CLARUSWAY

WAY TO REINVENT YOURSELF

CompTIA (7A-7B-7C) Explain Resiliency and Site Security Concepts

AGENDA

- 7A - Asset Management (10)
- 7B - Redundancy Strategies (14)
- 7C - Physical Security (5)
- TOTAL: 29

7A - Asset Management

7A - Asset Management

NO.1 Which of the following is a common source of unintentional corporate credential leakage in cloud environments?

A. Code repositories
B. Dark web
C. Threat feeds
D. State actors
E. Vulnerability databases

7A - Asset Management

NO.1 Which of the following is a common source of unintentional corporate credential leakage in cloud environments?

A. Code repositories
B. Dark web
C. Threat feeds
D. State actors
E. Vulnerability databases

7A - Asset Management

NO.2 A company is required to use certified hardware when building networks. Which of the following best addresses the risks associated with procuring counterfeit hardware?

A. A thorough analysis of the supply chain
B. A legally enforceable corporate acquisition policy
C. A right to audit clause in vendor contracts and SOWs
D. An in-depth penetration test of all suppliers and vendors

7A - Asset Management

NO.2 A company is required to use certified hardware when building networks. Which of the following best addresses the risks associated with procuring counterfeit hardware?

A. A thorough analysis of the supply chain
B. A legally enforceable corporate acquisition policy
C. A right to audit clause in vendor contracts and SOWs
D. An in-depth penetration test of all suppliers and vendors

7A - Asset Management

NO.3 A company is discarding a classified storage array and hires an outside vendor to complete the disposal.
Which of the following should the company request from the vendor?

A. Certification
B. Inventory list
C. Classification
D. Proof of ownership

7A - Asset Management

NO.3 A company is discarding a classified storage array and hires an outside vendor to complete the disposal.
Which of the following should the company request from the vendor?

A. Certification
B. Inventory list
C. Classification
D. Proof of ownership

7A - Asset Management

NO.4 A company requires hard drives to be securely wiped before sending decommissioned systems to recycling.
Which of the following best describes this policy?

A. Enumeration
B. Sanitization
C. Destruction
D. Inventory

7A - Asset Management

NO.4 A company requires hard drives to be securely wiped before sending decommissioned systems to recycling.
Which of the following best describes this policy?

A. Enumeration
B. Sanitization
C. Destruction
D. Inventory

7A - Asset Management

NO.5 Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?

A. A full inventory of all hardware and software
B. Documentation of system classifications
C. A list of system owners and their departments
D. Third-party risk assessment documentation

7A - Asset Management

NO.5 Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?

A. A full inventory of all hardware and software
B. Documentation of system classifications
C. A list of system owners and their departments
D. Third-party risk assessment documentation

7A - Asset Management

NO.6 An IT security team is concerned about the confidentiality of documents left unattended in MFPs.

Which of the following should the security team do to mitigate the situation?

A. Educate users about the importance of paper shredder devices.

B. Deploy an authentication factor that requires ln-person action before printing.

C. Install a software client in every computer authorized to use the MFPs.

D. Update the management software to utilize encryption.

7A - Asset Management

NO.6 An IT security team is **concerned about the confidentiality** of documents left unattended in MFPs.

Which of the following should the security team do to mitigate the situation?

A. Educate users about the importance of paper shredder devices.

B. Deploy an authentication factor that requires ln-person action before printing.

C. Install a software client in every computer authorized to use the MFPs.

D. Update the management software to utilize encryption.

7A - Asset Management

NO.7 The Chief Information Security Officer (CISO) asks a security analyst to install an OS update to a production VM that has a 99% uptime SLA. The CISO tells the analyst the installation must be done as quickly as possible.

Which of the following courses of action should the security analyst take first?

A. Log in to the server and perform a health check on the VM.

B. Install the patch Immediately.

C. Confirm that the backup service is running.

D. Take a snapshot of the VM.

7A - Asset Management

NO.7 The Chief Information Security Officer (CISO) asks a security analyst to install an OS update to a production VM that has a 99% uptime SLA. The CISO tells the analyst the installation must be done as quickly as possible.

Which of the following courses of action should the security analyst take first?

A. Log in to the server and perform a health check on the VM.

B. Install the patch Immediately.

C. Confirm that the backup service is running.

D. Take a snapshot of the VM.

7A - Asset Management

NO.8 A systems administrator wants to implement a backup solution. The solution needs to allow recovery of the entire system, including the operating system, in case of a disaster.

Which of the following backup types should the administrator consider?

A. Incremental

B. Storage area network

C. Differential

D. Image

7A - Asset Management

NO.8 A systems administrator wants to implement a backup solution. The solution needs to allow **recovery of the entire system**, including the operating system, in case of a disaster.

Which of the following backup types should the administrator consider?

A. Incremental

B. Storage area network

C. Differential

D. Image

7A - Asset Management

NO.9 During a recent company safety stand-down, the cyber-awareness team gave a presentation on the importance of cyber hygiene. One topic the team covered was best practices for printing centers.

Which of the following describes an attack method that relates to printing centers?

A. Whaling

B. Credential harvesting

C. Prepending

D. Dumpster diving

7A - Asset Management

NO.9 During a recent company safety stand-down, the cyber-awareness team gave a presentation on the **importance of cyber hygiene**. One topic the team covered was <u>best practices for printing centers.</u>

Which of the following describes an attack method that relates to printing centers?

A. Whaling

B. Credential harvesting

C. Prepending

D. Dumpster diving

7A - Asset Management

NO.10 An important patch for a critical application has just been released, and a systems administrator is identifying all of the systems requiring the patch.

Which of the following must be maintained in order to ensure that all systems requiring the patch are updated?

A. Asset inventory

B. Network enumeration

C. Data certification

D. Procurement process

7A - Asset Management

NO.10 An important patch for a critical application has just been released, and a systems administrator is identifying all of the systems requiring the patch.

Which of the following must be maintained in order to ensure that all systems requiring the patch are updated?

A. Asset inventory

B. Network enumeration

C. Data certification

D. Procurement process

7B - Redundancy Strategies

7B - Redundancy Strategies

NO.1 An organization is building a new backup data center with cost-benefit as the primary requirement and RTO and RPO values around two days.
Which of the following types of sites is the best for this scenario?

A. Real-time recovery
B. Hot
C. Cold
D. Warm

7B - Redundancy Strategies

NO.1 An organization is building a new backup data center with cost-benefit as the primary requirement and RTO and RPO values around two days.
Which of the following types of sites is the best for this scenario?

A. Real-time recovery
B. Hot
C. Cold
D. Warm

7B - Redundancy Strategies

NO.2 A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption. Which of the following best describes this step?

A. Capacity planning
B. Redundancy
C. Geographic dispersion
D. Tablet exercise

7B - Redundancy Strategies

NO.2 A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption. Which of the following best describes this step?

A. Capacity planning
B. Redundancy
C. Geographic dispersion
D. Tablet exercise

7B - Redundancy Strategies

NO.3 A company is planning a disaster recovery site and needs to ensure that a single natural disaster would not result in the complete loss of regulated backup dat
Which of the following should the company consider?

A. Geographic dispersion
B. Load balancing
C. Hot site
D. Platform diversity

7B - Redundancy Strategies

NO.3 A company is planning a disaster recovery site and needs to ensure that a single natural disaster would not result in the complete loss of regulated backup dat
Which of the following should the company consider?

A. Geographic dispersion
B. Load balancing
C. Hot site
D. Platform diversity

7B - Redundancy Strategies

NO.4 Which of the following can be used to identify potential attacker activities without affecting production servers?

A. Honey pot
B. Video surveillance
C. Zero Trust
D. Geofencing

7B - Redundancy Strategies

NO.4 Which of the following can be used to identify potential attacker activities without affecting production servers?

A. Honey pot
B. Video surveillance
C. Zero Trust
D. Geofencing

7B - Redundancy Strategies

NO.5 A company is concerned about weather events causing damage to the server room and downtime.
Which of the following should the company consider?

A. Clustering servers
B. Geographic dispersion
C. Load balancers
D. Off-site backups

7B - Redundancy Strategies

NO.5 A company is concerned about weather events causing damage to the server room and downtime.
Which of the following should the company consider?

A. Clustering servers
B. Geographic dispersion
C. Load balancers
D. Off-site backups

7B - Redundancy Strategies

NO.6 Which of the following must be considered when designing a high-availability network? (Choose two).

A. Ease of recovery
B. Ability to patch
C. Physical isolation
D. Responsiveness
E. Attack surface
F. Extensible authentication

7B - Redundancy Strategies

NO.6 Which of the following must be considered when designing a high-availability network? (Choose two).

A. Ease of recovery
B. Ability to patch
C. Physical isolation
D. Responsiveness
E. Attack surface
F. Extensible authentication

7B - Redundancy Strategies

NO.7 Which of the following must be considered when designing a high-availability network? (Select two).

A. Ease of recovery
B. Ability to patch
C. Physical isolation
D. Responsiveness
E. Attack surface
F. Extensible authentication

7B - Redundancy Strategies

NO.7 Which of the following must be considered when designing a high-availability network? (Select two).

A. Ease of recovery
B. Ability to patch
C. Physical isolation
D. Responsiveness
E. Attack surface
F. Extensible authentication

7B - Redundancy Strategies

NO.8 An organization is building a single virtual environment that will host customer applications and data that require availability at all times. The data center that is hosting the environment will provide generator power and ISP services.
Which of the following is the best solution to support the organization's requirement?

A. NIC teaming
B. Cloud backups
C. A load balancer appliance
D. UPS

7B - Redundancy Strategies

NO.8 An organization is building a single virtual environment that will host customer applications and data that require availability at all times. The data center that is hosting the environment will provide generator power and ISP services.
Which of the following is the best solution to support the organization's requirement?

A. NIC teaming
B. Cloud backups
C. A load balancer appliance
D. UPS

7B - Redundancy Strategies

NO.9 Which of the following exercises should an organization use to improve its incident response process?

A. Tabletop
B. Replication
C. Failover
D. Recovery

7B - Redundancy Strategies

NO.9 Which of the following exercises should an organization use to improve its incident response process?

A. Tabletop
B. Replication
C. Failover
D. Recovery

7B - Redundancy Strategies

NO.10 Which of the following is classified as high availability in a cloud environment?

A. Access broker
B. Cloud HSM
C. WAF
D. Load balancer

7B - Redundancy Strategies

NO.10 Which of the following is classified as **high availability** in a cloud environment?

A. Access broker
B. Cloud HSM
C. WAF
D. Load balancer

7B - Redundancy Strategies

NO.11 Which of the following would most likely mitigate the impact of an extended power outage on a company's environment?

A. Hot site
B. UPS
C. Snapshots
D. SOAR

7B - Redundancy Strategies

NO.11 Which of the following would most likely **mitigate the impact of an extended power outage** on a company's environment?

A. Hot site
B. UPS
C. Snapshots
D. SOAR

7B - Redundancy Strategies

NO.12 A company that is located in an area prone to hurricanes is developing a disaster recovery plan and looking at site considerations that allow the company to immediately continue operations.

Which of the following is the best type of site for this company?
A. Cold
B. Tertiary
C. Warm
D. Hot

7B - Redundancy Strategies

NO.12 A company that is located in an area prone to hurricanes is **developing a disaster recovery plan** and looking at site considerations that allow the company to immediately continue operations.

Which of the following is the best type of site for this company?

A. Cold

B. Tertiary

C. Warm

D. Hot

7B - Redundancy Strategies

NO.13 Various stakeholders are meeting to discuss their hypothetical roles and responsibilities in a specific situation, such as a security incident or major disaster.

Which of the following best describes this meeting?

A. Penetration test

B. Continuity of operations planning

C. Tabletop exercise

D. Simulation

7B - Redundancy Strategies

NO.13 Various stakeholders are meeting to discuss their **hypothetical roles and responsibilities** in a specific situation, such as a security incident or major disaster.

Which of the following best describes this meeting?

A. Penetration test

B. Continuity of operations planning

C. Tabletop exercise

D. Simulation

7B - Redundancy Strategies

NO.14 A business needs a recovery site but does not require immediate failover. The business also wants to reduce the workload required to recover from an outage.

Which of the following recovery sites is the best option?

A. Hot

B. Cold

C. Warm

D. Geographically dispersed

7B - Redundancy Strategies

NO.14 A business needs a recovery site but does not require immediate failover. The business also wants to **reduce the workload** required to recover from an outage.

Which of the following recovery sites is the best option?

A. Hot

B. Cold

C. Warm

D. Geographically dispersed

7C - Physical Security

7C - Physical Security

NO.1 Which of the following would be the best ways to ensure only authorized personnel can access a secure facility? (Select two).

A. Fencing
B. Video surveillance
C. Badge access
D. Access control vestibule
E. Sign-in sheet
F. Sensor

7C - Physical Security

NO.1 Which of the following would be the best ways to ensure only authorized personnel can access a secure facility? (Select two).

A. Fencing
B. Video surveillance
C. Badge access
D. Access control vestibule
E. Sign-in sheet
F. Sensor

7C - Physical Security

NO.2 Which of the following is the best way to secure an on-site data center against intrusion from an insider?

A. Bollards
B. Access badge
C. Motion sensor
D. Video surveillance

7C - Physical Security

NO.2 Which of the following is the best way to secure an on-site data center against **intrusion from an insider?**

A. Bollards
B. Access badge
C. Motion sensor
D. Video surveillance

7C - Physical Security

NO.3 To improve the security at a data center, a security administrator implements a CCTV system and posts several signs about the possibility of being filmed.

Which of the following best describe these types of controls? (Select two).

A. Preventive
B. Deterrent
C. Corrective
D. Directive
E. Compensating
F. Detective

7C - Physical Security

NO.3 To improve the security at a data center, a security administrator implements a **CCTV system** and posts several signs about the possibility of being filmed.

Which of the following best describe these types of controls? (Select two).

A. Preventive
B. Deterrent
C. Corrective
D. Directive
E. Compensating
F. Detective

7C - Physical Security

NO.4 An organization implemented cloud-managed IP cameras to monitor building entry points and sensitive areas. The service provider enables direct TCP/IP connection to stream live video footage from each camera. The organization wants to ensure this stream is encrypted and authenticated.

Which of the following protocols should be implemented to best meet this objective?

A. SSH

B. SRTP

C. S/MIME

D. PPTP

7C - Physical Security

NO.4 An organization implemented cloud-managed IP cameras to **monitor building entry points and sensitive areas.** The service provider enables direct TCP/IP connection to stream live video footage from each camera. The organization wants to ensure this **stream is encrypted and authenticated.**

Which of the following protocols should be implemented to best meet this objective?

A. SSH

B. SRTP

C. S/MIME

D. PPTP

7C - Physical Security

NO.5 A systems administrator is redesigning now devices will perform network authentication. The following requirements need to be met:

* **An existing Internal certificate must be used.**

* **Wired and wireless networks must be supported**

* **Any unapproved device should be Isolated in a quarantine subnet**

* **Approved devices should be updated before accessing resources**

Which of the following would best meet the requirements?

A. 802.1x

B. EAP

C. RADIUS

D. WPA2

7C - Physical Security

NO.5 A systems administrator is redesigning now devices will perform network authentication. The following requirements need to be met:

* **An existing Internal certificate must be used.**

* **Wired and wireless networks must be supported**

* **Any unapproved device should be Isolated in a quarantine subnet**

* **Approved devices should be updated before accessing resources**

Which of the following would best meet the requirements?

A. 802.1x

B. EAP

C. RADIUS

D. WPA2

THANKS!

Any questions?

Our Graduates are Hired By

DEPARTMENT OF EDUCATION ★ UNITED STATES OF AMERICA ★

Google

Deloitte.

AT&T

ally
do it right.

DEN NORSKE KIRKE
Kirkepartner

Robinhood

VIZNET

COMCAST

INSPARK

ING BANK

proValus™

SOCRadar®
Extension to Your SOC Team!

AGILIS
TECHNOLOGIES

Humana
Wellness

EQUANS

BGA
SECURITY

BBS

gravity
IT RESOURCES

GetMoneyGlobal

proximus

northramp

ease
LEARNING