Certs4Sale
Pass With 100% Guarantee

AKYLADE CRF-002

AKYLADE Certified Cyber Resilience Fundamentals (A/CCRF)

Thank You for Downloading CRF-002 Updated Exam Questions

https://certs4sale.com/AKYLADE/crf-002-pdf-exam-dumps

QUESTION: 1

Which of the following best describes how the NIST Cybersecurity Framework facilitates organizational cybersecurity practices?

Option A : By utilizing rigid structures that limit its adaptability and evolution
Option B : By ensuring absolute cybersecurity by elimiating all risk of a data breaches
Option C : By dictating precise cybersecurity policies to be followed without deviation
Option D : By providing a common language to promote effective collaboration

Correct Answer: D

Explanation/Reference:

The NIST Cybersecurity Framework helps facilitate effective communication and collaboration among organizational stakeholders. It provides a common language and structure for discussing cybersecurity risks, enabling different teams and departments to communicate effectively and align their efforts. This characteristic fosters a culture of collaboration, ensuring that cybersecurity considerations are integrated into various aspects of the organization's operations. For support or reporting issues, include Question ID: 66199eccfd737f4da39602e4 in your ticket. Thank you.

QUESTION: 2

A software company identifies a significant risk of source code leaks due to inadequate version control and employee access management. What key elements should be included in their risk management plan to address this issue effectively?

Option A : Increase general cybersecurity awareness training, especially social engineering attacks, for all employees.
Option B : Outsource source code development to external contractors to reduce internal risks
Option C : Implement robust version control systems and restrict access to sensitive information based on roles and responsibilities
Option D : Conduct a public relations campaign to reassure stakeholders about data security and emphasize cybersecurity training

Correct Answer: C

Explanation/Reference:

Including strict version control measures and role-based access control in the risk management plan directly targets the identified risks by securing the source code and limiting access to authorized personnel only, thereby reducing the likelihood of leaks. While managing stakeholder perceptions is important, it does not address the internal operational changes needed to secure the source code. Outsourcing may shift some responsibilities but could introduce new risks and does not resolve the fundamental issues of version control and internal access management. General training is beneficial but does not specifically

address the specialized needs related to version control and access management for source code protection. For support or reporting issues, include Question ID: 6624034f0bf297753767cc9f in your ticket. Thank you.

QUESTION: 3

In what way does the NIST Cybersecurity Framework's nature impact its adoption across various industries and sectors, including critical infrastructure and small businesses?

Option A : Mandates compliance which could strain resources for sectors not typically targeted by cybersecurity regulations
Option B : Limits its use strictly to government entities required to implement it by regulation to maintain compliance throughout organizations
Option C : Encourages a wider adoption by allowing organizations to tailor the guidelines to their specific needs and capabilities
Option D : Discourages small businesses from adopting it due to the perceived complexity and cost which ensures its elite status

Correct Answer: C

Explanation/Reference:

The voluntary nature of the NIST Cybersecurity Framework enables organizations of all sizes and sectors, from critical infrastructure to small businesses, to adopt and adapt the framework according to their specific risk profiles and resources. The NIST Cybersecurity Framework is voluntary and does not mandate compliance, thus it is designed to be adaptable and resource-sensitive for different sectors. The framework's flexibility and scalability actually help to encourage adoption by businesses of all sizes, not discourage them. The NIST Cybersecurity Framework is not limited to government use; its voluntary nature encourages adoption across various sectors. For support or reporting issues, include Question ID: 66240bb3e5c1df8090231f60 in your ticket. Thank you.

QUESTION: 4

A company assesses the potential loss from a data breach involving customer information. If the estimated loss per record is $100 and the breach could expose 800 records, what is the Single-Loss Expectancy (SLE)?

Option A : $12,500.00
Option B : $8,000.00
Option C : $1,250.00
Option D : $80,000.00

Correct Answer: D

Explanation/Reference:

SLE is calculated by multiplying the loss per record by the number of records exposed. Here, $100 per record times 800 records equals $80,000, which is the correct calculation of SLE for this scenario.

QUESTION: 5

Which of the following best describes the purpose of the Identity Management, Authentication, and Access Control (PR.AA) category in the NIST Cybersecurity Framework?

Option A : To monitor network traffic and detect unauthorized access
Option B : To control access through identity verification and permissions management
Option C : To secure physical entry points in information and data systems
Option D : To conduct cybersecurity training for all organizational administrators and employees

Correct Answer: B

Explanation/Reference:

The PR.AA category ensures that access to systems and data is regulated through robust identity verification and permission management processes. Training is essential but is specifically targeted by the Awareness and Training (PR.AT) category, not Identity Management, Authentication, and Access Control. While critical, monitoring network traffic and detecting unauthorized access aligns more with the Detect function's continuous monitoring, not specifically with identity management and access control. Securing physical entry points is a component of broader security measures but does not directly focus on the digital authentication and access control intended by PR.AA. For support or reporting issues, include Question ID: 661c96c37f25571005e9c27c in your ticket. Thank you.

QUESTION: 6

A startup is currently managing cybersecurity issues on an incident-by-incident basis without any predefined strategy. Most decisions are made spontaneously without consulting any established guidelines or standards. What tier best describes their cybersecurity implementation?

Option A : Tier 3 (Repeatable)
Option B : Tier 4 (Adaptive)
Option C : Tier 1 (Partial)
Option D : Tier 2 (Risk Informed)

Correct Answer: C

Explanation/Reference:

Tier 1 (Partial) is the best fit as it reflects organizations that manage cybersecurity in an informal, reactive manner, with little to no predetermined strategy or process integration. Tier 4 (Adaptive) characterizes highly mature organizations that proactively adapt their cybersecurity practices based on predictive modeling and ongoing assessments, not relevant to the startup's current practices. Tier 2 (Risk Informed) implies some level of formal risk awareness which is lacking in the startup's approach, as described. Tier 3 (Repeatable) describes organizations with formalized and consistent cybersecurity practices across the board, which does not match the startup's ad hoc methods. For support or reporting issues, include Question ID: 661d702e6c62df68d36d7641 in your ticket. Thank you.

QUESTION: 7

A technology company utilizes advanced encryption methods to secure data in transit and at rest to ensure that sensitive customer information is protected from unauthorized access and breaches. Which of the following subcategories in the NIST Cybersecurity Framework best supports this scenario for effectively managing the organization's security?

Option A : DE.CM-02
Option B : RS.CO-1
Option C : PR.DS-02
Option D : ID.IM-02

Correct Answer: C

Explanation/Reference:

PR.DS-2 involves protecting data in transit, ensuring encryption methods are used to secure data as it moves across networks, and is crucial for safeguarding sensitive information during transfer. RS.CO-1 involves coordinating incident response activities with stakholders, which is important after a breach but does not directly engage with preemptive data encryption strategies. DE.CM-02 focuses on monitoring the physical environment for potential adverse events, but does not address proactive measures like encryption for data in transit or at rest. ID.IM-02 involves Improvements being identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties,, but it does not directly deal with encryption practices. For support or reporting issues, include Question ID: 661cb02d5acc0ce3a6dd2d89 in your ticket. Thank you.

QUESTION: 8

In the context of quantitative risk assessment, what does the ARO measure?

Option A : The maximum potential loss from a single occurrence of a threat or event

Option B : The effectiveness of security measures implemented to reduce incidents and events
Option C : The total number of incidents that have occurred over a specific period, such as a week, month, or year
Option D : The estimated frequency at which a specific threat is expected to occur within a year

Correct Answer: D

Explanation/Reference:

The Annualized Rate of Occurrence (ARO) quantifies how often a particular threat is anticipated to occur annually, helping in the calculation of ALE by providing a frequency rate for risk estimation. ARO measures frequency of occurrences, not the effectiveness of the security measures. While it measures occurrences over time, ARO specifically predicts the frequency of a future event happening within a year. The maximum potential loss from a single occurrence of a threat is related to Single-Loss Expectancy (SLE), not ARO, which focuses on the frequency of occurrences. For support or reporting issues, include Question ID: 6623095d8f6a0af54bf95bfe in your ticket. Thank you.

QUESTION: 9

How do subcategories in the NIST Cybersecurity Framework assist organizations in managing their cybersecurity risks?

Option A : By mandating the types of cybersecurity training programs that must be conducted
Option B : By serving as independent compliance standards that organizations must follow
Option C : By providing a checklist of cybersecurity measures to be implemented immediately
Option D : By outlining specific actions to achieve the security outcomes of each framework category

Correct Answer: D

Explanation/Reference:

Subcategories detail precise actions needed to reach the security outcomes set forth in the framework's broader categories, aiding structured risk management. Subcategories are guidelines within the framework and not independent compliance standards. Subcategories recommend considerations for training but do not mandate specific types or content of cybersecurity training programs. Subcategories suggest actionable steps but are not merely checklists; they guide strategic implementation over time. For support or reporting issues, include Question ID: 661cb1acf296c0d1d32d1fa2 in your ticket. Thank you.

QUESTION: 10

Which of the following information security publications provides guidelines for secure web application development and is aligned with outcomes listed in the NIST Cybersecurity Framework?

Option A : PCI-DSS
Option B : HIPAA
Option C : FedRAMP
Option D : OWASP

Correct Answer: D

Explanation/Reference:

OWASP (Open Web Application Security Project) provides guidelines for secure web application development, which align with NIST Cybersecurity Framework outcomes, especially in terms of identifying and mitigating web application security risks. While the Payment Card Industry Data Security Standard (PCI-DSS) focuses on payment card data security, the Health Insurance Portability and Accountability Act (HIPAA) is specific to healthcare data protection, and the Federal Risk and Authorization Management Program (FedRAMP) deals with cloud security, they do not directly address web application security as comprehensively as OWASP. For support or reporting issues, include Question ID: 664797e549e3610d12ae394e in your ticket. Thank you.

QUESTION: 11

What is the benefit of comparing an organization's current profile against its target profile?

Option A : To determine the return on investment for the information technology and cybersecurity department budgets
Option B : To fulfill the organization's mandatory reporting requirements to regulatory agencies and legal bodies
Option C : To identify discrepancies between current practices and desired outcomes, guiding focused improvements
Option D : To evaluate the performance of the cybersecurity tools currently in use within the organization

Correct Answer: C

Explanation/Reference:

Comparing the current profile and the target profile helps to identify specific areas where the organization falls short of its cybersecurity goals, facilitating targeted improvements and strategic alignment. Budget planning is influenced by many factors, and while important, it’s not the primary benefit of profile comparison. While tool performance evaluation is part of overall assessments, the broader benefit involves strategic alignment and progress tracking. While compliance reporting is crucial, the primary benefit is internal improvement and alignment with strategic goals. For support or reporting issues, include Question ID: 6622f746c7ca975a319bdf6a in your ticket. Thank you.

QUESTION: 12

In the context of cybersecurity investments, what does Total Cost of Ownership (TCO) encompass?

Option A : The price comparison between different cybersecurity vendors over time
Option B : The potential savings gained by preventing cybersecurity incidents over time
Option C : The calculation of all costs associated with a cybersecurity solution throughout its lifecycle
Option D : The initial purchase price of cybersecurity hardware and software only

Correct Answer: C

Explanation/Reference:

The Total Cost of Ownership (TCO) includes initial purchase costs, ongoing operation and maintenance expenses, and any indirect costs such as training and downtime, providing a holistic view of the investment's financial impact. TCO helps in assessing overall costs but is not solely about comparing prices between vendors; it's about understanding all costs involved with a solution. TCO includes more than the initial purchase; it encompasses all associated costs over the life of the asset. While preventing incidents can result in savings, TCO primarily measures the total expenditure, not the savings. The savings would be related to the Return on Investment or Return on Assets. For support or reporting issues, include Question ID: 662307630098829f7463d4fd in your ticket. Thank you.

QUESTION: 13

What advantage does the Cyber Risk Institute (CRI) Profile offer to financial institutions implementing the NIST Cybersecurity Framework?

Option A : To provide a uniform cybersecurity training program for all employees within the sector
Option B : To replace existing financial regulations with a newer and more secure standard
Option C : To enforce a minimum cybersecurity budget across all financial institutions
Option D : To align measures with financial regulatory requirements, streamlining compliance efforts

Correct Answer: D

Explanation/Reference:

The CRI Profile is specifically tailored to the financial sector, helping institutions align their cybersecurity practices with regulatory requirements and streamline their compliance processes. While training is part of a comprehensive cybersecurity strategy, the CRI Profile primarily focuses on aligning security measures with regulatory requirements, not on uniform training programs. The CRI Profile does not replace existing regulations but works within the framework of existing laws to enhance cybersecurity. The CRI Profile does not dictate financial spending but focuses on aligning cybersecurity practices with specific sector needs and compliance requirements. For support or reporting issues, include Question ID: 66230246c7ca975a319bdfba in your ticket. Thank you.

QUESTION: 14

Which of the following information security publications provides standards for cloud service providers' security measures and can be used to complement the NIST Cybersecurity Framework outcomes for cloud migrations and adoptions?

Option A : FedRAMP
Option B : PCI-DSS
Option C : HIPAA
Option D : OWASP

Correct Answer: A

Explanation/Reference:

FedRAMP (Federal Risk and Authorization Management Program) provides standards for cloud service providers' security measures and aligns with NIST Cybersecurity Framework outcomes, especially when organizations adopt cloud technologies. The Payment Card Industry Data Security Standard (PCI-DSS) focuses on payment card data security, the Health Insurance Portability and Accountability Act (HIPAA) relates to healthcare data protection, and the Open Web Application Security Project (OWASP) emphasizes web application security. FedRAMP specifically addresses security in cloud environments, making it the most complementary choice to NIST's framework for cloud adoption. For support or reporting issues, include Question ID: 664794d8b2f0e96dc750b854 in your ticket. Thank you.

QUESTION: 15

Which of the following terms best describes the assurance that digital systems, services, and resources are accessible and usable when needed, without disruptions or services being denied?

Option A : Integrity
Option B : Non-repudiation
Option C : Availability
Option D : Confidentiality

Correct Answer: C

Explanation/Reference:

Availability is the assurance that digital systems, services, and resources are accessible and usable when needed, without disruptions or services being denied. Non-repudiation is the assurance that the originator of a digital communication or transaction cannot deny their involvement or the authenticity of the data being exchanged. Confidentiality is the protection of sensitive information from unauthorized access or disclosure by ensuring that only authorized individuals or entities can access

and view confidential data. Integrity involves ensuring that data remains accurate, consistent, and unaltered throughout its lifecycle by protecting it against unauthorized modification, deletion, or corruption. For support or reporting issues, include Question ID: 66199685fd737f4da3960271 in your ticket. Thank you.

QUESTION: 16

Which of the following best describes the purpose of the Asset Management (ID.AM) category?

Option A : To audit and assess the efficiency of an organization's cybersecurity measures
Option B : To provide financial resources for proposed cybersecurity improvements
Option C : To identify and manage all assets that support organizational objectives
Option D : To implement technical controls and defenses for digital and physical assets

Correct Answer: C

Explanation/Reference:

The ID.AM category directly involves identifying and managing assets to ensure that they are aligned with the organization's risk strategy and business requirements. While implementing defenses is important, the ID.AM category specifically focuses on identifying and managing the data, personnel, devices, systems, and facilities that enable the organization to achieve its purposes. The ID.AM category does not focus on financial resource allocation but on identifying and managing assets critical to an organization's cybersecurity. While auditing is crucial, the ID.AM category's primary focus is on managing assets rather than auditing cybersecurity measures. For support or reporting issues, include Question ID: 661c92cd090aba64a3425d14 in your ticket. Thank you.

QUESTION: 17

A company's IT department has identified an increase in phishing attacks targeting employees. To address this cybersecurity risk, what strategic action should be included in their comprehensive cybersecurity strategy?

Option A : Outsource all email management to a third-party provider without implementing additional security measures
Option B : Upgrade the physical security systems within company facilities
Option C : Decrease the frequency of network security audits to allocate more resources to training and other phishing defenses
Option D : Implement a continuous employee training program focused on recognizing and responding to phishing attempts

Correct Answer: D

Explanation/Reference:

Including continuous training in the cybersecurity strategy directly addresses the risk of phishing by empowering employees with the knowledge to recognize and avoid malicious attempts, thus reducing the likelihood of successful attacks. Outsourcing email management could potentially reduce some risks, but without specific additional security measures for phishing, this does not fully address the identified threat. While physical security is important, it does not address the specific risk of phishing attacks, which are digital in nature. Decreasing the frequency of network security audits could undermine overall security posture and does not strategically align with addressing the digital threat of phishing. For support or reporting issues, include Question ID: 6624007b1715796cddf78fba in your ticket. Thank you.

QUESTION: 18

Which of the following occurs within the Protect function of the NIST Cybersecurity Framework?

Option A : Establishing data encryption and secure information storage solutions
Option B : Documenting and communicating cybersecurity risks to stakeholders
Option C : Conducting forensic analysis after a security incident
Option D : Identifying the cause of an adverse cybersecurity incident

Correct Answer: A

Explanation/Reference:

The Protect function in the NIST Cybersecurity Framework is used by organizations to develop and implement safeguards to ensure the delivery of critical services and the protection of physical and digital assets against cyber threats. For support or reporting issues, include Question ID: 66199baffd737f4da39602c1 in your ticket. Thank you.

QUESTION: 19

Which of the following is a goal within the Detect function of the NIST Cybersecurity Framework?

Option A : To establish processes for identifying cybersecurity events
Option B : To restore services and capabilities after a cybersecurity incident
Option C : To develop strategies for reacting to a cybersecurity incident
Option D : To ensure continuous monitoring to find cybersecurity events quickly

Correct Answer: D

Explanation/Reference:

The Detect function in the NIST Cybersecurity Framework is used by organizations to develop and implement appropriate

activities to identify the occurrence of a cybersecurity event through timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events. The Govern function involves creating, communicating, implementing, monitoring, and overseeing an organization's cybersecurity risk management strategy, expectations, and policy. The Recover function in the NIST Cybersecurity Framework helps an organization develop and implement appropriate activities to maintain resilience plans and restore any capabilities or services that were impaired due to a cybersecurity incident. The Respond function in the NIST Cybersecurity Framework is used by organizations to develop and implement appropriate activities to perform actions regarding a detected cybersecurity incident. For support or reporting issues, include Question ID: 66199c44fd737f4da39602cb in your ticket. Thank you.

QUESTION: 20

An e-commerce company is upgrading its cybersecurity measures to include automated tools that detect and respond to unusual network traffic, which could indicate a cyber attack. They aim to quickly contain any identified threats to prevent data breaches. Which subcategory in the NIST Cybersecurity Framework could best support the implementation of these automated detection and response systems?

Option A : GV.SC-01
Option B : DE.CM-01
Option C : PR.DS-01
Option D : ID.AM-04

Correct Answer: B

Explanation/Reference:

DE.CM-01 involves monitoring networks and network services to find potentially adverse events. GV.SC-01is concerned with ensuring a cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders. PR.DS-01 focuses on protecting data at rest, which is crucial for overall data security but does not directly involve monitoring network traffic or automated response systems. ID.AM-04 deals with external information systems, which is important for managing risks related to third-party services but not specifically for internal automated detection systems. For support or reporting issues, include Question ID: 661cb293f296c0d1d32d1fb1 in your ticket. Thank you.

QUESTION: 21

A financial services firm has established and documented cybersecurity policies and procedures that are consistently implemented across all branches. They conduct regular training sessions and audits to ensure that these practices are maintained and effective. What tier best describes their cybersecurity implementation?

Option A : Tier 1 (Partial)

Option B : Tier 2 (Risk Informed)
Option C : Tier 3 (Repeatable)
Option D : Tier 4 (Adaptive)

Correct Answer: C

Explanation/Reference:

Tier 3 (Repeatable) characterizes organizations where cybersecurity practices are well-established, documented, and consistently applied across the organization. Tier 1 (Partial) is too rudimentary for this scenario, as it pertains to organizations with informal, uncoordinated cybersecurity practices. Tier 4 (Adaptive) goes beyond consistent application, focusing on adapting cybersecurity measures in response to predictive analytics and advanced threat intelligence, which is not explicitly stated in the scenario. Tier 2 (Risk Informed) describes organizations that have begun to implement risk-informed policies, but without the consistency and thoroughness required for Tier 3. For support or reporting issues, include Question ID: 661d71c74a52a2e238128900 in your ticket. Thank you.

QUESTION: 22

A healthcare provider is enhancing its cybersecurity policies to better protect patient information, particularly by implementing stricter access controls and auditing mechanisms to detect any unauthorized access or data manipulation. This is part of their compliance efforts with health data protection regulations. Which subcategory in the NIST Cybersecurity Framework could best guide the implementation of these stricter access controls and auditing mechanisms?

Option A : PR.AA-05
Option B : DE.AE-02
Option C : GV.OV-01
Option D : PR.AT-02

Correct Answer: A

Explanation/Reference:

PR.AA-05 involves access permissions, entitlements, and authorizations being defined in a policy, managed, enforced, and reviewed, and incorporates the principles of least privilege and the separation of duties. DE.AE-02 focuses on detecting anomalies and events, which is important for identifying unauthorized access but does not directly guide the implementation of access controls. PR.AT-02 ensures that individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind. GV.OC-01 ensures that cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction. For support or reporting issues, include Question ID: 661cb2ecf296c0d1d32d1fb6 in your ticket. Thank you.

QUESTION: 23

An aeronautical engineering firm works primarily with the Department of Defense and relies heavily upon semiconductors that are manufactured outside the United States. They are concerned about the risk or attack surface associated with foreign made semiconductors. Which of the following subcategories in the NIST Cybersecurity Framework covers the firm's concern?

Option A : Asset Management
Option B : Risk Assessment
Option C : Data Security
Option D : Cybersecurity Supply Chain Risk Management

Correct Answer: D

Explanation/Reference:

Subcategories related to vendor risk assessment are primarily applied within the Cybersecurity Supply Chain Risk Management (GV.SC) category in the NIST Cybersecurity Framework. This category focuses on assessing and mitigating risks associated with the supply chain and external vendors. Risk Assessment (ID.RA) evaluates risks but may not specifically address vendor risks. Data Security (PR.DS) deals with safeguarding data but not necessarily vendor-related risk or risks related to the supply chain of a critical business. Asset Management (ID.AM) focuses on the identification and consistent management of assets that enable the organization to achieve business purposes relative to their importance to their organizational objectives and the organization's risk strategy. For support or reporting issues, include Question ID: 6647afe671aee918de72bd59 in your ticket. Thank you.

THANK YOU FOR DOWNLOADING CRF-002 UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our CRF-002 Exam Product

Visit Our Site to Purchase the Full Set of Actual CRF-002 Exam Questions With Answers.

Money Back Guarantee

Click The Link Below

https://certs4sale.com/AKYLADE/crf-002-pdf-exam-dumps