QUESTION 406
Which of the following statements below regarding Key Performance indicators (KPIs) are true?

A. Development of KPI's are most useful when done independently
B. They are a strictly quantitative measure of success
C. They should be standard throughout the organization versus domain-specific so they are more easily correlated
D. They are a strictly qualitative measure of success

Answer: A
Explanation:
https://kpi.org/KPI-Basics/KPI-Development

QUESTION 407
When information security falls under the Chief Information Officer (CIO), what is their MOST essential role?

A. Oversees the organization's day-to-day operations, creating the policies and strategies that govern operations
B. Enlisting support from key executives the information security program budget and policies
C. Charged with developing and implementing policies designed to protect employees and customers' data from unauthorized access
D. Responsible for the success or failure of the IT organization and setting strategic direction

Answer: D
Explanation:
https://www.investopedia.com/terms/c/cio.asp

QUESTION 408
ABC Limited has recently suffered a security breach with customers' social security number available on the dark web for sale. The CISO, during the time of the incident, has been fired, and you have been hired as the replacement. The analysis of the breach found that the absence of an insider threat program, lack of least privilege policy, and weak access control was to blame.
You would like to implement key performance indicators to mitigate the risk.
Which metric would meet the requirement?

A. Number of times third parties access critical information systems
B. Number of systems with known vulnerabilities
C. Number of users with elevated privileges
D. Number of websites with weak or misconfigured certificates

Answer: C

QUESTION 409
An organization recently acquired a Data Loss Prevention (DLP) solution, and two months after the implementation, it was found that sensitive data was posted to numerous Dark Web sites. The DLP application was checked, and there are no apparent malfunctions and no errors. What is the MOST likely reason why the sensitive data was posted?

A. The DLP Solution was not integrated with mobile device anti-malware
B. Data classification was not properly performed on the assets
C. The sensitive data was not encrypted while at rest
D. A risk assessment was not performed after purchasing the DLP solution

Answer: D

QUESTION 410
The main purpose of the SOC is:

A. An organization which provides Tier 1 support for technology issues and provides escalation when needed
B. A distributed organization which provides intelligence to governments and private sectors on cyber-criminal activities
C. The coordination of personnel, processes and technology to identify information security events and provide timely response and remediation
D. A device which consolidates event logs and provides real-time analysis of security alerts generated by applications and network hardware

Answer: C
Explanation:
https://www.eccouncil.org/what-is-soc/

QUESTION 411
When obtaining new products and services, why is it essential to collaborate with lawyers, IT security professionals, privacy professionals, security engineers, suppliers, and others?

A. This makes sure the files you exchange aren't unnecessarily flagged by the Data Loss Prevention (DLP) system
B. Contracting rules typically require you to have conversations with two or more groups
C. Discussing decisions with a very large group of people always provides a better outcome
D. It helps to avoid regulatory or internal compliance issues

Answer: D
Explanation:
https://www.eccouncil.org/wp-content/uploads/2016/07/NICE-2.0-and-EC-Council-Cert-Mapping.pdf

QUESTION 412
A cloud computing environment that is bound together by technology that allows data and applications to be shared between public and private clouds is BEST referred to as a?

A. Public cloud
B. Private cloud
C. Community cloud
D. Hybrid cloud

Answer: D
Explanation:
https://www.datacenters.com/services/cloud-services#:~:text=Hybrid%20clouds%20combine%20public%20and,flexibility%20and%20more%20dep

loyment%20options

QUESTION 413
When reviewing a Solution as a Service (SaaS) provider's security health and posture, which key document should you review?

A. SaaS provider's website certifications and representations (certs and reps)
B. SOC-2 Report
C. Metasploit Audit Report
D. Statement from SaaS provider attesting their ability to secure your data

Answer: B
Explanation:
https://www.threatstack.com/blog/how-saas-companies-can-build-a-compliance-roadmap

QUESTION 414
As the Risk Manager of an organization, you are task with managing vendor risk assessments. During the assessment, you identified that the vendor is engaged with high profiled clients, and bad publicity can jeopardize your own brand. Which is the BEST type of risk that defines this event?

A. Compliance Risk
B. Reputation Risk
C. Operational Risk
D. Strategic Risk

Answer: B

QUESTION 415
What is a Statement of Objectives (SOA)?

A. A section of a contract that defines tasks to be performed under said contract
B. An outline of what the military will do during war
C. A document that outlines specific desired outcomes as part of a request for proposal
D. Business guidance provided by the CEO

Answer: A

QUESTION 416
During a cyber incident, which non-security personnel might be needed to assist the security team?

A. Threat analyst, IT auditor, forensic analyst
B. Network engineer, help desk technician, system administrator
C. CIO, CFO, CSO
D. Financial analyst, payroll clerk, HR manager

Answer: A

QUESTION 417
With a focus on the review and approval aspects of board responsibilities, the Data Governance Council recommends that the boards provide strategic oversight regarding information and information security, include these four things:

A. Metrics tracking security milestones, understanding criticality of information and information security, visibility into the types of information and how it is used, endorsement by the board of directors
B. Annual security training for all employees, continual budget reviews, endorsement of the development and implementation of a security program, metrics to track the program

C. Understanding criticality of information and information security, review investment in information security, endorse development and implementation of a security program, and require regular reports on adequacy and effectiveness
D. Endorsement by the board of directors for security program, metrics of security program milestones, annual budget review, report on integration and acceptance of program

Answer: C
Explanation:
https://nanopdf.com/download/information-security-governance-guidance-for-boards-of_pdf (9)

QUESTION 418
You are the CISO for an investment banking firm. The firm is using artificial intelligence (AI) to assist in approving clients for loans.
Which control is MOST important to protect AI products?

A. Hash datasets
B. Sanitize datasets
C. Delete datasets
D. Encrypt datasets

Answer: D

QUESTION 419
Which level of data destruction applies logical techniques to sanitize data in all user-addressable storage locations?

A. Purge
B. Clear
C. Mangle
D. Destroy

Answer: B
Explanation:
https://it.brown.edu/computing-policies/electronic-equipment-disposition-policy/data-removal-recommendations

QUESTION 420
A university recently hired a CISO. One of the first tasks is to develop a continuity of operations plan (COOP).
In developing the business impact assessment (BIA), which of the following MOST closely relate to the data backup and restoral?

A. Recovery Point Objective (RPO)
B. Mean Time to Delivery (MTD)
C. Recovery Time Objective (RTO)
D. Maximum Tolerable Downtime (MTD)

Answer: C
Explanation:
https://www.druva.com/glossary/what-is-a-recovery-point-objective-definition-and-related-faqs/#:~:text=The%20recovery%20time%20objective%20(RTO,consequences%20associated%20with%20the%20disruption

QUESTION 421
A key cybersecurity feature of a Personal Identification Verification (PIV) Card is:

A. Inability to export the private certificate/key
B. It can double as physical identification at the DMV
C. It has the user's photograph to help ID them

D. It can be used as a secure flash drive

Answer: C
Explanation:
https://www.securew2.com/blog/piv-personal-identity-verification

QUESTION 422
When performing a forensic investigation, what are the two MOST common data sources for obtaining evidence from a computer and mobile devices?

A. RAM and unallocated space
B. Unallocated space and RAM
C. Slack space and browser cache
D. Persistent and volatile data

Answer: D
Explanation:
https://study.com/academy/lesson/data-storage-formats-digital-forensics-devices-types.html

QUESTION 423
To make sure that the actions of all employees, applications, and systems follow the organization's rules and regulations can BEST be described as which of the following?

A. Compliance management
B. Asset management
C. Risk management
D. Security management

Answer: D
Explanation:
https://www.eccouncil.org/information-security-management/

QUESTION 424
You have been hired as the Information System Security Officer (ISSO) for a US federal government agency. Your role is to ensure the security posture of the system is maintained. One of your tasks is to develop and maintain the system security plan (SSP) and supporting documentation. Which of the following is NOT documented in the SSP?

A. The controls in place to secure the system
B. Name of the connected system
C. The results of a third-party audits and recommendations
D. Type of information used in the system

Answer: C
Explanation:
https://www.govinfo.gov/content/pkg/GOVPUB-C13-63e84ab7af43b36228f10e4f0b5f8c38/pdf/GOVPUB-C13-63e84ab7af43b36228f10e4f0b5f8c38.pdf (65)

QUESTION 425
Who should be involved in the development of an internal campaign to address email phishing?

A. Business unit leaders, CIO, CEO
B. Business Unite Leaders, CISO, CIO and CEO
C. All employees
D. CFO, CEO, CIO

Answer: B

QUESTION 426
Of the following types of SOCs (Security Operations Centers), which one would be MOST likely used if the CISO has decided to outsource the infrastructure and administration of it?

A. Virtual
B. Dedicated
C. Fusion
D. Command

Answer: A
Explanation:
https://www.techtarget.com/searchsecurity/definition/Security-Operations-Center-SOC

QUESTION 427
Many successful cyber-attacks currently include:

A. Phishing Attacks
B. Misconfigurations
C. Social engineering
D. All of these

Answer: C
Explanation:
https://www.eccouncil.org/what-is-social-engineering/

QUESTION 428
When evaluating a Managed Security Services Provider (MSSP), which service(s) is/are most important:

A. Patch management
B. Network monitoring
C. Ability to provide security services tailored to the business' needs
D. 24/7 tollfree number

Answer: C
Explanation:
https://digitalguardian.com/blog/how-hire-evaluate-managed-security-service-providers-mssps

QUESTION 429
Which of the following strategies provides the BEST response to a ransomware attack?

A. Real-time off-site replication
B. Daily incremental backup
C. Daily full backup
D. Daily differential backup

Answer: B

QUESTION 430
What is the MOST critical output of the incident response process?

A. A complete document of all involved team members and the support they provided
B. Recovery of all data from affected systems
C. Lessons learned from the incident, so they can be incorporated into the incident response processes

D. Clearly defined documents detailing standard evidence collection and preservation processes

Answer: C
Explanation:
https://www.eccouncil.org/incident-response-plan-phases/

QUESTION 431
Who is responsible for verifying that audit directives are implemented?

A. IT Management
B. Internal Audit
C. IT Security
D. BOD Audit Committee

Answer: B
Explanation:
https://www.eccouncil.org/information-security-management/

QUESTION 432
XYZ is a publicly-traded software development company. Who is ultimately accountable to the shareholders in the event of a cybersecurity breach?

A. Chief Financial Officer (CFO)
B. Chief Software Architect (CIO)
C. CISO
D. Chief Executive Officer (CEO)

Answer: C
Explanation:
https://www.eccouncil.org/information-security-management/

QUESTION 433
What organizational structure combines the functional and project structures to create a hybrid of the two?

A. Traditional
B. Composite
C. Project
D. Matrix

Answer: D
Explanation:
https://www.knowledgehut.com/tutorials/project-management/organization-structures

QUESTION 434
The primary responsibility for assigning entitlements to a network share lies with which role?

A. CISO
B. Data owner
C. Chief Information Officer (CIO)
D. Security system administrator

Answer: B
Explanation:
https://resources.infosecinstitute.com/certification/data-and-system-ownership/

QUESTION 435

What does RACI stand for?

A. Reasonable, Actionable, Controlled, and Implemented
B. Responsible, Actors, Consult, and Instigate
C. Responsible, Accountable, Consulted, and Informed
D. Review, Act, Communicate, and Inform

Answer: C
Explanation:
https://www.google.com/search?q=What+does+RACI+stand+for&oq=What+does+RACI+stand+for&aqs=edge..69i57.220j0j4&sourceid=chrome&ie=UTF-8

QUESTION 436
What key technology can mitigate ransomware threats?

A. Use immutable data storage
B. Phishing exercises
C. Application of multiple end point anti-malware solutions
D. Blocking use of wireless networks

Answer: A
Explanation:
https://cloud.google.com/blog/products/identity-security/5-pillars-of-protection-to-prevent-ransomware-attacks

QUESTION 437
Which of the following are the triple constraints of project management?

A. Time, quality, and scope
B. Cost, quality, and time
C. Scope, time, and cost
D. Quality, scope, and cost

Answer: C
Explanation:
https://www.teamgantt.com/blog/triple-constraint-project-management#:~:text=Each%20side%20or%20point%20of,scope%2C%20time%2C%20and%20cost

QUESTION 438
A Security Operations (SecOps) Manager is considering implementing threat hunting to be able to make better decisions on protecting information and assets. What is the MAIN goal of threat hunting to the SecOps Manager?

A. Improve discovery of valid detected events
B. Enhance tuning of automated tools to detect and prevent attacks
C. Replace existing threat detection strategies
D. Validate patterns of behavior related to an attack

Answer: A
Explanation:
https://www.techtarget.com/searchsecurity/feature/7-SecOps-roles-and-responsibilities-for-the-modern-enterprise

QUESTION 439
A bastion host should be placed:

A. Inside the DMZ
B. In-line with the data center firewall

C. Beyond the outer perimeter firewall
D. As the gatekeeper to the organization's honeynet

Answer: C
Explanation:
https://www.skillset.com/questions/a-bastion-host-is-which-of-the-following

QUESTION 440
Optical biometric recognition such as retina scanning provides access to facilities through reading the unique characteristics of a person's eye.
However, authorization failures can occur with individuals who have?

A. Glaucoma or cataracts
B. Two different colored eyes (heterochromia iridium)
C. Contact lens
D. Malaria

Answer: A