

CLARUSWAY

WAY TO REINVENT YOURSELF



CompTIA (14A-14B-14C)

AGENDA

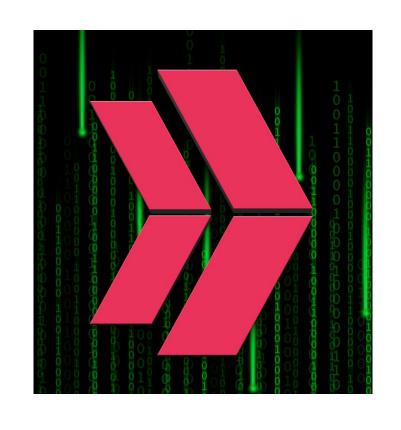


- 14A Policies, Standards, and Procedures
- 14B Change Management
- 14C Automation and Orchestration

AGENDA



- 14A Policies, Standards, and Procedures (5)
- 14B Change Management (7)
- 14C Automation and Orchestration (4)
- ► **TOTAL**: **16**



CompTIA (14A)







NO1. A company hired a security manager from outside the organization to lead security operations.

Which of the following actions should the security manager perform first in this new role?

- A. Establish a security baseline.
- **B.** Review security policies.
- **C.** Adopt security benchmarks.
- **D.** Perform a user ID revalidation.



NO1. A company hired a security manager from outside the organization to lead security operations.

Which of the following actions should the security manager perform first in this new role?

- A. Establish a security baseline.
- B. Review security policies.
- C. Adopt security benchmarks.
- **D.** Perform a user ID revalidation.



NO.2 Which of the following data roles is responsible for identifying risks and appropriate access to data?

- A. Owner
- B. Custodian
- C. Steward
- D. Controller



NO.2 Which of the following data roles is responsible for identifying risks and appropriate access to data?

- A. Owner
- B. Custodian
- C. Steward
- D. Controller



NO.3 A security team created a document that details the order in which critical systems should be through back online after a major outage.

Which of the following documents did the team create?

- A. Communication plan
- B. Incident response plan
- C. Data retention policy
- D. Disaster recovery plan



NO.3 A security team **created a document** that details the order in which <u>critical</u> systems should be through back online after a major outage.

Which of the following documents did the team create?

- A. Communication plan
- B. Incident response plan
- C. Data retention policy
- D. Disaster recovery plan



NO.4 Which of the following topics would most likely be included within an organization's SDLC?

- A. Service-level agreements
- B. Information security policy
- C. Penetration testing methodology
- D. Branch protection requirements



NO.4 Which of the following topics would most likely be included within an organization's SDLC?

- A. Service-level agreements
- B. Information security policy
- C. Penetration testing methodology
- D. Branch protection requirements



NO.5 Which of the following environments utilizes a subset of customer data and is most likely to be used to assess the impacts of major system upgrades and demonstrate system features?

- A. Development
- B. Test
- C. Production
- D. Staging



NO.5 Which of the following environments **utilizes a subset of customer data** and is most likely to be used <u>to assess the impacts of major system upgrades and demonstrate system features?</u>

A. Development

B. Test

C. Production

D. Staging



CompTIA (14B)







NO.1 Which of the following should a security administrator adhere to when setting up a new set of firewall rules?

- A. Disaster recovery plan
- B. Incident response procedure
- C. Business continuity plan
- D. Change management procedure



NO.1 Which of the following should a **security administrator** adhere to when **setting up a new set of firewall rules**?

- A. Disaster recovery plan
- B. Incident response procedure
- C. Business continuity plan
- D. Change management procedure



NO.2 A technician needs to apply a high-priority patch to a production system.

Which of the following steps should be taken first?

- A. Air gap the system.
- B. Move the system to a different network segment.
- C. Create a change control request.
- D. Apply the patch to the system.



NO.2 A technician needs to apply a high-priority patch to a production system.

Which of the following steps should be taken <u>first</u>?

- A. Air gap the system.
- B. Move the system to a different network segment.
- C. Create a change control request.
- D. Apply the patch to the system.



NO.3 Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?

- A. Impact analysis
- B. Scheduled downtime
- C. Backout plan
- D. Change management boards



NO.3 Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?

A. Impact analysis

B. Scheduled downtime

C. Backout plan

D. Change management boards



NO.4 Which of the following practices would be best to prevent an insider from introducing malicious code into a company's development process?

- A. Code scanning for vulnerabilities
- B. Open-source component usage
- C. Quality assurance testing
- D. Peer review and approval



NO.4 Which of the following practices would be best **to prevent an insider** from introducing malicious code into a company's development process?

- A. Code scanning for vulnerabilities
- B. Open-source component usage
- C. Quality assurance testing
- D. Peer review and approval



NO.5 Which of the following describes effective change management procedures?

- A. Approving the change after a successful deployment
- **B.** Having a backout plan when a patch fails
- C. Using a spreadsheet for tracking changes
- **D.** Using an automatic change control bypass for security updates



NO.5 Which of the following describes effective change management procedures?

- A. Approving the change after a successful deployment
- B. Having a backout plan when a patch fails
- C. Using a spreadsheet for tracking changes
- **D.** Using an automatic change control bypass for security updates



NO.6 A systems administrator would like to deploy a change to a production system.

Which of the following must the administrator submit to demonstrate that the system can be restored to a working state in the event of a performance issue?

- A. Backout plan
- **B.** Impact analysis
- C. Test procedure
- **D.** Approval procedure



NO.6 A systems administrator would like to deploy a change to a production system.

Which of the following must the administrator submit to demonstrate that the **system** can be restored to a working state in the event of a performance issue?

- A. Backout plan
- **B.** Impact analysis
- C. Test procedure
- **D.** Approval procedure



NO.7 Which of the following is the most important security concern when using legacy systems to provide production service?

- A. Instability
- B. Lack of vendor support
- C. Loss of availability
- D. Use of insecure protocols



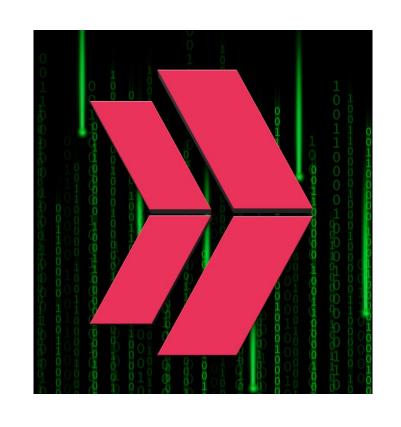
NO.7 Which of the following is the most important security concern when using legacy systems to provide production service?

A. Instability

B. Lack of vendor support

C. Loss of availability

D. Use of insecure protocols



CompTIA (14C)







NO.1 The management team notices that new accounts that are set up manually do not always have correct access or permissions.

Which of the following automation techniques should a systems administrator use to streamline account creation?

- A. Guardrail script
- B. Ticketing workflow
- C. Escalation script
- D. User provisioning script



NO.1 The management team notices that <u>new accounts that are set up manually</u> do not always have correct access or permissions.

Which of the following <u>automation techniques</u> should a systems administrator use **to streamline account creation**?

- A. Guardrail script
- B. Ticketing workflow
- C. Escalation script
- D. User provisioning script





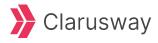
NO.2 Which of the following is the best way to consistently determine on a daily basis whether security settings on servers have been modified?

- A. Automation
- B. Compliance checklist
- C. Attestation
- D. Manual audit



NO.2 Which of the following is the best way to consistently determine **on a daily basis** whether **security settings on servers have been modified**?

- A. Automation
- B. Compliance checklist
- C. Attestation
- D. Manual audit





NO.3 A systems administrator is creating a script that would save time and prevent human error when performing account creation for a large number of end users.

Which of the following would be a good use case for this task?

- A. Off-the-shelf software
- B. Orchestration
- C. Baseline
- D. Policy enforcement



NO.3 A systems administrator is **creating a script** that would save time and prevent human error when performing account creation for a large number of end users.

Which of the following would be a good use case for this task?

- A. Off-the-shelf software
- **B.** Orchestration
- C. Baseline
- D. Policy enforcement



NO.4 A security analyst developed a script to automate a trivial and repeatable task. Which of the following best describes the benefits of ensuring other team members understand how the script works?

- A. To reduce implementation cost
- B. To identify complexity
- C. To remediate technical debt
- D. To prevent a single point of failure



NO.4 A security analyst developed a script to automate a trivial and repeatable task. Which of the following best describes the <u>benefits of ensuring other team members understand how the script works?</u>

- A. To reduce implementation cost
- B. To identify complexity
- C. To remediate technical debt
- D. To prevent a single point of failure



THANKS!

Any questions?





Our Graduates are Hired By





Google Deloitte. AT&T ally













































