

Exam Name - Certified Information Security Professional (CISP)[™]

Sample Exam

1. Which statement best defines the CIA Triad?

- A. Confidentiality, Integrity, Accessibility
- B. Confidentiality, Integrity, Availability
- C. Access, Integrity, Authentication
- D. Confidentiality, Authentication, Accountability

Answer **B**

2. What formula represents Annualized Loss Expectancy (ALE)?

- A. Asset Value × Exposure Factor × Annualized Rate of Occurrence
- B. Single Loss Expectancy × Exposure Factor
- C. Single Loss Expectancy × Annualized Rate of Occurrence
- D. Asset Value × Frequency of Occurrence

Answer **C**

3. Partial-knowledge (grey-box) penetration testing means the tester

- A. Has no prior system knowledge
- B. Has full system knowledge
- C. Has some details like network ranges or architecture
- D. Uses automated tools only

Answer **C**

4. Which is an open standard for exchanging authentication and authorization data?

- A. HTML
- B. XML
- C. JSON
- D. SAML

Answer **D**

5. The Maximum Tolerable Downtime (MTD) equals

- A. $RTO + WRT$
- B. $ALE \times \text{Frequency}$
- C. $SLE + ARO$
- D. $RPO + WRT$

Answer **A**

6. Which entity is the individual linked to PII?

- A. Data Controller
- B. Data Processor
- C. Data Owner
- D. Data Subject

Answer **D**