Started on	Saturday, 16 May 2020, 8:11 AM
State	Finished
Completed on	Saturday, 16 May 2020, 9:02 AM
Time taken	51 mins 18 secs
Grade	**50.5** out of 56.0 (**90**%)

Question **1**

Correct

Mark 1.0 out of 1.0

Business continuity plans (BCPs) for organizational Information Systems should be developed primarily considering:

Select one:

● a. Business needs and its relation with the information systems ✓

○ b. Levels of effort

○ c. Available resources

○ d. Projected costs

The correct answer is: Business needs and its relation with the information systems

Question **2**

Correct

Mark 1.0 out of 1.0

An **interoperability error** is what type of vulnerability?

Select one:

● a. Emergent ✓

○ b. Technical

○ c. Organizational

○ d. Process

The correct answer is: Emergent

Question **3**

Correct

Mark 1.0 out of 1.0

Which two factors are used to calculate the **likelihood of an event**?

Select one:

● a. Threat and vulnerability ✓

○ b. Asset count and asset value

○ c. Threat and asset count

○ d. Vulnerability and asset value

The correct answer is: Threat and vulnerability

Question **4**

Incorrect

Mark 0.0 out of 1.0

Ingress (input) and **egress(output)** are types of:

Select one:

○ a. Attack vector

○ b. Data

● c. Horizontal defense ✗

○ d. Vertical defense

The correct answer is: Attack vector

Question **5**

Correct

Mark 1.0 out of 1.0

Nonrepudiation is implemented through which of the following methods? Select 2:

Select one or more:

□ a. Backups

☑ b. Digital signatures ✓

□ c. Encryption

☑ d. Transactional logs ✓

The correct answers are: Transactional logs, Digital signatures

Question **6**

Correct

Mark 1.0 out of 1.0

Virtualization involves:

Select one:

○ a. The creation of a layer between physical and logical access controls

○ b. DNS interrogation, WHOIS queries and network sniffing

● c. Multiple guests coexisting on the same physical server in isolation each one of another ✓

○ d. Simultaneous use of kernel mode and user mode

The correct answer is: Multiple guests coexisting on the same physical server in isolation each one of another

Question **7**

Correct

Mark 1.0 out of 1.0

Authentication is defined as which of the following? Select 2:

Select one or more:

□ a. Users within an organization authorized to maintain and protect systems and networks

□ b. A system's ability to identify the activity of the users

☑ c. The act of verifying a user's eligibility to access a system ✓

☑ d. The act of verifying identity ✓

The correct answers are: The act of verifying identity, The act of verifying a user's eligibility to access a system

Question **8**

Correct

Mark 1.0 out of 1.0

Major risks of cloud computing include which of the following? Select 3:

Select one or more:

☑ a. Difficult to protect data ✓

☑ b. Provider non-compliance with requirements ✓

☑ c. Loss of governance ✓

☐ d. Lack of scalability

The correct answers are: Difficult to protect data, Provider non-compliance with requirements, Loss of governance

Question **9**

Incorrect

Mark 0.0 out of 1.0

"Penetration testing" includes "Vulnerability scan" because "Penetration testing" is conformed by the following phases: Planning, Discovery, Attack and Reporting. So, "Vulnerability scan" can be seen **in a practical way** as a process that just include the Planning and Discovery phases.

Select one:

○ True

● False ✗

The correct answer is 'True'.

Question **10**

Correct

Mark 1.0 out of 1.0

The **concept** that states the establishment and maintenance of user profiles defining authentication, authorization and access controls for each user is called:

Select one:

○ a. Privileged user management

○ b. Authentication

● c. Identity management ✓

○ d. Access rights

The correct answer is: Identity management

Question **11**

Correct

Mark 1.0 out of 1.0

It is defined as “a **model** for enabling convenient, on-demand network access to a **shared pool of configurable resources** (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management or service provider interaction.”

Select one:

○ a. Platform as a Service (PaaS)

○ b. Software as a Service (SaaS)

○ c. Big data

● d. Cloud computing ✓

The correct answer is: Cloud computing

Question **12**

Correct

Mark 1.0 out of 1.0

The **process** of eliminating as many security risks as possible by removing all **nonessential components** is called:

Select one:

● a. System hardening ✓

○ b. Isolation

○ c. Stateful inspection

○ d. Stateless filtering

The correct answer is: System hardening

Question **13**

Partially correct

Mark 0.5 out of 1.0

There are 4 types of vulnerabilities: Technical, Process, Organizational and Emergent. Make the proper relation between the "type of vulnerability" and the "definition":

Errors in design, implementation, placement or configuration	Technical ▼	✓
Errors in the interactions between environments	Organizational ▼	✗
Errors in operation	Process ▼	✓
Errors in management, decision, planning or from ignorance	Emergent ▼	✗

The correct answer is: Errors in design, implementation, placement or configuration → Technical, Errors in the interactions between environments → Emergent, Errors in operation → Process, Errors in management, decision, planning or from ignorance → Organizational

Question **14**

Correct

Mark 1.0 out of 1.0

A **Business Continuity Plan (BCP**) is not complete, unless it includes:

Select one:

● a. Detailed procedures about the recovery of the critical processes ✓

○ b. No critical processes

○ c. Network diagrams

○ d. Dedicated resources

The correct answer is: Detailed procedures about the recovery of the critical processes

Question 15

Correct

Mark 1.0 out of 1.0

Updates in cloud-computing environments can be done quickly because the environment is:

Select one:

○ a. Secure

○ b. Diversified

○ c. Distributed

● d. Homegeneous ✓

The correct answer is: Homegeneous

Question 16

Correct

Mark 1.0 out of 1.0

Outsourcing poses the greatest risk to an organization when it involves:

Select one:

○ a. Cybersecurity capabilities

○ b. Technology infrastructure

● c. Core business functions ✓

○ d. Business support services

The correct answer is: Core business functions

Question 17

Correct

Mark 1.0 out of 1.0

A **small, isolated network** for an organization's **public** servers, bastion host information servers and modem pools is called a(n):

Select one:

● a. Demilitarized zone (DMZ) ✓

○ b. Dual-homed firewall

○ c. Virtual local area network (VLAN)

○ d. Screened-host firewall

The correct answer is: Demilitarized zone (DMZ)

Question 18

Correct

Mark 1.0 out of 1.0

Which cybersecurity principle is most important when attempting to trace the **source of malicious activity**?

Select one:

○ a. Confidentiality

● b. Non repudiation ✓

○ c. Integrity

○ d. Availability

The correct answer is: Non repudiation

Question 19

Correct

Mark 1.0 out of 1.0

The risk assessment process is a one-time process, this means an organization just need to identify assets, threats and vulnerabilities **one time in its life** in order to be protected.

Select one:

○ True

● False ✓

The correct answer is 'False'.

Question 20

Incorrect

Mark 0.0 out of 1.0

In a Disaster Recovery Plan (DRP), the **last known point of good data** is identified as:

Select one:

○ a. Recovery point objective

○ b. Data recovery

○ c. Full backup

● d. Recovery time objective ✗

The correct answer is: Recovery point objective

Question 21

Correct

Mark 1.0 out of 1.0

A firewall that tracks **open connection-oriented protocol sessions** is said to be:

Select one:

● a. Stateful ✓

○ b. Stated

○ c. Stateless

○ d. State-sponsored

The correct answer is: Stateful

Question 22

Correct

Mark 1.0 out of 1.0

Which of the following activities is associated with **identifying digital assets**?

Select one:

○ a. Recovery management

● b. Asset management ✓

○ c. Awareness and training

○ d. Security continuous monitoring

The correct answer is: Asset management

Question **23**

Correct

Mark 1.0 out of 1.0

Securing **Supervisory Control and Data Acquisition (SCADA)** systems can be challenging because they:

Select one:

○ a. Are subject to specialized requirements established for national security systems

○ b. Cannot be replaced due to aging infrastructure and the complexity of included components

○ c. Support critical infrastructure processes for which any risk of compromise is unacceptable

● d. Operate in specialized environments and often have non-standard design elements ✓

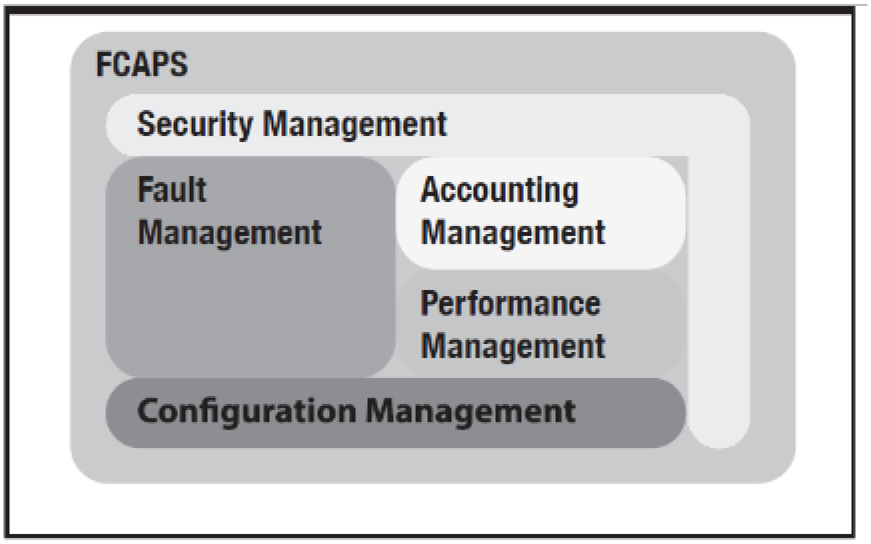
The correct answer is: Operate in specialized environments and often have non-standard design elements

Question **24**

Correct

Mark 1.0 out of 1.0

FCAPS (Five functional areas of network management) includes the 5 Functional Areas considered as "essential" in the **process of Network Management**. These are represented in the following image:



According to FCAPS, select the WRONG statement:

Select one:

○ a. "Performance management" includes to develop quality metrics like optimal response time, low error rates, etc.

○ b. "Configuration management" includes to store and manage the configuration file of the network devices.

● c. "Fault management" implies to be able to configure a network that is connected to internet. ✓

○ d. "Accounting management" refers to know how much the network is used.

○ e. "Security management" includes securing the devices with authentication and authorization methods, additionally to attack detection actions.

The correct answer is: "Fault management" implies to be able to configure a network that is connected to internet.

Question **25**

Correct

Mark 1.0 out of 1.0

All of the following are **encryption techniques,** except:

Select one:

○ a. Elliptical curve cryptography

○ b. Advanced encryption standard

● c. Key length ✓

○ d. Quantum cryptography

The correct answer is: Key length

Question **26**

Incorrect

Mark 0.0 out of 1.0

In practical applications:

Select one:

○ a. Symmetric key encryption is used only for short messages, such as digital signatures

○ b. Asymmetric key encryption is used to securely obtain symmetric keys

○ c. Asymmetric key encryption is used in cases where speed is important

● d. Symmetric key encryption is used to securely distribute asymmetric keys ✗

The correct answer is: Asymmetric key encryption is used to securely obtain symmetric keys

Question **27**

Correct

Mark 1.0 out of 1.0

Which information security component considers the **level of sensitivity** and **legal requirements** and is subject to **change** over time?

Select one:

○ a. Availability

● b. Confidentiality ✓

○ c. Integrity

○ d. Authentication

The correct answer is: Confidentiality

Question **28**

Correct

Mark 1.0 out of 1.0

To which of the following layers of the Open Systems Interconnect (OSI) model would belongs **Ethernet**?

Select one:

○ a. Transport

● b. Data Link ✓

○ c. Network

○ d. Application

The correct answer is: Data Link

Question **29**

Correct

Mark 1.0 out of 1.0

The key attributes of an **Advanced Persistent Threat (APT)** include which of the following? Select 3:

Select one or more:

☑ a. Stealthy ✓

☑ b. Sophisticated ✓

□ c. Web services oriented

☑ d. Persistent ✓

The correct answers are: Stealthy, Sophisticated, Persistent

Question **30**

Correct

Mark 1.0 out of 1.0

Which activity ensures that business processes can continue **after** a security incident?

Select one:

● a. Recovery ✓

○ b. Response

○ c. Detection

○ d. Protection

The correct answer is: Recovery

Question **31**

Correct

Mark 1.0 out of 1.0

During which phase of the **Six-Phase Incident Response Model** (Preparation, Identification, Containment, Eradication, Recovery, Lessons learned) is the **root cause** determined?

Select one:

○ a. Recovery

● b. Eradication ✓

○ c. Identification

○ d. Containment

The correct answer is: Eradication

Question **32**

Incorrect

Mark 0.0 out of 1.0

Even if **virtualization** is a very attractive computational model for many organization, it also requires protection through **countermeasures**. From the following countermeasures select the **one** that does NOT apply to protect virtualized infrastructure:

Select one:

○ a. Make network segregation. Avoid to put virtual machines in the demilitarized zone (DMZ). Place management tools on a separate network segment.

○ b. Patching, antivirus, limited services, logging and set appropriate permissions for the host and its virtual machines

○ c. Implement specific database security techniques

● d. Strong physical and logical access controls, especially over the hypervisor host and its management console ✗

The correct answer is: Implement specific database security techniques

Question **33**

Correct

Mark 1.0 out of 1.0

Where should an organization’s network **terminate** Virtual Private Network (VPN) tunnels?

Select one:

○ a. At an interior router, to reduce network traffic congestion

● b. At the perimeter, to allow for effective internal monitoring ✓

○ c. At a dedicated “honey pot” system in the demilitarized zone (DMZ)

○ d. At the destination system, to prevent loss of confidentiality

The correct answer is: At the perimeter, to allow for effective internal monitoring

Question **34**

Correct

Mark 1.0 out of 1.0

Maintaining a high degree of confidence regarding the **integrity of evidence** requires a(n):

Select one:

○ a. Power of attorney

○ b. Affidavit

○ c. Sworn statement

● d. Chain of custody ✓

The correct answer is: Chain of custody

Question **35**

Correct

Mark 1.0 out of 1.0

This key function ensures that organizational objectives and stakeholder needs are **aligned** with desired outcomes through effective decision making and prioritization

Select one:

○ a. Risk mitigation

● b. Governance ✓

○ c. Risk assessment

○ d. Risk management

The correct answer is: Governance

Question **36**

Correct

Mark 1.0 out of 1.0

Which of the following are **types of backups**?

Select one:

○ a. Full, incremental and variable

○ b. Full, partial and differential

○ c. Full and differential

● d. Full, incremental and differential ✓

The correct answer is: Full, incremental and differential

Question **37**

Correct

Mark 1.0 out of 1.0

Risk assessments should be performed:

Select one:

○ a. At the start of a program

○ b. When an asset changes

● c. On a regular basis ✓

○ d. When a vulnerability is discovered

The correct answer is: On a regular basis

Question **38**

Correct

Mark 1.0 out of 1.0

Which of the following elements **interpret policies** and **apply them** to specific situations?

Select one:

○ a. Guidelines

○ b. Contracts

○ c. Procedures

● d. Standards ✓

The correct answer is: Standards

Question **39**

Correct

Mark 1.0 out of 1.0

A **segmented network**:

Select one:

○ a. Maximizes the delay experienced by an attacker

● b. Consists of two or more security zones ✓

○ c. Is not related with Defense in Depth implementations

○ d. Delivers inferior performance for internal applications

The correct answer is: Consists of two or more security zones

Question **40**

Correct

Mark 1.0 out of 1.0

The **primary** objective of cybersecurity is:

Select one:

● a. Protecting the company's digital assets ✓

○ b. Managing risk through countermeasures and controls

○ c. Responding to security incidents

○ d. Protection of all company assets

The correct answer is: Protecting the company's digital assets

Question **41**

Correct

Mark 1.0 out of 1.0

During which phase of the **System Development Lifecycle (SDLC)** should security first be considered?

Select one:

○ a. Design

● b. Planning ✓

○ c. Implementation

○ d. Analysis

The correct answer is: Planning

Question 42

Correct

Mark 1.0 out of 1.0

The **lack of formal training** for employees on the use of mobile devices is considered a(n):

Select one:

- ● a. Organizational risk ✓
- ○ b. Technical risk
- ○ c. Informational risk
- ○ d. Physical risk

The correct answer is: Organizational risk

Question 43

Correct

Mark 1.0 out of 1.0

Which of the following describes the **typical activities** developed by a security engineer to identify the occurrence of a cybersecurity **incident**?

Select one:

- ○ a. Communications, analysis and mitigation
- ● b. Security continuous monitoring, detection and evaluating anomalies/incidents ✓
- ○ c. Asset management, risk management and risk assessment
- ○ d. Data security, awareness/training, access control and processes/procedures

The correct answer is: Security continuous monitoring, detection and evaluating anomalies/incidents

Question **44**

Correct

Mark 1.0 out of 1.0

[Optional] Under the US-CERT model for incident categorization, a **CAT-3 incident** refers to which of the following?

Note: US-CERT defines 6 categories for security incidents (1-6) being the CAT 1 the most critical and the one that requires inmediate attention. CAT 6 is the less critical incident.

Select one:

○ a. Investigation

● b. Malicious code ✓

○ c. Improper usage

○ d. Denial of service (DoS)

The correct answer is: Malicious code

Question **45**

Correct

Mark 1.0 out of 1.0

The practice of putting **multiple layers** to provide aditional protection is called:

Select one:

● a. Defense in depth ✓

○ b. Network foundation protection

○ c. Risk mitigation

○ d. Edge protection

The correct answer is: Defense in depth

Question **46**

Correct

Mark 1.0 out of 1.0

Which type of documentation makes the **record of details of events** in an organized record-keeping system, usually sequenced in the order in which they occurred?

Select one:

○ a. Backup

○ b. Digital signature

○ c. Digital certificate

● d. Log ✓

The correct answer is: Log

Question **47**

Correct

Mark 1.0 out of 1.0

A cybersecurity architecture designed **around the concept of a perimeter** is said to be:

Select one:

● a. System-centric ✓

○ b. User-centric

○ c. Data-centric

○ d. Integrated

The correct answer is: System-centric

Question **48**

Correct

Mark 1.0 out of 1.0

Which of the following describes a **differential backup**?

Select one:

○ a. Copies every file in the system, regardless of last backup

● b. Only copies files that have changed since last full backup ✓

○ c. None of the above

○ d. Copies all files that have changed, regardless of last backup type

The correct answer is: Only copies files that have changed since last full backup

Question **49**

Correct

Mark 1.0 out of 1.0

The **amount of time allowed** for the **recovery** of a business function or resource **after** a disaster occurs is called:

Select one:

○ a. Service delivery objective

○ b. Recovery point objective (RPO)

● c. Recovery time objective (RTO) ✓

○ d. Maximum tolerable outages

The correct answer is: Recovery time objective (RTO)

Question **50**

Correct

Mark 1.0 out of 1.0

An **authority** in a network that **verifies user requests** for a digital certificate and tells the certificate authority (CA) to issue it is called:

Select one:

○ a. Digital signature

● b. Registration authority ✓

○ c. Certificate authority

○ d. Digital certificate

The correct answer is: Registration authority

Question **51**

Correct

Mark 1.0 out of 1.0

The **attack mechanism** directed against a system is commonly called a(n):

Select one:

○ a. Attack Vector

○ b. Vulnerability

● c. Payload ✓

○ d. Exploit

The correct answer is: Payload

Question **52**

Correct

Mark 1.0 out of 1.0

What is one advantage of a **firewall implemented in software** over a firewall appliance?

Select one:

○ a. Power consumption

● b. Flexibility ✓

○ c. Performance

○ d. Resiliency

The correct answer is: Flexibility

Question **53**

Correct

Mark 1.0 out of 1.0

Which of the following shemes offers the **strongest protection for wireless network traffic**?

Select one:

○ a. Wireless Protected Access-Temporary Key Integrity Protocol (WPA-TKIP)

○ b. Wired Equivalent Protection 128-bit (WEP-128)

● c. Wireless Protected Access 2 (WPA2) ✓

○ d. Wireless Protected Access-Advanced Encryption Standard (WPA-AES)

The correct answer is: Wireless Protected Access 2 (WPA2)

Question **54**

Correct

Mark 1.0 out of 1.0

A **passive network hub** operates at which layer of the OSI model?

Select one:

○ a. Transport

● b. Physical ✓

○ c. Data link

○ d. Network

The correct answer is: Physical

Question 55

Correct

Mark 1.0 out of 1.0

Which term describes a **cryptology technique** used to prove message integrity using algorithms to create unique numeric values?

Select one:

○ a. Access controls

○ b. Digital signatures

● c. Hashes ✓

○ d. Encryption

The correct answer is: Hashes

Question 56

Correct

Mark 1.0 out of 1.0

Network devices should be **managed** using a dedicated **Virtual Local Area Network** (VLAN) because:

Select one:

○ a. Segregation of management traffic and use traffic dramatically improves performance

● b. Insecure protocols used in normal traffic could result in a compromise of privileged user credentials (used in management protocols) ✓

○ c. Network topologies do not always property identify the locations of virtual servers

○ d. VLAN encryption provides a double layer of protection for virtual system data

The correct answer is: Insecure protocols used in normal traffic could result in a compromise of privileged user credentials (used in management protocols)