Question 1

An information security officer is asked to write a retention policy for a financial system. She is aware of the fact that some data must be kept for a long time and other data must be deleted.

Where should she look for guidelines first?

Options:

A- In company policies

B- In finance management procedures

C- In legislation

Answer:

C

Question 2

The handling of security incidents is done by the incident management process under guidelines of information security management. These guidelines call for several types of mitigation plans.

Which mitigation plan covers short-term recovery after a security incident has occurred?

Options:

A- The Business Continuity Plan (BCP)

B- The disaster recovery plan

C- The incident response plan

D- The risk treatment plan

Answer:

C

Question 3

Question Type: MultipleChoice

Who should be asked to check compliance with the information security policy throughout the company?

Options:

A- Internal audit department

B- External forensics investigators

C- The same company that checks the yearly financial statement

Answer:

B

Question 4

Question Type: **MultipleChoice**

The security manager of a global company has decided that a risk assessment needs to be completed across the company.

What is the primary objective of the risk assessment?

Options:

A- Identify, quantify and prioritize each of the business-critical assets residing on the corporate infrastructure

B- Identify, quantify and prioritize risks against criteria for risk acceptance

C- Identify, quantify and prioritize the scope of this risk assessment

D- Identify, quantify and prioritize which controls are going to be used to mitigate risk

Answer:

B

Question 5

Question Type: MultipleChoice

Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are key terms in business continuity management (BCM). Reducing loss of data is one of the focus areas of a BCM policy.

What requirement is in the data recovery policy to realize minimal data loss?

Options:

A- Maximize RPO

B- Reduce RPO

C- Reduce RTO

D- Reduce the time between RTO and RPO

Answer:

B

Question 6

Question Type: MultipleChoice

What is a key item that must be kept in mind when designing an enterprise-wide information security program?

Options:

A- When defining controls follow an approach and framework that is consistent with organizational culture

B- Determine controls in the light of specific risks an organization is facing

C- Put an enterprise-wide network and Host-Based Intrusion Detection and Prevention System (Host-Based IDPS) into place as soon as possible

D- Put an incident management and log file analysis program in place immediately

Answer:

B

Question 7

In a company a personalized smart card is used for both physical and logical access control.

What is the main purpose of the person's picture on the smart card?

Options:

A- To authenticate the owner of the card

B- To authorize the owner of the card

C- To identify the role of the card owner

D- To verify the iris of the card owner

Question 8

Question Type: **MultipleChoice**

An employee has worked on the organizational risk assessment. The goal of the assessment is not to bring residual risks to zero, but to bring the residual risks in line with an organization's risk appetite.

When has the risk assessment program accomplished its primary goal?

Options:

A- Once the controls are implemented

B- Once the transference of the risk is complete

C- When decision makers have been informed of uncontrolled risks and proper authority groups decide to leave the risks in place

D- When the risk analysis is completed

Answer:

C

Question 9

When is revision of an employee's access rights mandatory?

Options:

A- After any position change

B- At hire

C- At least each year

D- At all moments stated in the information security policy

Answer:

D

Question 10

The information security architect of a large service provider advocates an open design of the security architecture, as opposed to a secret design.

What is her main argument for this choice?

Options:

A- Open designs are easily configured.

B- Open designs have more functionality.

C- Open designs are tested extensively.

Answer:

C

Question 11

Question Type: **MultipleChoice**

In a company the IT strategy is migrating towards a Service Oriented Architecture (SOA) so that migrating to the cloud is better feasible in the future. The security architect is asked to make a first draft of the security

architecture.

Which elements should the security architect draft?

Options:

A- Management and control of the security services

B- The information security policy, the risk assessment and the controls in the security services

C- Which security services are provided and in which supporting architectures are they defined

Answer:

C

Question 12

Question Type: **MultipleChoice**

A company's webshop offers prospects and customers the possibility to search the catalog and place orders around the clock. In order to satisfy the needs of both customer and business several requirements have to

be met. One of the criteria is data classification.

What is the most important classification aspect of the unit price of an object in a 24h webshop?

Options:

A- Confidentiality

B- Integrity

C- Availability

Answer:

C