Plan
D. Incident Response Plan

Answer: C

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

Answer: B

Question: 11

You have completed a review of your current security baseline policy. In order to minimize financial, legal, and reputational damage, the baseline configuration requires that infrastructure be categorized for the BIA.

Which categorizations are necessary for the BIA?

A. Mission critical and business critical only
B. Mission critical, safety critical, and business critical
C. Security critical, safety critical, and business critical
D. Mission critical and safety critical only

Answer: B

Question: 12

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 transaction is verified?

A. SDLC
B. IRP
C. Baseline
D. ISCM

Answer: C

Question: 13

What activity informs situational awareness of the security status of an organization's systems?

A. IDP
B. RMF
C. ISCM
D. DPI

Answer: C

Question: 14

What is the effect of changing the Baseline defined in the NIST Cybersecurity Framework?

A. Negative impact on recovery
B. Does not result in changes to the BIA
C. Positive impact on detection
D. Review of previously generated alerts

Answer: C

Question: 15

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.

Answer: C

Question: 16

Which category addresses the detection of unauthorized code in software?

A. P
B. DS
C. D
D. DP
E. P
F. AT
G. D
H. CM

Answer: D

Question: 17

Which phase in the SDLC is most concerned with maintaining proper authentication of users and processes to ensure an appropriate access control policy is defined?

A. Implementation
B. Operation / Maintenance
C. Initiation
D. Development / Acquisition

Answer: B

Question: 18

A company failed to detect a breach of their production system. The breach originated from a legacy system that was originally thought to be decommissioned. It turned out that system was still operating and occasionally connected to the production system for reporting purposes.

Which part of the process failed?

A. D
B. CM
C. I
D. BE

E. I
F. AM
G. P
H. DS

Answer: C

Question: 19

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

Answer: A

Question: 20

What are the five categories that make up the Response function?

A. Response Planning, Data Security, Communications, Analysis, and Mitigation
B. Response Planning, Communications, Analysis, Mitigation, and Improvements
C. Mitigation, Improvements, Maintenance, Response Planning, and Governance
D. Awareness and Training, Improvements, Communications, Analysis, and Governance

Answer: B

Question: 21

What is the purpose of the Asset Management category?

A. Prevent unauthorized access, damage, and interference to business premises and information
B. Support asset management strategy and information infrastructure security policies
C. Avoid breaches of any criminal or civil law, statutory, regulatory, or contractual obligations
D. Inventory physical devices and systems, software platform and applications, and communication flows

Answer: D

Question: 22

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.

Answer: A

Question: 23

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

Answer: A

Question: 24

What is used to ensure an organization understands the security risk to operations, assets, and individuals?

A. Risk Management Strategy
B. Risk Assessment
C. Operational Assessment
D. Risk Profile

Answer: B

Question: 25

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

Answer: A

Question: 26

A bank has been alerted to a breach of its reconciliation systems. The notification came from the cybercriminals claiming responsibility in an email to the CEO. The CEO has alerted the company CSIRT.

What does the Communication Plan for the IRP specifically guide against?

A. Transfer of chain of custody
B. Accelerated turn over
C. Rushed disclosure
D. Initiating kill chain

Answer: C

Question: 27

An organization has a policy to respond âASAPâ 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. âPost mortemâ documentation
C. Classification of incidents
D. Containment of incidents

Answer: C

Question: 28

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

Answer: A

Question: 29

What helps an organization compare an "as-is, to-be" document and identify opportunities for improving cybersecurity posture useful for capturing organizational baselines of today and their desired state of tomorrow so that a gap analysis can be conducted?

A. Framework
B. Core
C. Assessment
D. Profile

Answer: D

Question: 30

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

Answer: A

Question: 31

What is the purpose of a baseline assessment?

A. Enhance data integrity
B. Determine costs
C. Reduce deployment time
D. Determine risk

Answer: D

Question: 32

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 function
D. Identify business process gaps to improve business efficiency

Answer: B

Question: 33

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

Answer: B

Question: 34

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

Answer: C

Question: 35

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

Answer: A

Question: 36

At what cyber kill chain stage do attackers use malware to exploit specific software or hardware vulnerabilities on the target, based on the information retrieved at the reconnaissance stage?

A. Installation
B. Reconnaissance
C. Weaponization
D. Delivery

Answer: C

Question: 37

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

Answer: C

Question: 38

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

Answer: B

Question: 39

The information security manager for a major web based retailer has determined that the product catalog database is corrupt. The business can still accept orders online but the products cannot be updated. Expected downtime to rebuild is roughly four hours.

What type of asset should the product catalog database be categorized as?

A. Mission critical
B. Safety critical
C. Non-critical
D. Business critical

Answer: D

Question: 40

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

Answer: D

SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

***Actual Exam Questions**: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

***Exam Dumps**: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

***Practice Tests**: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

***Guaranteed Success**: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

***Updated Content:** Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

***Technical Support**: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*