

1. A security attack is defined as which of the following?

1 point

☐ All cybersecurity events.

☒ An event that has been identified by correlation and analytics tools as a malicious activity.

☐ An event that has been reviewed by analysts and deemed worthy of deeper investigation.

☐ An event on a system or network detected by a device.
2. Which order does a typical compliance process follow?

1 point

☐ Readiness assessment, establish scope, testing/auditing, management reporting, gap remediation

☐ Readiness assessment, establish scope, gap remediation, testing/auditing, management reporting

☒ Establish scope, readiness assessment, gap remediation, testing/auditing, management reporting

☐ Establish scope, readiness assessment, testing/auditing, management reporting, gap remediation
3. Under GDPR, who determines the purpose and means of processing of personal data?

1 point

☒ Controller

☐ Analyst

☐ Data Subject

☐ Processor
4. Under the International Organization for Standardization (ISO), which standard focuses on Privacy?

1 point

☐ ISO 27003

☒ ISO 27018

☐ ISO 27001

☐ ISO 27017
5. Which SOC report is closest to an ISO report?

1 point

☒ Type 1

☐ Type 3

☐ Type 1 and Type 2

☐ Type 2
6. What is an auditor looking for when they test the control for implementation over an entire offering with no gaps?

1 point

☐ Consistency

☐ Accuracy

☐ Timeliness

☒ Completeness
7. The HIPAA Security Rule requires covered entities to maintain which three (3) reasonable safeguards for protecting e-PHI?

1 point

☒ technical

☐ operational

☒ physical

☒ administrative
8. HIPAA Administrative safeguards include which two (2) of the following?

1 point

☒ Security Personnel

☐ Access controls

☒ Workforce training and management

☐ Integrity controls
9. Who is the governing entity for HIPAA?

1 point

☐ Department of Homeland Security

☐ US Legislature

☒ US Department of Health and Human Services Office of Civil Rights

☐ Cyber Security and Infrastructure Security Agency (CISA)
10. HIPAA Physical safeguards include which two (2) of the following?

1 point

☒ Facility Access and Control

☐ Transmission Security

☐ Information Access Management

☒ Workstation and Device Security
11. PCI uses which three (3) of the following Card Holder Data Environment categories to determine scope?

1 point

☒ Processes

☒ People

☒ Technology

☐ Governance
12. One PCI Requirement is using an approved scanning vendor to scan at what frequency?

1 point

☐ Weekly

☐ Monthly

☒ Quarterly

☐ Annually
13. In which CIS control category will you find Incident Response and Management?


1 point

☒ Organizational

☐ Foundational

☐ Advanced

☐ Basic

Coursera Honor Code [Learn more](#) 

☒ I, **Giang Pham**, understand that submitting work that isn't my own may result in permanent failure of this course or deactivation of my Coursera account.

Submit

Save draft