Quiz - Compliance Frameworks and Industry Standards

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

- ○ An event on a system or network detected by a device.
- ○ 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.

---

2. Which order does a typical compliance process follow?

- ◉ Establish scope, readiness assessment, gap remediation, testing/auditing, management reporting
- ○ Readiness assessment, establish scope, gap remediation, testing/auditing, management reporting
- ○ Readiness assessment, establish scope, testing/auditing, management reporting, gap remediation
- ○ Establish scope, readiness assessment, testing/auditing, management reporting, gap remediation

---

3. Under GDPR who determines the purpose and means of processing of personal data?

- ○ Data Subject
- ○ Processor
- ○ Analyst
- ◉ Controller

---

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

- ◉ ISO 27018
- ○ ISO 27001
- ○ ISO 27003
- ○ ISO 27017

---

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

- ◉ Type 1
- ○ Type 1 and Type 2
- ○ Type 3
- ○ Type 2

---

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

- ○ Consistency
- ○ Accuracy
- ◉ Completeness
- ○ Timeliness

---

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

- ☑ physical
- ☑ administrative
- ☐ operational
- ☑ technical

---

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

- ☐ Integrity controls
- ☑ Workforce training and management
- ☑ Security Personnel
- ☐ Access controls

---

9. Who is the governing entity for HIPAA?

- ○ Cyber Security and Infrastructure Security Agency (CISA)
- ◉ US Department of Health and Human Services Office of Civil Rights
- ○ Department of Homeland Security
- ○ US Legislature

---

10. HIPAA Physical safeguards include which two (2) of the following?

- ☑ Workstation and Device Security
- ☐ Information Access Management
- ☑ Facility Access and Control
- ☐ Transmission Security

---

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

- ☑ Processes
- ☑ Technology
- ☑ People
- ☐ Governance

---

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

- ○ Weekly
- ○ Monthly
- ◉ Quarterly
- ○ Annually

---

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

- ○ Foundational
- ○ Basic
- ○ Advanced
- ◉ Organizational
