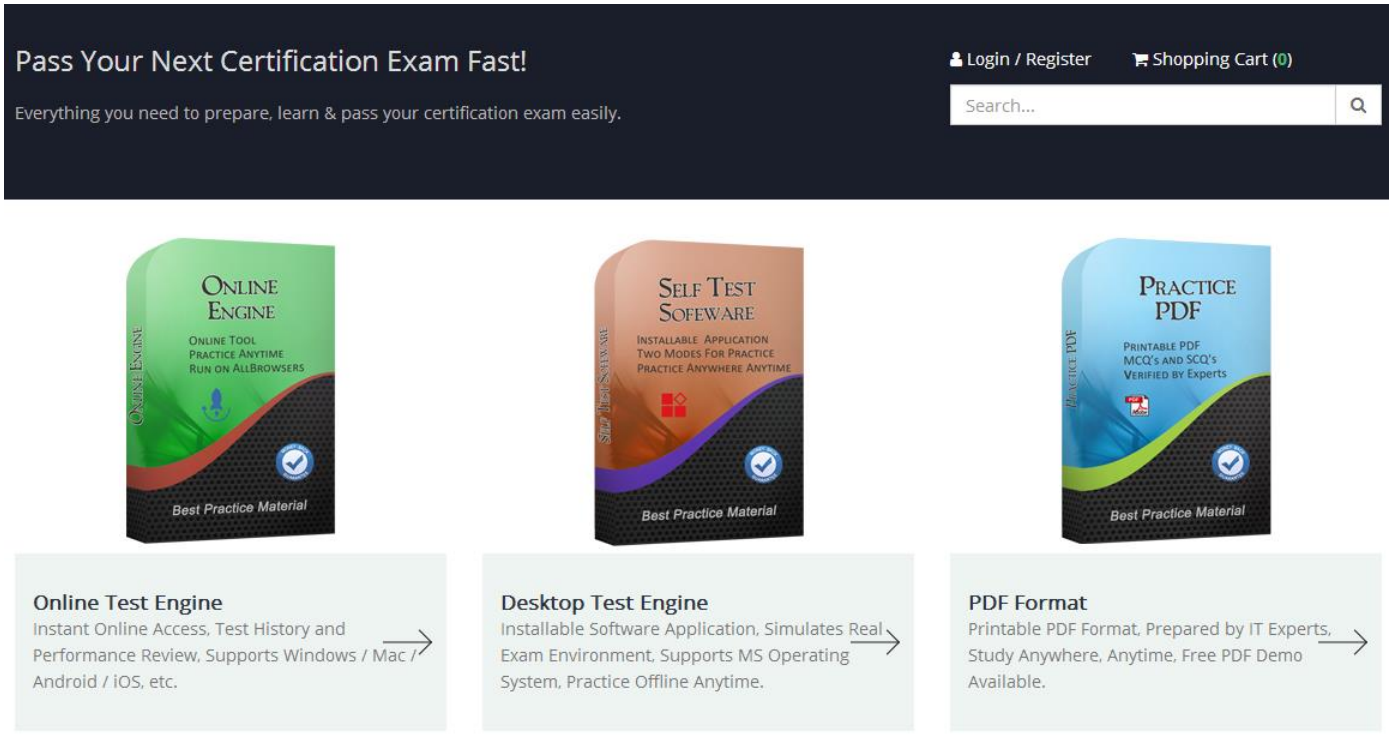
Actual4Labs



Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

http://www.actual4labs.com

Excellent Quality Exam Dumps Questions Never Let You down - Actual4Labs

Exam : **712-50-Deutsch**

Title : EC-Council Certified CISO (CCISO) (712-50 Deutsch Version)

Vendor : EC-COUNCIL

Version : DEMO

QUESTION NO: 1
Welcher der folgenden Prozesse gilt als einer der Eckpfeilerzyklen des Standards 27001 der Internationalen Organisation für Normung (ISO)?
A. Planen – Prüfen – Handeln
B. Plan-Do-Check-Act
C. Plan-Select-Implement-Evaluate
D. SCORE (Security Consensus Operational Readiness Evaluation)
Answer: B
Explanation:
ISO 27001 Core Cycle:
* Plan-Do-Check-Act (PDCA) is the cornerstone methodology in ISO 27001 for continual improvement of the Information Security Management System (ISMS).
Why This is Correct:
* Ensures systematic planning, implementation, monitoring, and refinement of security processes.
* Promotes a structured approach to maintaining and improving information security.
Why Other Options Are Incorrect:
* A. Plan-Check-Do-Act: Incorrect sequence.
* C. Plan-Select-Implement-Evaluate: Not a recognized ISO process.
* D. SCORE: A readiness evaluation tool, not an ISO process.
References:
EC-Council emphasizes PDCA as integral to ISO 27001's continuous improvement framework.

QUESTION NO: 2
Welche Gruppe überprüft in den meisten Organisationen regelmäßig die Systemprotokolle zur Erkennung von Netzwerkangriffen für alle Systeme als Teil ihrer täglichen Aufgaben?
A. Internes Audit
B. Datenbankverwaltung
C. Informationssicherheit
D. Einhaltung
Answer: C
Explanation:
Role of Information Security:
* The information security team is typically responsible for monitoring intrusion detection system (IDS) logs to identify and respond to threats.
Operational Responsibilities:
* Regular log reviews are a key task in maintaining network security and ensuring proactive threat management.
Supporting Reference:
* CCISO training describes log analysis and monitoring as core responsibilities of information security operations.

QUESTION NO: 3

Welche der folgenden Backup-Sites benötigt die längste Wiederherstellungszeit?
A. Kalte Seite
B. Heiße Seite
C. Warme Seite
D. Mobile Backup-Site
Answer: A
Explanation:
A cold site is a backup facility that provides minimal infrastructure and requires significant time to become operational after a disaster. It typically includes only basic physical space, utilities, and possibly some hardware.
* Definition of Backup Sites:
* Cold Site: Minimal or no IT infrastructure; requires setting up systems, installing software, and restoring data, leading to the longest recovery time.
* Hot Site: Fully equipped with operational IT infrastructure; minimal setup time required for recovery.
* Warm Site: Partially equipped with essential systems but requires additional setup and restoration before becoming fully operational.
* Mobile Backup Site: Portable and flexible backup sites with quicker setup times but still slower than hot sites.
* Recovery Time Comparison:
* Cold sites are cost-effective but slowest for recovery.
* They are suitable for organizations with lower criticality needs or budget constraints.
* Use Cases:
* Best for non-critical applications or organizations willing to tolerate extended downtime.
* Disaster Recovery Planning: EC-Council outlines the use of backup sites as part of a comprehensive disaster recovery plan, emphasizing the trade-offs between cost and recovery time.
* Risk Management Framework: The importance of selecting backup sites based on organizational risk tolerance and business continuity needs is stressed.

QUESTION NO: 4
Welcher Standard bietet einen Rahmen für das Informationssicherheitsrisikomanagement in Organisationen?
A. Informationssicherheitsmanagementsystem (ISMS)
B. Control Objectives for Information and Related Technology (COBIT)
C. Nationales Institut für Standards und Technologie (NIST)
D. Internationale Organisation für Normung (ISO) 27005
Answer: D
Explanation:
Comprehensive and Detailed Explanation (250-350 words)
According to EC-Council CCISO documentation, ISO/IEC 27005 is the international standard that provides a formal framework for information security risk management.
ISO 27005 supports ISO 27001 by defining structured processes for risk identification, analysis, evaluation, treatment, monitoring, and communication. CCISO materials highlight

ISO 27005 as the preferred risk management standard for organizations implementing or operating an ISMS.
An ISMS (Option A) is a management system, not a risk framework. COBIT (Option B) focuses on IT governance. NIST (Option C) is an organization that publishes frameworks, not a single risk standard.
Therefore, Option D is correct.

QUESTION NO: 5
Die Hauptbucheinrichtungsfunktion in einem Enterprise-Ressourcenpaket ermöglicht das Festlegen von Buchungszeiträumen. Der Zugriff auf diese Funktion wurde Benutzern in der Finanzabteilung, der Versandabteilung und der Produktionsplanung gestattet. Was ist der wahrscheinlichste Grund für einen so breiten Zugang?
A. Die Notwendigkeit, Rechnungsperioden regelmäßig zu ändern.
B. Die Anforderung, Einträge für eine abgeschlossene Buchungsperiode zu buchen.
C. Die Notwendigkeit, den Kontenplan und seine Zuordnungen zu erstellen und zu ändern.
D. Das Fehlen von Richtlinien und Verfahren für die ordnungsgemäße Aufgabentrennung.
Answer: D
Explanation:
* Granting broad access to critical functions like accounting period setups is often a result of inadequate segregation of duties.
* Proper policies would limit access to essential personnel, reducing the risk of errors or fraud.
Why Other Options Are Incorrect:
* A. Changing periods regularly: Does not justify access beyond finance personnel.
* B. Posting entries for a closed period: Limited personnel should handle this, not multiple departments.
* C. Chart of accounts modifications: A specialized task, not broadly needed across departments.
EC-Council CISO Reference:
Reinforces the need for strict access controls and clear segregation of duties as a security best practice.

QUESTION NO: 6
Datenflussdiagramme werden von IT-Auditoren verwendet, um:
A. Daten hierarchisch ordnen.
B. Datendefinitionen auf hoher Ebene hervorheben.
C. Datenpfade und Speichervorgänge grafisch zusammenfassen.
D. Stellen Sie Schritt für Schritt Details der Datengenerierung dar.
Answer: C
Explanation:
Purpose of Dataflow Diagrams:
* Visual representation of how data moves through a system, including paths, processes, and storage locations.
Why This is Correct:
* Provides auditors with an overview of system processes and data handling practices.

* Helps identify vulnerabilities or inefficiencies in data handling.
Why Other Options Are Incorrect:
* A. Order data hierarchically: Not the function of dataflow diagrams.
* B. Highlight high-level data definitions: Focuses on detail, not flow.
* D. Step-by-step details: Refers to process flows, not dataflows.
References:
Dataflow diagrams are a standard tool referenced by EC-Council for mapping data handling processes during audits.

QUESTION NO: 7
Welche der folgenden Funktionen wertet Patches aus, die zum Schließen von Software-Schwachstellen neuer Systeme verwendet werden, um die Einhaltung von Richtlinien bei der Implementierung eines Informationssicherheitsprogramms sicherzustellen?
A. Systemtest
B. Risikobewertung
C. Vorfallsreaktion
D. Planung
Answer: A
Explanation:
Role of System Testing:
System testing evaluates patches and updates to ensure they address vulnerabilities effectively and comply with organizational policies before deployment in live environments.
Key Actions:
* Verifies the functionality of patches and updates.
* Confirms that updates align with compliance requirements and do not introduce new vulnerabilities.
Why Not Other Options:
* Risk Assessment (B): Identifies risks but does not focus on testing patches.
* Incident Response (C): Manages incidents, not preventive patch evaluation.
* Planning (D): Focuses on strategic alignment rather than patch validation.
EC-Council Alignment:
System testing is critical to maintaining the integrity and compliance of systems, ensuring vulnerabilities are properly addressed.

QUESTION NO: 8
Welches ist die BESTE Lösung, um Änderungen an kritischen Daten in einem System zu überwachen, zu messen und zu melden?
A. Anwendungsprotokolle
B. Überwachung der Dateiintegrität
C. SNMP-Traps
D. Syslog
Answer: B
Explanation:
Purpose of File Integrity Monitoring (FIM):
* FIM tracks changes to critical files and directories, providing alerts for unauthorized or

unexpected modifications.
* Ensures integrity and compliance with standards like PCI-DSS.
Why This is Correct:
* Specifically designed to detect and report changes in critical data.
Why Other Options Are Incorrect:
* A. Application Logs: Track application events but lack specific focus on data changes.
* C. SNMP Traps: Focus on network device monitoring, not file integrity.
* D. Syslog: Centralizes logs but doesn't inherently monitor data changes.
References:
EC-Council recognizes FIM as the best tool for monitoring critical data integrity.

QUESTION NO: 9
Die jährliche Verlusterwartung wird aus der Funktion welcher beiden Faktoren abgeleitet?
A. Jährliche Häufigkeit und Vermögenswert
B. Einzelverlusterwartung und Risikofaktor
C. Schutzwert und jährliche Häufigkeit des Auftretens
D. Jährliche Eintrittsrate und Einzelschadenerwartung
Answer: D
Explanation:
Definition of Annual Loss Expectancy (ALE)
* ALE is a quantitative risk analysis metric used to estimate the annual financial impact of a risk.
* Formula: ALE = Annual Rate of Occurrence (ARO) × Single Loss Expectancy (SLE) Key Components
* Annual Rate of Occurrence (ARO): The estimated frequency of a specific risk occurring in a year.
* Single Loss Expectancy (SLE): The financial impact of a single occurrence of the risk, calculated as Asset Value × Exposure Factor.
Comparison of Options
* A. Annual Rate of Occurrence and Asset Value: Asset Value is used indirectly in SLE but not directly with ARO.
* B. Single Loss Expectancy and Exposure Factor: These factors combine to calculate SLE, not ALE.
* C. Safeguard Value and Annual Rate of Occurrence: Safeguard Value is unrelated to ALE calculation.
EC-Council References
* EC-Council frameworks and CISO resources consistently highlight ALE as a critical tool for financial risk assessment.

QUESTION NO: 10
Der Netzwerkadministrator möchte die physische Sicherheit in der Organisation stärken. Insbesondere, um eine Lösung zu implementieren, die Personen daran hindert, bestimmte Sperrzonen ohne ordnungsgemäße Anmeldeinformationen zu betreten. Welche der folgenden physischen Sicherheitsmaßnahmen sollte der Administrator anwenden?
A. Videoüberwachung

B. Menschenfalle
C. Poller
D. Zaun
Answer: D

QUESTION NO: 11
Szenario: Eine Organisation hat kürzlich einen CISO ernannt. Dies ist eine neue Rolle in der Organisation und signalisiert die zunehmende Notwendigkeit, Sicherheit konsequent auf Unternehmensebene anzugehen. Dieser neue CISO ist zwar zuversichtlich in Bezug auf Fähigkeiten und Erfahrung, befindet sich jedoch ständig in der Defensive und ist nicht in der Lage, die auf IT-Sicherheit ausgerichtete Agenda a voranzutreiben.
Der CISO war in der Lage, eine Reihe technischer Kontrollen zu implementieren und kann die IT-Teams beeinflussen, aber nicht den Rest der Organisation. Was ist aus organisatorischer Sicht der WAHRSCHEINLICHE Grund dafür?
A. Der CISO ist nicht direkt dem CEO der Organisation unterstellt
B. Der CISO berichtet an die IT-Organisation
C. Der CISO hat kein Framework für die Richtlinienverwaltung implementiert
D. Der CISO hat kein Sicherheitsbewusstseinsprogramm implementiert
Answer: B
Explanation:
Challenges of Reporting to IT
* When the CISO reports to the IT organization, their influence is often limited to technical teams, and they lack visibility and authority across other business units.
* Security needs to be seen as a business enabler, not just a technical function.
Why Not Other Options?
* A. Not reporting directly to the CEO: While ideal, reporting to the CEO is not always feasible and doesn't necessarily guarantee influence across the organization.
* C. Lack of policy framework: Important but secondary to organizational reporting structure.
* D. Lack of awareness program: Relevant but insufficient to explain the lack of organizational influence.
EC-Council References
* Highlights the strategic placement of the CISO within the organizational hierarchy to ensure enterprise- wide influence.

QUESTION NO: 12
Die Informationssicherheitsrichtlinie einer Organisation ist von HÖCHSTER Bedeutung, weil
A. Es kommuniziert die Verpflichtung des Managements zum Schutz von Informationsressourcen
B. Es wird von allen Mitarbeitern und Lieferanten offiziell anerkannt
C. Es definiert einen Prozess zur Erfüllung von Compliance-Anforderungen
D. Es schafft einen Rahmen zum Schutz vertraulicher Informationen
Answer: A
Explanation:
Purpose of an Information Security Policy:

* The policy serves as a foundational document that articulates the organization's commitment to safeguarding its information assets.
* It demonstrates management's intent and direction toward implementing robust security measures.
Management Commitment:
* As per EC-Council CCISO, management's visible commitment to security is essential for creating a culture of compliance and accountability across the organization.
* Policies provide a basis for decision-making, risk management, and incident response.
Supporting Reference:
* The CCISO program outlines that a well-documented and communicated information security policy ensures clarity in roles and responsibilities, fostering alignment among all stakeholders, including employees and vendors.

QUESTION NO: 13
Sie können derzeit keine 24/7-Abdeckung Ihrer Sicherheitsüberwachungs- und Vorfallreaktionspflichten gewährleisten, und Ihr Unternehmen widersetzt sich der Idee, mehr Vollzeitmitarbeiter auf die Gehaltsliste zu setzen. Welche Kombination von Lösungen würde dazu beitragen, die erforderliche Abdeckung bereitzustellen, ohne dass mehr engagiertes Personal hinzugefügt werden müsste? (wähle die beste Antwort):
A. Setzen Sie eine SEIM-Lösung ein und lassen Sie Vorfälle gleich morgens von aktuellen Mitarbeitern überprüfen
B. Vertrag mit einem Managed Security Provider und aktuelles Personal auf Abruf für die Reaktion auf Vorfälle
C. Konfigurieren Sie Ihr Syslog so, dass SMS-Nachrichten an aktuelle Mitarbeiter gesendet werden, wenn Zielereignisse ausgelöst werden
D. Verwenden Sie ein Annahmeprotokoll für Sicherheitsverletzungen und verteidigen Sie nur wesentliche Informationsressourcen
Answer: B
Explanation:
* Explanation:
* Contracting with a managed security service provider (MSSP) offers 24/7 monitoring and incident detection capabilities without adding full-time staff.
* Current staff can remain on-call for critical incident response, ensuring coverage without increasing headcount.
* Why Other Options Are Incorrect:
* A. Deploy a SEIM solution: While useful, a SEIM requires constant monitoring to be effective.
Simply reviewing incidents in the morning is insufficient.
* C. Configure syslog to send SMS messages: This approach lacks comprehensive monitoring and is reactive rather than proactive.
* D. Employ an assumption of breach protocol: This does not address the need for consistent monitoring and is not a direct solution to coverage gaps.
* EC-Council CISO Reference:The program highlights the value of MSSPs in enhancing organizational security capabilities while managing costs.

QUESTION NO: 14
In welchem der folgenden Fälle würde eine Organisation eher zur Risikoakzeptanz gegenüber Risikominderung neigen?
A. Die Organisation verwendet ausschließlich einen quantitativen Prozess zur Risikomessung
B. Die Organisation verwendet ausschließlich einen qualitativen Prozess zur Risikomessung
C. Die Risikotoleranz der Organisation ist hoch
D. Die Risikotoleranz der Organisation ist gering
Answer: C
Explanation:
Risk Acceptance vs. Mitigation:
* High risk tolerance allows an organization to accept risks instead of mitigating them, provided the potential impact is within acceptable thresholds.
Decision Dynamics:
* Organizations with high risk tolerance may prioritize cost savings or strategic objectives over implementing costly mitigation controls.
Supporting Reference:
* The CCISO framework discusses risk tolerance as a key determinant in choosing risk acceptance strategies, emphasizing alignment with organizational goals.

QUESTION NO: 15
Welches Enterprise-Architektur-Framework ist geschäftsorientiert und besteht aus acht Phasen?
A. Globale regulatorische Sicherheitsarchitektur
B. Das Open Group Architecture Framework (TOGAF)
C. Föderierte Unternehmensarchitektur
D. Control Objectives for Information Technology (COBIT)
Answer: B
Explanation:
Comprehensive and Detailed Explanation (250-350 words)
According to EC-Council CCISO documentation, TOGAF is a business-centric enterprise architecture framework composed of eight core phases within the Architecture Development Method (ADM).
TOGAF emphasizes aligning IT and security architecture with business strategy, which is why it is referenced in CCISO materials for enterprise-level planning. COBIT focuses on governance, not architecture phases. The other options are not recognized enterprise architecture frameworks within CCISO guidance.
Thus, Option B is correct.

QUESTION NO: 16
Das PRIMÄRE Ziel für die Entwicklung von Informationssicherheitsprogrammen sollte sein:
A. Verringerung der Auswirkungen des Risikos auf das Geschäft.
B. Herstellen einer strategischen Ausrichtung mit den Kontinuitätsanforderungen des Unternehmens

C. Erstellen von Incident-Response-Programmen.

D. Ermittlung und Implementierung der besten Sicherheitslösungen.

Answer: A

Explanation:

Objective of Information Security Programs:

The primary objective of an information security program is to manage risks in a manner that aligns with business goals and minimizes the impact of potential security incidents. This involves identifying risks, implementing appropriate controls, and ensuring that security measures are integrated into the organization's overall risk management framework.

Risk-Centric Approach:

The EC-Council emphasizes that information security programs should not merely focus on compliance or deploying the latest tools but on reducing risks that could disrupt business processes or cause harm to assets.

Alignment with Business Continuity:

While strategic alignment with business continuity requirements (Option B) is critical, it is part of the broader objective of reducing the overall impact of risks on the business.

References:

This is highlighted in the EC-Council's emphasis on aligning security initiatives with business strategies while prioritizing risk mitigation.

QUESTION NO: 17

Welche der folgenden Punkte ist am wichtigsten, wenn die Sicherheitsverantwortlichen einer Organisation die Sicherheit so ausrichten müssen, dass sie die Kultur einer Organisation beeinflusst?

A. Besitzt einen starken technischen Hintergrund

B. Alle Vorschriften verstehen, die die Organisation betreffen

C. Die Geschäftsziele der Organisation verstehen

D. Hat einen starken Auditing-Hintergrund

Answer: C

Explanation:

Aligning Security with Organizational Culture:

Security leaders must align security initiatives with business objectives to gain stakeholder support and integrate security into daily operations effectively.

Key Traits of Security Leaders:

* Business acumen to link security practices with organizational goals.
* The ability to communicate security's value in enabling business success.

Why Other Options Are Incorrect:

* A. Technical Background: Helpful but not sufficient for cultural influence.
* B. Understanding Regulations: Essential but secondary to business alignment.
* D. Auditing Background: Supports governance but does not directly influence culture.

References:

EC-Council emphasizes that understanding business goals is crucial for CISOs to align security with organizational priorities effectively.

QUESTION NO: 18

Was ist die wahrscheinlichste Erklärung dafür, dass eine Sicherheitsrichtlinie häufig ignoriert und nicht durchgesetzt wird?

A. Fehlende formale Risikomanagementfähigkeiten

B. Mangelnde ordnungsgemäße politische Steuerung

C. Fehlende formale Richtlinie für ein Sicherheitsbewusstseinsprogramm

D. Fehlende formale Definition von Rollen und Verantwortlichkeiten innerhalb der Richtlinie

Answer: B

Explanation:

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge identifies lack of proper policy governance as the most common reason security policies are ignored or unenforced. Policy governance includes executive sponsorship, ownership assignment, approval authority, enforcement mechanisms, and periodic review.

CCISO documentation explains that without governance, policies become theoretical documents with no accountability or enforcement power. Even well-written policies fail when leadership does not mandate compliance or assign responsibility for enforcement.

While awareness, role clarity, and risk management contribute to policy effectiveness, CCISO materials emphasize that governance is the root enabler. Governance ensures that policies are aligned with business objectives, formally approved, communicated, enforced, and audited.

Therefore, lack of proper policy governance is the most probable explanation.

QUESTION NO: 19

Welche der folgenden Lösungen eignet sich am besten zur Überwachung, Messung und Berichterstattung von Änderungen an kritischen Daten in einem System oder Repository?

A. Überwachung der Dateiintegrität

B. Anwendungsschnittstellen

C. Intrusion Detection Systems

D. Datenbankprotokollspeicherung

Answer: A

Explanation:

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge identifies File Integrity Monitoring (FIM) as the most effective solution for monitoring, measuring, and reporting changes to critical data, system files, and repositories. FIM tools establish a known-good baseline of files and continuously monitor for unauthorized or unexpected changes.

CCISO documentation emphasizes that integrity is a core pillar of the CIA triad, and FIM directly supports integrity assurance by detecting alterations caused by malware, insider threats, configuration drift, or unauthorized administrative activity. FIM solutions generate alerts, logs, and reports that provide auditable evidence of when changes occurred, what was changed, and often who initiated the change.

Intrusion Detection Systems focus on detecting malicious activity or traffic patterns, not on

validating the integrity of stored data. Database logs record transactions but do not inherently validate unauthorized changes or provide baseline comparison. Application interfaces enable access but do not monitor integrity.
CCISO guidance further notes that FIM is often required for regulatory compliance (e.g., PCI DSS, SOX) because it provides measurable, reportable assurance of data integrity.
Therefore, File Integrity Monitoring is the best solution.

QUESTION NO: 20
Sie sind der Chief Information Security Officer einer großen, multinationalen Bank und vermuten, dass ein Token-Verwaltungsprozess für die Zwei-Faktor-Authentifizierung einen Fehler aufweist. Welche der folgenden Vorgehensweisen ist Ihre BESTE Vorgehensweise?
A. Überprüfen Sie, ob der Inhalt des Sicherheitsbewusstseinsprogramms Informationen über die potenzielle Schwachstelle enthält
B. Führen Sie eine gründliche Risikobewertung der aktuellen Implementierung durch, um die Systemfunktionen zu bestimmen
C. Programmbesitz bestimmen, um kompensierende Kontrollen zu implementieren
D. Schicken Sie einen Bericht an Ihre Kollegen in der Geschäftsleitung und die Eigentümer der Geschäftseinheiten, in dem Sie Ihren Verdacht detailliert beschreiben
Answer: B
Explanation:
Risk Assessment as a Best Practice:
EC-Council CISO stresses that suspected vulnerabilities, especially in critical systems like two-factor authentication, require an immediate and thorough risk assessment. This ensures that risks are quantified and mitigation efforts are appropriately prioritized.
Steps in the Process:
* Conduct a detailed assessment of the token management process.
* Identify vulnerabilities, potential exploitation scenarios, and system dependencies.
* Assess the impact of the flaw on the organization's security posture.
Why Not Other Options:
* Security awareness (A) is important but doesn't address the root technical issue.
* Reporting suspicions (D) is premature without substantiating evidence.
* Determining program ownership (C) is part of the response plan but not the first step.
CISO Alignment:
This approach ensures a proactive, measured, and evidence-driven resolution to the issue.

QUESTION NO: 21
Welcher Geschäftspartner ist für die Integrität eines neuen Sicherheitssystems innerhalb des Security Operations Center (SOC) verantwortlich?
A. Chief Information Officer (CIO)
B. Chief Executive Officer (CEO)
C. Chief Compliance Officer (CCO)
D. Chief Information Security Officer (CISO)
Answer: D
Explanation:
Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief

Information Security Officer (CCISO) Documents:
The EC-Council CCISO Body of Knowledge clearly assigns accountability for the integrity and effectiveness of security systems to the Chief Information Security Officer (CISO). Within a Security Operations Center (SOC), the CISO is responsible for ensuring that security technologies operate as intended and support organizational risk objectives.
Integrity, as defined by CCISO guidance, refers to the accuracy, reliability, and trustworthiness of security systems and the data they produce. This includes SIEM platforms, detection tools, logging mechanisms, and response workflows.
While the CIO oversees IT infrastructure, and the CEO holds overall organizational accountability, CCISO materials emphasize that security system governance, validation, and assurance fall squarely under the CISO' s role. The Chief Compliance Officer ensures regulatory adherence but does not own operational security integrity.
Therefore, the correct and CCISO-validated answer is Chief Information Security Officer (CISO).

QUESTION NO: 22
Welche der folgenden Sicherheitskennzahlen ist die BESTE Wahl für die Präsentation vor einem Aufsichtsrat?
A. Sicherheitslücken auf Servern und Desktop-Computern gefunden
B. Alle Schwachstellen, die kritische Produktionsserver beeinträchtigen
C. Kritische und hohe Sicherheitslücken in Produktionsumgebungen
D. Kritische und hohe Sicherheitslücken bei Druckern und Faxgeräten
Answer: C
Explanation:
Comprehensive and Detailed Explanation:
CCISO guidance stresses that board-level metrics must be high-level, risk-focused, and business-relevant.
Reporting critical and high vulnerabilities in production environments communicates exposure without overwhelming technical detail.
Boards are concerned with material risk, not asset-level findings. Therefore, option C is correct.

QUESTION NO: 23
Welche der folgenden Aussagen veranschaulicht einen betrieblichen Kontrollprozess:
A. Einstufung eines Informationssystems im Rahmen einer Risikobewertung
B. Installieren eines geeigneten Feuerlöschsystems im Rechenzentrum
C. Durchführen eines Audits des Konfigurationsverwaltungsprozesses
D. Festlegung von Beschaffungsstandards für Cloud-Anbieter
Answer: B
Explanation:
Operational Control Processes:
* Operational controls are physical or procedural measures implemented to support security operations.
Installing fire suppression systems protects critical infrastructure from physical hazards.
Illustration:

* The example of fire suppression directly aligns with operational controls, ensuring the safety of the physical environment.
Supporting Reference:
* CCISO materials classify fire suppression systems as operational controls focused on maintaining secure and resilient environments.

QUESTION NO: 24
Welche Schlüsseltechnologie kann Ransomware-Bedrohungen mindern?
A. Unveränderlichen Datenspeicher verwenden
B. Phishing-Übungen
C. Anwendung von Anti-Malware-Lösungen für mehrere Endpunkte
D. Blockieren der Nutzung drahtloser Netzwerke
Answer: A
Explanation:
Immutable data storage protects against ransomware threats by ensuring that once data is written, it cannot be altered or deleted. This technology prevents ransomware from encrypting or modifying critical backups, enabling rapid restoration. Options B, C, and D are valuable for prevention and awareness but do not provide the direct protection against ransomware that immutable storage offers.
Reference: https://cloud.google.com/blog/products/identity-security/5-pillars-of-protection-to-prevent- ransomware-attacks

QUESTION NO: 25
Welche Rolle sollte der CISO beim richtigen Scoping einer PCI-Umgebung spielen?
A. Validieren Sie die Vorschläge der Geschäftsbereiche, was in den Scoping-Prozess aufgenommen werden sollte
B. Arbeiten Sie mit einem Qualified Security Assessor (QSA) zusammen, um den Umfang der PCI-Umgebung zu bestimmen
C. Stellen Sie sicher, dass die interne Bereichsvalidierung abgeschlossen ist und dass eine Bewertung durchgeführt wurde, um alle Kreditkartendaten zu ermitteln
D. Füllen Sie den Fragebogen zur Selbsteinschätzung aus und arbeiten Sie mit einem zugelassenen Scanning-Anbieter (ASV) zusammen, um den Umfang zu bestimmen
Answer: C
Explanation:
Role of the CISO in PCI Scoping:
* The CISO is responsible for ensuring that all credit card data locations are identified and properly assessed during the scoping process. This includes internal validation to confirm scope accuracy.
Compliance Assurance:
* Thorough scope validation is crucial for meeting PCI DSS requirements and avoiding compliance gaps.
Supporting Reference:
* CCISO materials identify the CISO's role as pivotal in scoping PCI environments to ensure all relevant systems and processes are accounted for.

QUESTION NO: 26
Welche Funktion erfüllt Management Response im Hinblick auf den Auditmanagementprozess?
A. Melden von leistungsschwachen Einheiten wegen Nichterfüllung von Standards
B. Bestimmen, ob Ressourcen zugewiesen werden, um einen Befund zu beheben
C. Hinzufügen von Kontrollen, um sicherzustellen, dass eine angemessene Aufsicht durch das Management erreicht wird
D. Aufdecken der „Grundursache“ des Prozessausfalls und Abmilderung für alle internen und externen Einheiten
Answer: B
Explanation:
Function of Management Response in Audits:
* The management response evaluates audit findings and decides on resource allocation for addressing identified issues.
Purpose:
* This step ensures that management's priorities align with the organization's risk management and operational goals.
Supporting Reference:
* CCISO materials emphasize management's role in assessing and addressing audit findings to improve organizational processes.

QUESTION NO: 27
Die durchschnittliche Zeit bis zum Patchen, die Anzahl der verhinderten Virusausbrüche und die Anzahl der behobenen Sicherheitslücken sind Beispiele für welche Art von Leistungskennzahlen?
A. Definierte Metriken
B. Betriebskennzahlen
C. Auditmetriken
D. Managementkennzahlen
Answer: B
Explanation:
Comprehensive and Detailed Explanation:
CCISO materials define operational metrics as measurements of day-to-day security activities and control performance. These metrics track effectiveness of operational processes such as patching, malware prevention, and vulnerability remediation.

QUESTION NO: 28
Eine Methode zur Risikoübertragung ist:
A. Redundanz implementieren
B. Operationen in eine andere Region verschieben
C. Kauf einer Verletzungsversicherung
D. Ausrichtung auf den Geschäftsbetrieb
Answer: C
Explanation:

Risk Transfer Through Insurance:
* Breach insurance is a common method of transferring financial risks associated with cybersecurity incidents, covering costs like fines, legal fees, and recovery.
Risk Management Strategies:
* Risk transfer does not eliminate the risk but provides financial safeguards, complementing other security measures.
Supporting Reference:
* EC-Council CCISO materials describe purchasing insurance as a key financial strategy in the risk transfer process.

QUESTION NO: 29
Effektive Informationssicherheits-Managementprogramme erfordern die aktive Beteiligung von_____
A. CIOS
B. Alle Mitarbeiter
C. Sicherheitsmanager
D. Führungskräfte
Answer: B

QUESTION NO: 30
Risiko ist definiert als:
A. Bedrohung mal Verwundbarkeit dividiert durch Kontrolle
B. Beratung plus Fähigkeit plus Schwachstelle
C. Vermögensverlust multipliziert mit der Wahrscheinlichkeit des Ereignisses
D. Quantitative plus qualitative Auswirkung
Answer: C
Explanation:
Definition of Risk:
* Risk is calculated by multiplying the asset value or potential loss by the likelihood of a threat event occurring.
Mathematical Basis:
* This formula underpins quantitative risk assessments and guides mitigation priorities.
Supporting Reference:
* CCISO training outlines this calculation as standard practice in risk analysis methodologies.

QUESTION NO: 31
Ein global tätiges Einzelhandelsunternehmen entwickelt einen neuen Compliance-Management-Prozess. Welcher der folgenden Standards wäre von primärer Bedeutung?
A. Internationale Organisation für Normung (ISO)
B. Nationales Institut für Standards und Technologie (NIST)
C. Payment Card Industry Data Security Standard (PCI DSS)
D. Information Technology Infrastructure Library (ITIL)
Answer: C
Explanation:

Comprehensive and Detailed Explanation (250-350 words)
According to EC-Council CCISO documentation, a global retail organization's primary compliance obligation relates to the protection of payment card data, making PCI DSS the most critical standard.
PCI DSS is a mandatory, industry-specific compliance standard enforced by payment brands and acquirers.
CCISO materials highlight that failure to comply can result in fines, increased transaction fees, loss of card processing privileges, and reputational damage.
ISO and NIST (Options A and B) provide broad frameworks and best practices, while ITIL (Option D) focuses on service management. None impose direct, enforceable obligations on retail payment environments.
Thus, Option C is correct.

QUESTION NO: 32
Welcher der folgenden Aspekte ist der wichtigste einer Sicherheitsrichtlinie?
A. Klar definierte Prozesse zur Erfüllung der Compliance-Anforderungen
B. Formale Bestätigung durch die meisten Mitarbeiter und Lieferanten
C. Eine etablierte Richtlinie zum Schutz vertraulicher Informationen
D. Kommunikation des Engagements des Managements für die Sicherheit
Answer: D
Explanation:
Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:
CCISO documentation stresses that the most critical aspect of a security policy is visible communication of management's commitment. Leadership endorsement establishes authority, accountability, and enforceability.
Processes, acknowledgements, and guidelines are important, but without leadership commitment, policies are ignored. CCISO materials consistently identify leadership commitment as the foundation of policy effectiveness.

QUESTION NO: 33
Ein Chief Information Security Officer erhielt eine Liste mit Prüfungsergebnissen mit hoher, mittlerer und geringer Auswirkung. Welche der folgenden Vorgehensweisen stellt die BESTE Vorgehensweise dar?
A. Wenn sich die Befunde auf die Einhaltung gesetzlicher Vorschriften auswirken, versuchen Sie, Abhilfemaßnahmen anzuwenden, die die meisten Befunde zu den geringsten Kosten beheben.
B. Wenn sich die Befunde nicht auf die Einhaltung gesetzlicher Vorschriften auswirken, beheben Sie nur die Befunde mit hohem und mittlerem Risiko.
C. Wenn sich die Befunde auf die Einhaltung gesetzlicher Vorschriften auswirken, beheben Sie die hohen Befunde so schnell wie möglich.
D. Wenn sich die Ergebnisse nicht auf die Einhaltung gesetzlicher Vorschriften auswirken, überprüfen Sie die aktuellen Sicherheitskontrollen.
Answer: C
Explanation:

Regulatory Compliance Priority:
Compliance-related findings are typically high priority because they directly impact the organization's legal and operational obligations. The EC-Council CISO curriculum emphasizes that compliance issues must be addressed promptly to avoid penalties, reputational damage, and legal consequences.
Focus on High-Impact Findings:
High-impact findings often represent the most critical risks to the organization, whether due to potential financial, operational, or reputational harm. Resolving these first aligns with risk management best practices as outlined in the EC-Council CISO program.
Remediation Steps:
* Identify which findings impact regulatory compliance.
* Prioritize high-impact findings for immediate remediation.
* Develop a remediation plan that aligns with regulatory and organizational risk thresholds.
EC-Council CISO Emphasis:
This approach ensures alignment with compliance and strategic risk mitigation while fostering regulatory confidence.

QUESTION NO: 34
Welche der folgenden Informationen können in Tabletop-Übungen zur Reaktion auf Vorfälle gefunden werden?
A. Erhöhung des Sicherheitsbudgets
B. Prozessverbesserungen
C. Echtzeit zur Behebung
D. Auswahl der Sicherheitskontrolle
Answer: B

QUESTION NO: 35
Szenario: Ihre Unternehmenssysteme werden seit mehr als einer Woche ständig von fremden IP-Adressen untersucht und angegriffen. Ihr Sicherheitsteam und Ihre Sicherheitsinfrastruktur haben sich unter der Belastung gut bewährt. Sie sind zuversichtlich, dass Ihre Verteidigung dem Test standgehalten hat, aber es gehen Gerüchte um, dass sensible Kundendaten gestohlen wurden und nun von kriminellen Elementen im Internet verkauft werden. Während Ihrer Untersuchung der angeblichen Kompromittierung stellen Sie fest, dass Daten kompromittiert wurden, und Sie haben das Repository gestohlener Daten auf einem Server entdeckt, der sich im Ausland befindet. Ihr Team hat nun vollen Zugriff auf die Daten auf dem fremden Server.
Welche Maßnahmen sollten Sie ZUERST ergreifen?
A. Zerstöre das Depot gestohlener Daten
B. Wenden Sie sich an Ihre örtliche Strafverfolgungsbehörde
C. Beraten Sie sich mit anderen C-Level-Führungskräften, um einen Aktionsplan zu entwickeln
D. Vertrag mit einer Kreditauskunftei über kostenpflichtige Überwachungsdienste für betroffene Kunden
Answer: B
Explanation:

Appropriate First Action After a Data Breach
* Engaging law enforcement ensures proper handling of the breach within the legal framework, particularly when dealing with data stored on foreign servers.
* Unauthorized actions, such as destroying data, may have legal repercussions and hinder investigations.
Why Not Other Options?
* A. Destroy the repository of stolen data: Illegal and could result in evidence tampering.
* C. Consult with C-Level executives: Important but secondary to legal compliance.
* D. Contract with credit monitoring services: A remediation step that follows breach confirmation and law enforcement involvement.
EC-Council References
* Emphasizes involving legal authorities and following incident response procedures to ensure compliance.