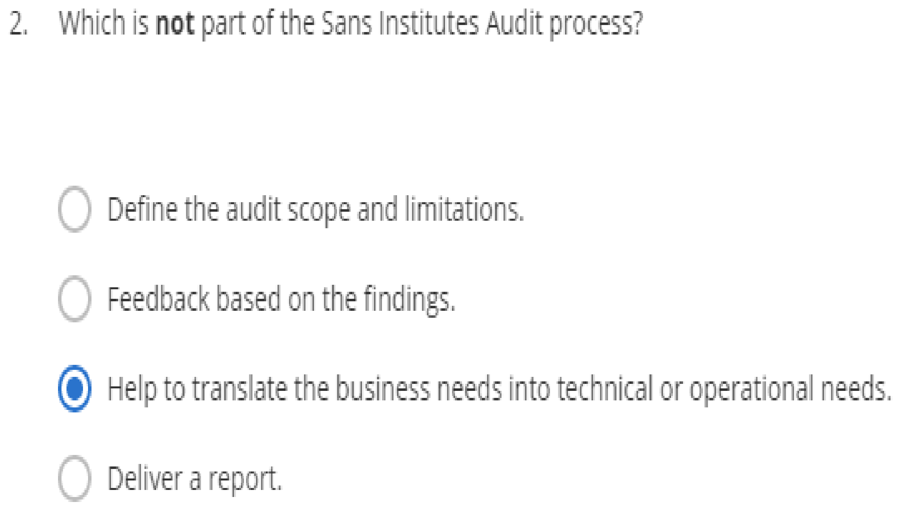
Quiz - Quiz Key concepts



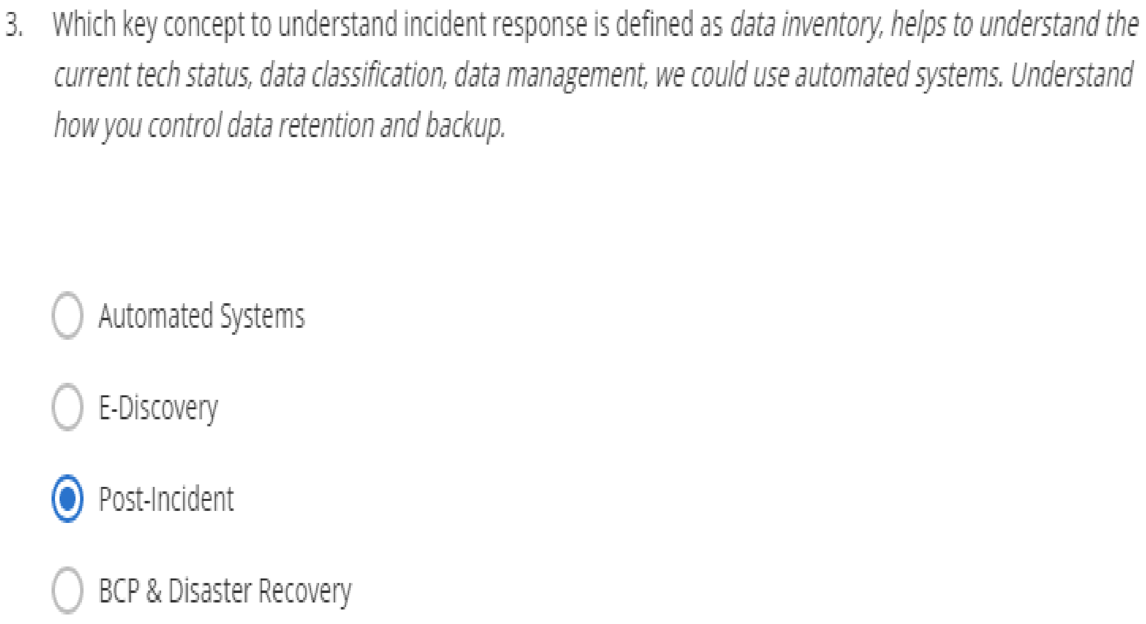
2. Which is **not** part of the Sans Institutes Audit process?

○ Define the audit scope and limitations.

○ Feedback based on the findings.

● Help to translate the business needs into technical or operational needs.

○ Deliver a report.



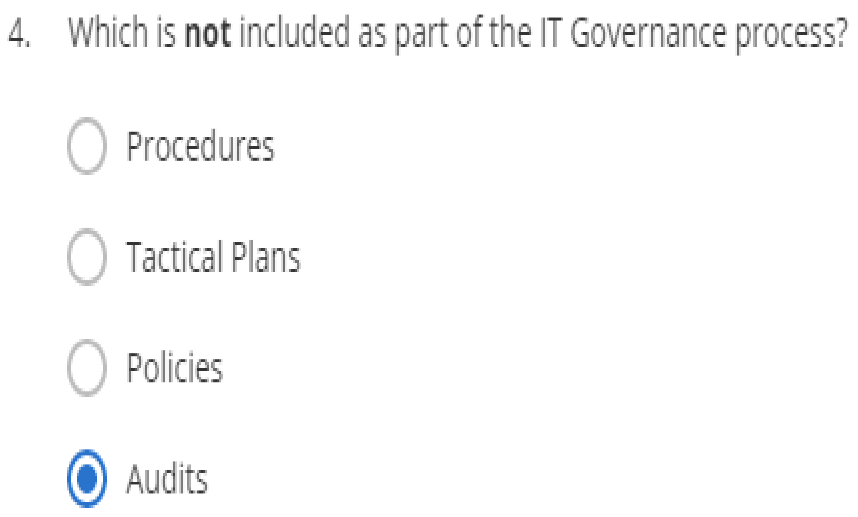
3. Which key concept to understand incident response is defined as *data inventory, helps to understand the current tech status, data classification, data management, we could use automated systems. Understand how you control data retention and backup.*

○ Automated Systems

○ E-Discovery

● Post-Incident

○ BCP & Disaster Recovery



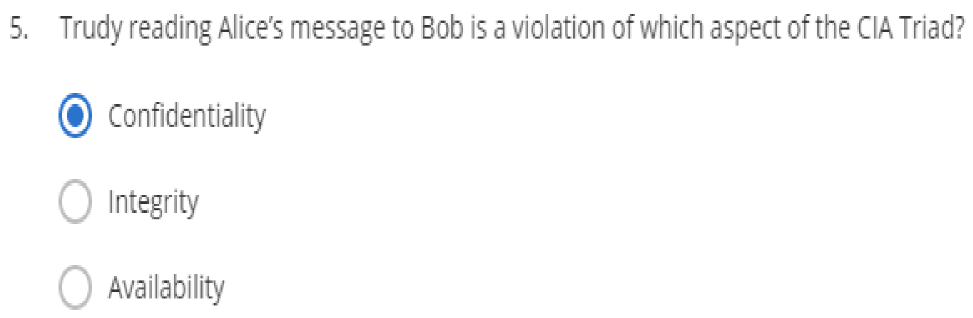
4. Which is **not** included as part of the IT Governance process?

○ Procedures

○ Tactical Plans

○ Policies

● Audits

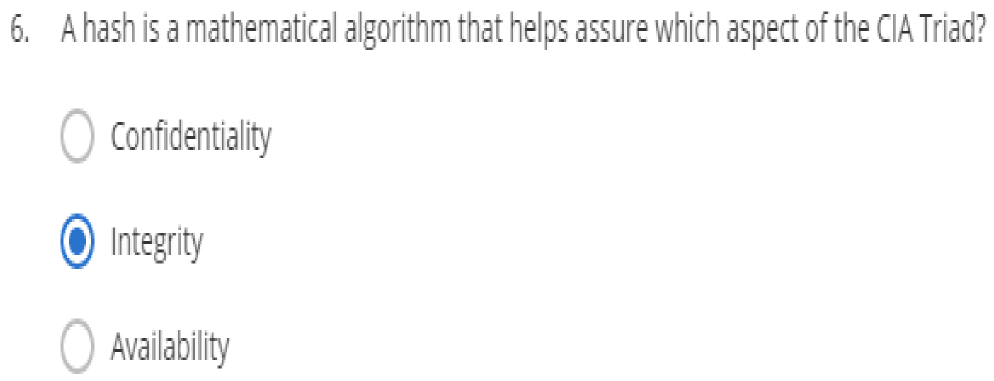


5. Trudy reading Alice's message to Bob is a violation of which aspect of the CIA Triad?

● Confidentiality

○ Integrity

○ Availability

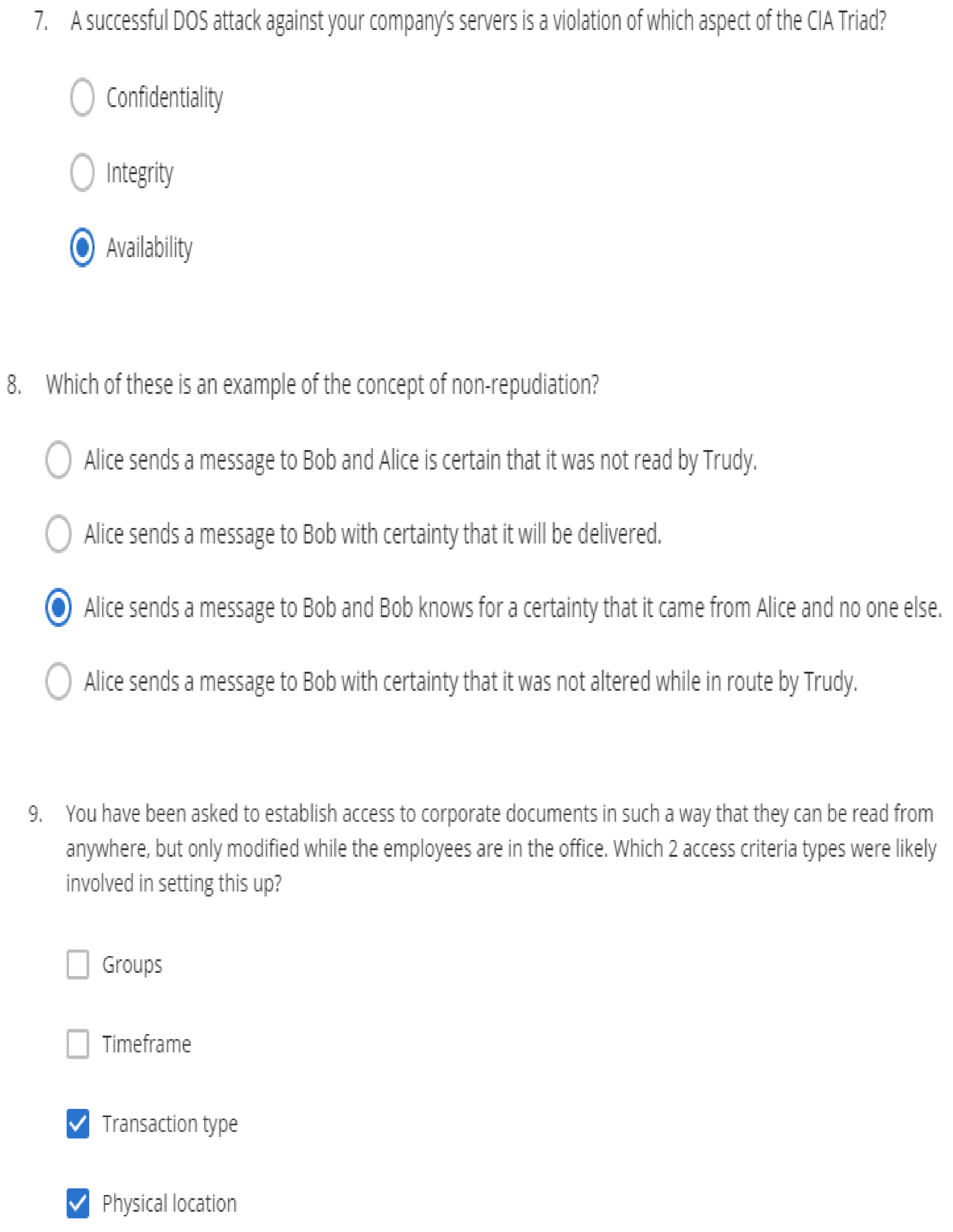


6. A hash is a mathematical algorithm that helps assure which aspect of the CIA Triad?

○ Confidentiality

● Integrity

○ Availability



7. A successful DOS attack against your company's servers is a violation of which aspect of the CIA Triad?

○ Confidentiality

○ Integrity

● Availability

8. Which of these is an example of the concept of non-repudiation?

○ Alice sends a message to Bob and Alice is certain that it was not read by Trudy.

○ Alice sends a message to Bob with certainty that it will be delivered.

● Alice sends a message to Bob and Bob knows for a certainty that it came from Alice and no one else.

○ Alice sends a message to Bob with certainty that it was not altered while in route by Trudy.

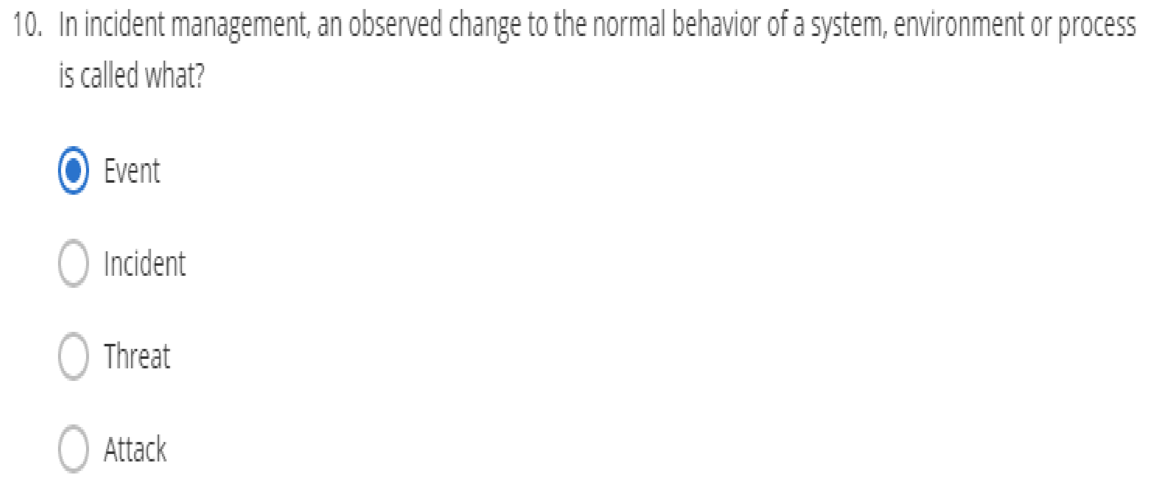
9. You have been asked to establish access to corporate documents in such a way that they can be read from anywhere, but only modified while the employees are in the office. Which 2 access criteria types were likely involved in setting this up?

□ Groups

□ Timeframe

☑ Transaction type

☑ Physical location



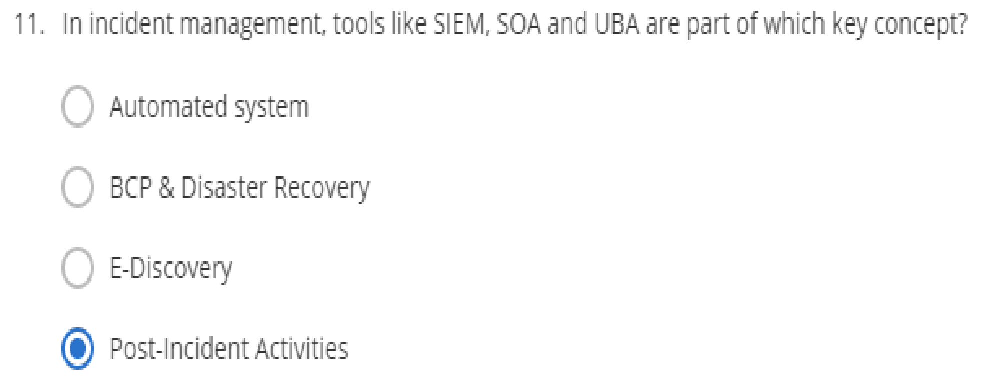
10. In incident management, an observed change to the normal behavior of a system, environment or process is called what?

● Event

○ Incident

○ Threat

○ Attack



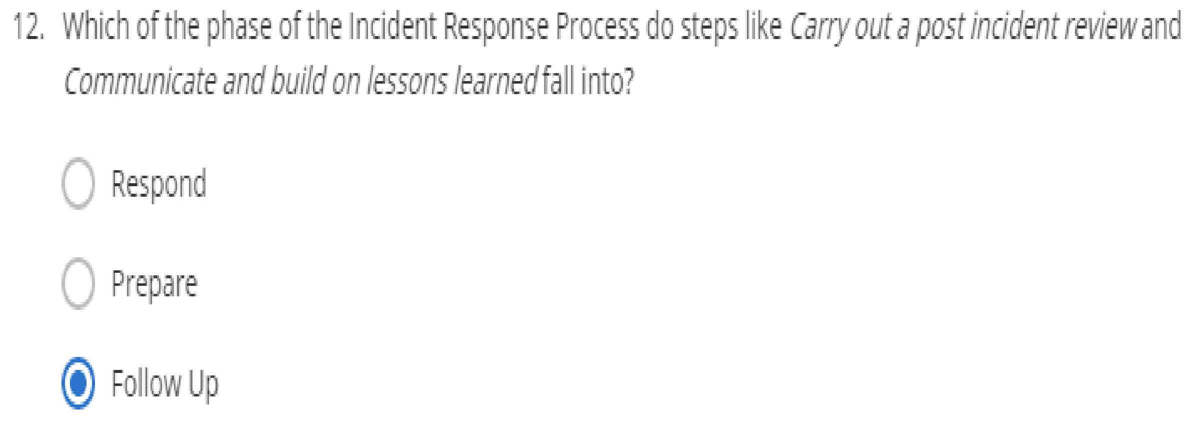
11. In incident management, tools like SIEM, SOA and UBA are part of which key concept?

○ Automated system

○ BCP & Disaster Recovery

○ E-Discovery

● Post-Incident Activities

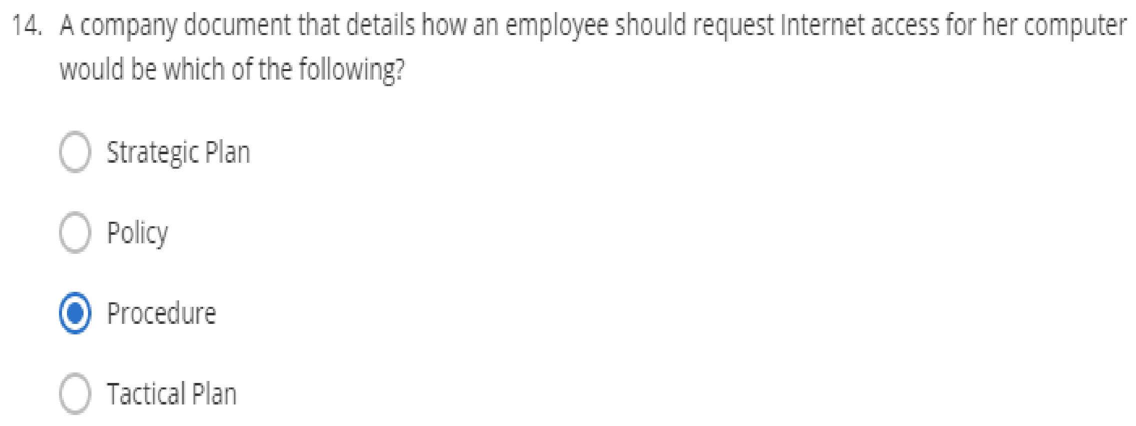


12. Which of the phase of the Incident Response Process do steps like *Carry out a post incident review* and *Communicate and build on lessons learned* fall into?

○ Respond

○ Prepare

● Follow Up



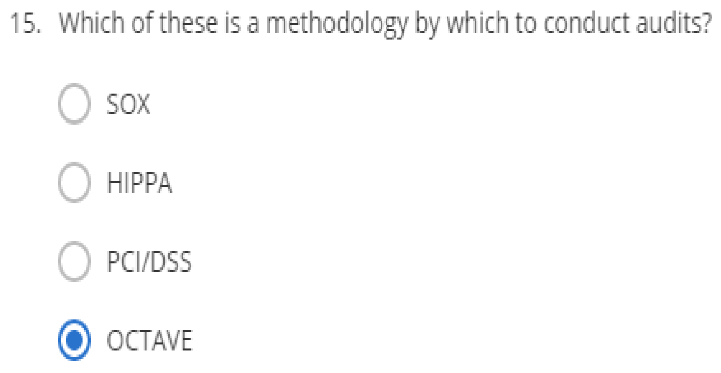
14. A company document that details how an employee should request Internet access for her computer would be which of the following?

○ Strategic Plan

○ Policy

● Procedure

○ Tactical Plan



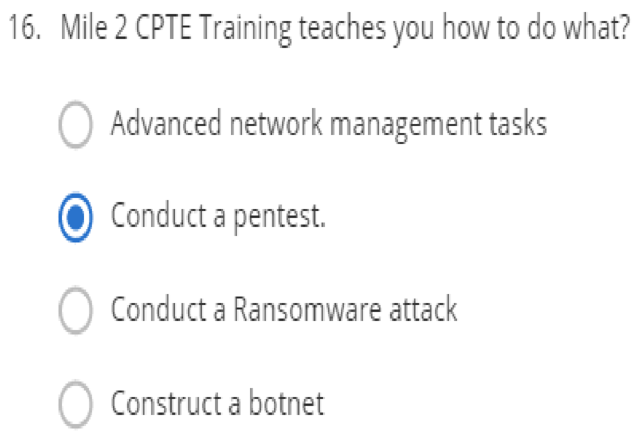
15. Which of these is a methodology by which to conduct audits?

○ SOX

○ HIPPA

○ PCI/DSS

● OCTAVE



16. Mile 2 CPTE Training teaches you how to do what?

○ Advanced network management tasks

● Conduct a pentest.

○ Conduct a Ransomware attack

○ Construct a botnet