QUESTION 390
Michael starts a new job and discovers that he has unnecessary access to a variety of systems. Which of the following best describes the problem he has encountered?

A. Rights collision
B. Excessive privileges
C. Privilege creep
D. Least privileges

Answer: B

QUESTION 391
Which of the following best describes the sensors designed to project and detect a light beam across an area?

A. Smoke
B. Thermal
C. Air-aspirating
D. Photo electric

Answer: D
Explanation:
https://en.wikipedia.org/wiki/Photoelectric_sensor

QUESTION 392
As the Chief Information Security Officer, you want to ensure data shared securely, especially when shared with third parties outside the organization. What protocol provides the ability to extend the network perimeter with the use of encapsulation and encryption?

A. File Transfer Protocol (FTP)
B. Virtual Local Area Network (VLAN)
C. Simple Mail Transfer Protocol
D. Virtual Private Network (VPN)

Answer: D
Explanation:
https://searchnetworking.techtarget.com/definition/virtual-private-network

QUESTION 393
As the CISO, you have been tasked with the execution of the company's key management program. You MUST ensure the integrity of encryption keys at the point of generation. Which principal of encryption key control will ensure no single individual can constitute or re-constitute a key?

A. Dual Control
B. Separation of Duties
C. Split Knowledge
D. Least Privilege

Answer: A
Explanation:
https://info.townsendsecurity.com/bid/23881/PCI-DSS-2-0-and-Encryption-Key-Management

QUESTION 394
What is one key difference between Capital expenditures and Operating expenditures?

A. Operating expense cannot be written off while Capital expense can
B. Operating expenses can be depreciated over time and Capital expenses cannot
C. Capital expenses cannot include salaries and Operating expenses can
D. Capital expenditures allow for the cost to be depreciated over time and Operating does not

Answer: C

QUESTION 395
Which of the following is used to lure attackers into false environments so they can be monitored, contained, or blocked from reaching critical systems?

A. Segmentation controls.
B. Shadow applications.
C. Deception technology.
D. Vulnerability management.

Answer: B

QUESTION 396
Which of the following is an accurate description of a balance sheet?

A. The percentage of earnings that are retained by the organization for reinvestment in the business
B. The details of expenses and revenue over a long period of time
C. A summarized statement of all assets and liabilities at a specific point in time
D. A review of regulations and requirements impacting the business from a financial perspective

Answer: C

QUESTION 397
A CISO wants to change the defense strategy to ward off attackers. To accomplish this the CISO is looking to a strategy where attackers are lured into a zone of a safe network where attackers can be monitored, controlled, quarantined, or eradicated.

A. Moderate investment
B. Passive monitoring
C. Integrated security controls
D. Dynamic deception

Answer: D

QUESTION 398
What is the difference between encryption and tokenization?

A. Tokenization combined with hashing is always better than encryption
B. Encryption can be mathematically reversed to provide the original information
C. The token contains the all original information
D. Tokenization can be mathematically reversed to provide the original information

Answer: B
Explanation:
http://library.ahima.org/doc?oid=104090#.X_dwWolR3eQ

QUESTION 399
Which of the following information would MOST likely be reported at the board-level within an organization?

A. System scanning trends and results as they pertain to insider and external threat sources
B. The capabilities of a security program in terms of staffing support
C. Significant risks and security incidents that have been discovered since the last assembly of the membership
D. The numbers and types of cyberattacks experienced by the organization since the last assembly of the membership

Answer: C

QUESTION 400
Which technology can provide a computing environment without requiring a dedicated hardware backend?

A. Mainframe server
B. Virtual Desktop
C. Thin client
D. Virtual Local Area Network

Answer: B

QUESTION 401
What process defines the framework of rules and practices by which a board of directors ensure accountability, fairness and transparency in an organization's relationship with its shareholders?

A. Internal Audit
B. Corporate governance
C. Risk Oversight
D. Key Performance Indicators

Answer: B
Explanation:
https://www.igi-global.com/dictionary/corporate-governance/5957

QUESTION 402
As the Business Continuity Coordinator of a financial services organization, you are responsible for ensuring assets are recovered timely in the event of a disaster. Which is the BEST Disaster Recovery performance indicator to validate that you are prepared for a disaster?

A. Recovery Point Objective (RPO)
B. Disaster Recovery Plan
C. Recovery Time Objective (RTO)
D. Business Continuity Plan

Answer: D
Explanation:
https://www.resolver.com/resource/bcdr-metrics-that-matter/

QUESTION 403
What are the three hierarchically related aspects of strategic planning and in which order should they be done?

A. 1) Information technology strategic planning, 2) Enterprise strategic planning, 3) Cybersecurity or information security strategic planning
B. 1) Cybersecurity or information security strategic planning, 2) Enterprise strategic planning, 3) Information technology strategic planning
C. 1) Enterprise strategic planning, 2) Information technology strategic planning, 3) Cybersecurity or information security strategic planning
D. 1) Enterprise strategic planning, 2) Cybersecurity or information security strategic planning, 3) Information technology strategic planning

Answer: D

QUESTION 404
Which regulation or policy governs protection of personally identifiable user data gathered during a cyber investigation?

A. ITIL
B. Privacy Act
C. Sarbanes Oxley
D. PCI-DSS

Answer: B

QUESTION 405
Which of the following would negatively impact a log analysis of a multinational organization?

A. Centralized log management
B. Encrypted log files in transit
C. Each node set to local time
D. Log aggregation agent each node

Answer: D