QUESTION 79
An organization has the following risk mitigation policy:

- Risks with a probability of 95% or greater will be addressed before all others regardless of the impact.
- All other prioritization will be based on risk value.

The organization has identified the following risks:

Risk	Probability	Impact
A	95%	$110,000
B	99%	$100,000
C	50%	$120,000
D	90%	$50,000

Which of the following is the order of priority for risk mitigation from highest to lowest?

A. A, B, D, C
B. A, B, C, D
C. D, A, B, C
D. D, A, C, B

Correct Answer: B

QUESTION 80
Which of the following MOST accurately describes an HSM?

A. An HSM is a low-cost solution for encryption.
B. An HSM can be networked based or a removable USB
C. An HSM is slower at encrypting than software
D. An HSM is explicitly used for MFA

Correct Answer: B

QUESTION 81
Joe, a penetration tester, used a professional directory to identify a network administrator and ID administrator for a client's company. Joe then emailed the network administrator, identifying himself as the ID administrator, and asked for a current password as part of a security exercise. Which of the following techniques were used in this scenario?

A. Enumeration and OS fingerprinting
B. Email harvesting and host scanning
C. Social media profiling and phishing
D. Network and host scanning

Correct Answer: C

QUESTION 82
The security team at a large corporation is helping the payment-processing team to prepare for a

regulatory compliance audit and meet the following objectives:

- Reduce the number of potential findings by the auditors.
- Limit the scope of the audit to only devices used by the payment-processing team for activities directly impacted by the regulations.
- Prevent the external-facing web infrastructure used by other teams from coming into scope.
- Limit the amount of exposure the company will face if the systems used by the payment-processing team are compromised.

Which of the following would be the MOST effective way for the security team to meet these objectives?

A. Limit the permissions to prevent other employees from accessing data owned by the business unit.
B. Segment the servers and systems used by the business unit from the rest of the network.
C. Deploy patches to all servers and workstations across the entire organization.
D. Implement full-disk encryption on the laptops used by employees of the payment-processing team.

Correct Answer: B

QUESTION 83
A company's data is still being exfiltered to business competitors after the implementation of a DLP solution. Which of the following is the most likely reason why the data is still being compromised?

A. Printed reports from the database contain sensitive information
B. DRM must be implemented with the DLP solution
C. Users are not labeling the appropriate data sets
D. DLP solutions are only effective when they are implemented with disk encryption

Correct Answer: B

QUESTION 84
A security analyst is reviewing packet captures from a system that was compromised. The system was already isolated from the network, but it did have network access for a few hours after being compromised. When viewing the capture in a packet analyzer, the analyst sees the following:

```
11:03:09.095091 IP 10.1.1.10.47787 > 128.50.100.3.53:48202+ A? michael.smith.334-54-2343.985-334-5643.1123-kathman-dr.ajgidwle.com.
11:03:09.186945 IP 10.1.1.10.47788 > 128.50.100.3.53:49675+ A? ronald.young.437-96-6523.212-635-6528.2426-riverland-st.ajgidwle.com.
11:03:09.189567 IP 10.1.1.10.47789 > 128.50.100.3.53:50986+ A? mark.leblanc.485-63-5278.802-632-5841.68951-peachtree-st.ajgidwle.com.
11:03:09.296854 IP 10.1.1.10.47790 > 128.50.100.3.53:51567+ A? gina.buras.471-96-2354.313-654-9254.3698-mcghee-rd.ajgidwle.com.
```

Which of the following can the analyst conclude?

A. Malware is attempting to beacon to 128.50.100.3.
B. The system is running a DoS attack against ajgidwle.com.
C. The system is scanning ajgidwle.com for PII.
D. Data is being exfiltrated over DNS.
Correct Answer: D

QUESTION 85
An organization needs to limit its exposure to accidental disclosure when employees send emails that contain personal information to recipients outside the company. Which of the following technical controls would BEST accomplish this goal?

A. DLP
B. Encryption
C. Data masking
D. SPF

Correct Answer: C

QUESTION 86
A security analyst wants to identify which vulnerabilities a potential attacker might initially exploit if the network is compromised. Which of the following would provide the BEST results?

A. Baseline configuration assessment
B. Uncredentialed scan
C. Network ping sweep
D. External penetration test

Correct Answer: D

QUESTION 87
A security analyst is reviewing a suspected phishing campaign that has targeted an organisation. The organization has enabled a few email security technologies in the last year: however, the analyst believes the security features are not working. The analyst runs the following command:

> dig domain._domainkey.comptia.orq TXT

Which of the following email protection technologies is the analyst MOST likely validating?

A. SPF
B. DNSSEC
C. DMARC
D. DKIM

Correct Answer: A

QUESTION 88
As part of a merger with another organization, a Chief Information Security Officer (CISO) is working with an assessor to perform a risk assessment focused on data privacy compliance. The CISO is primarily concerned with the potential legal liability and fines associated with data privacy. Based on the CISO's concerns, the assessor will MOST likely focus on:

A. qualitative probabilities.
B. quantitative probabilities.
C. qualitative magnitude.
D. quantitative magnitude.

Correct Answer: D

QUESTION 89
A Chief Information Security Officer (CISO) is concerned about new privacy regulations that apply to the company. The CISO has tasked a security analyst with finding the proper control functions to verity that a user's data is not altered without the user's consent. Which of the following would be an appropriate course of action?

A. Use a DLP product to monitor the data sets for unauthorized edits and changes.
B. Use encryption first and then hash the data at regular, defined times.
C. Automate the use of a hashing algorithm after verified users make changes to their data
D. Replicate the data sets at regular intervals and continuously compare the copies for unauthorized changes.

Correct Answer: D

QUESTION 90
As part of a review of incident response plans, which of the following is MOST important for an organization to understand when establishing the breach notification period?

A. Organizational policies
B. Vendor requirements and contracts
C. Service-level agreements
D. Legal requirements

Correct Answer: D

QUESTION 91
A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too much access to customer data. Developers use personal workstations, giving the company little to no visibility into the development activities. Which of the following would be BEST to implement to alleviate the CISO's concern?

A. DLP
B. Encryption
C. Test data
D. NDA

Correct Answer: C

QUESTION 92
A remote code execution vulnerability was discovered in the RDP. An organization currently uses RDP for remote access to a portion of its VDI environment. The analyst verified network-level authentication is enabled. Which of the following is the BEST remediation for this vulnerability?

A. Verify the latest endpoint-protection signature is in place.
B. Verify the corresponding patch for the vulnerability is installed^
C. Verify the system logs do not contain indicator of compromise.
D. Verify the threat intelligence feed is updated with the latest solutions

Correct Answer: A

QUESTION 93
An information security analyst is reviewing backup data sets as part of a project focused on eliminating archival data sets. Which of the following should be considered FIRST prior to disposing of the electronic data?

A. Sanitization policy
B. Data sovereignty
C. Encryption policy
D. Retention standards

Correct Answer: D

QUESTION 94
An information security analyst observes anomalous behavior on the SCADA devices in a power plant. This behavior results in the industrial generators overheating and destabilizing the power supply. Which of the following would BEST identify potential indicators of compromise?

A. Use Burp Suite to capture packets to the SCADA device's IP.
B. Use tcpdump to capture packets from the SCADA device IP.
C. Use Wireshark to capture packets between SCADA devices and the management system.
D. Use Nmap to capture packets from the management system to the SCADA devices.

Correct Answer: C

QUESTION 95
A routine vulnerability scan detected a known vulnerability in a critical enterprise web application. Which of the following would be the BEST next step?

A. Submit a change request to have the system patched
B. Evaluate the risk and criticality to determine it further action is necessary
C. Notify a manager of the breach and initiate emergency procedures.
D. Remove the application from production and Inform the users.

Correct Answer: A

QUESTION 96
A critical server was compromised by malware, and all functionality was lost. Backups of this server were taken; however, management believes a logic bomb may have been injected by a rootkit. Which of the following should a security analyst perform to restore functionality quickly?

A. Work backward, restoring each backup until the server is clean
B. Restore the previous backup and scan with a live boot anti-malware scanner
C. Stand up a new server and restore critical data from backups
D. Offload the critical data to a new server and continue operations

Correct Answer: C