

CISSP

CERTIFICATION EXAM PREP

Practice Test Bank — Free Edition

QUESTIONS	DOMAIN	DIFFICULTY	FORMAT
50	Domain 1 Security & Risk Mgmt	Easy / Medium / Hard	4-Option MCQ

ABOUT THIS TEST BANK This free test bank covers all 50 questions from CISSP Domain 1 — Security and Risk Management — the largest domain, weighted at 15–19% of the actual exam. Every question includes a detailed explanation explaining the correct answer and why the distractors are wrong. Study the WHY, not just the answer.

HOW TO USE THIS PRACTICE TEST

01	Simulate real exam pacing Allow 75 seconds per question — the pace you need on the actual CISSP exam (125 questions, 3 hours).
02	Read every explanation Even questions you answered correctly. Understanding WHY each answer is right (and others are wrong) builds exam readiness.
03	Flag uncertain answers Mark any question you guessed or were unsure about. Return to those topics before sitting the real exam.
04	Think like a manager The CISSP tests strategic, risk-based thinking. When two answers seem right, choose the one a senior security manager would prioritize.
05	Score target: 80%+ 90–100% = Excellent 80–89% = On track 70–79% = More review needed Below 70% = Intensive study required.

UNLOCK THE PREMIUM EDITION Get 300 questions across ALL 8 CISSP domains with advanced explanations, scenario-based questions matching actual exam difficulty, a quick-reference formula sheet, and domain-by-domain score tracking. Visit threatnexus.com to upgrade.

D1**SECURITY AND RISK MANAGEMENT**

Questions 1–50 | Domain 1: Security and Risk Management | Exam Weight: 15–19% | Select the BEST answer for each question.

Question 1**MEDIUM**

An organization is selecting a risk treatment option for a vulnerability that would cost \$500,000 to remediate but only has a potential loss of \$50,000. Which risk response is MOST appropriate?

- A. Risk avoidance
- B. Risk acceptance
- C. Risk mitigation
- D. Risk transference

Question 2**HARD**

What is the PRIMARY purpose of a Business Impact Analysis (BIA)?

- A. To identify all threats to an organization
- B. To determine the Maximum Tolerable Downtime and recovery priorities for critical business functions
- C. To calculate the Annual Loss Expectancy for each asset
- D. To assign responsibility for disaster recovery procedures

Question 3**MEDIUM**

Which formula correctly represents Annual Loss Expectancy (ALE)?

- A. $ALE = Asset\ Value \times Threat\ Frequency$
- B. $ALE = SLE \times ARO$
- C. $ALE = SLE / ARO$
- D. $ALE = Asset\ Value / Exposure\ Factor$

Question 4**EASY**

Which of the following BEST describes the concept of 'due care'?

- A. Researching what security controls other companies use
- B. Taking reasonable actions to protect assets, demonstrating that management acted responsibly
- C. Documenting all security policies and procedures
- D. Hiring qualified security personnel

Question 5**HARD**

An organization has a policy that two employees must be present when accessing the safe. This is an example of which security principle?

- A. Least privilege
- B. Separation of duties
- C. Two-person integrity (dual control)
- D. Need to know

Question 6**MEDIUM**

Which type of law creates duties between private parties and provides for civil remedies?

- A. Criminal law
- B. Administrative law
- C. Tort law
- D. Regulatory law

Question 7**MEDIUM**

What does the term 'residual risk' mean?

- A. The risk that remains after all controls are considered too expensive
- B. The risk that remains after security controls have been applied
- C. The initial risk before any controls are implemented
- D. The risk transferred to an insurance company

Question 8**HARD**

Which of the following is the CORRECT order of data classification sensitivity from highest to lowest in a U.S. government context?

- A. Top Secret → Secret → Confidential → Unclassified
- B. Top Secret → Classified → Secret → Public
- C. Secret → Top Secret → Sensitive → Unclassified
- D. Classified → Top Secret → Secret → Public

Question 9**MEDIUM**

A security manager wants to compare the cost of a control against its benefit. Which analysis method is MOST appropriate?

- A. Qualitative risk analysis
- B. Cost-benefit analysis
- C. Business impact analysis
- D. Threat modeling

Question 10**MEDIUM**

Which of the following describes 'privacy by design'?

- A. Adding privacy controls after a system is built
- B. Requiring users to opt in to data collection
- C. Embedding privacy protections into system design from the outset rather than as an afterthought
- D. Encrypting all personal data at rest

Question 11**HARD**

Under GDPR, what is the maximum fine for the most serious violations?

- A. €10 million or 2% of annual global turnover
- B. €20 million or 4% of annual global turnover
- C. €50 million or 10% of annual global turnover
- D. €5 million or 1% of annual global turnover

Question 12**MEDIUM**

Which framework is specifically designed to align IT security controls with business objectives and is widely used for IT governance?

- A. ISO 27001
- B. COBIT
- C. NIST SP 800-53
- D. PCI DSS

Question 13**EASY**

What is the PRIMARY difference between a policy and a standard in an information security program?

- A. Policies are technical; standards are managerial
- B. Policies state high-level management intent; standards provide specific mandatory requirements supporting the policy
- C. Standards are optional guidelines; policies are mandatory
- D. Policies are written by IT; standards are written by HR

Question 14**HARD**

An organization purchases cyber liability insurance to cover the cost of a potential data breach. This is an example of which risk treatment?

- A. Risk avoidance
- B. Risk mitigation
- C. Risk acceptance
- D. Risk transference

Question 15**MEDIUM**

Which regulation specifically governs the protection of health information in the United States?

- A. GLBA
- B. FERPA
- C. HIPAA
- D. SOX

Question 16**MEDIUM**

What is the MAIN goal of a security awareness training program?

- A. To teach employees how to configure security tools
- B. To satisfy compliance requirements
- C. To change employee behavior to reduce human-related security risks
- D. To prepare employees for security certifications

Question 17**HARD**

A company decides to stop offering an online service because the security risks are too high and cannot be adequately mitigated. This is an example of which risk strategy?

- A. Risk transference
- B. Risk mitigation
- C. Risk acceptance
- D. Risk avoidance

Question 18**MEDIUM**

Which of the following is a key characteristic of quantitative risk analysis compared to qualitative risk analysis?

- A. It uses descriptive terms like high, medium, and low
- B. It assigns specific monetary values to assets and losses
- C. It is faster to perform and requires less data
- D. It relies on expert opinion rather than data

Question 19**MEDIUM**

In the context of information security, what does 'non-repudiation' provide?

- A. Ensures only authorized users can access data
- B. Prevents a party from denying they sent or received a communication
- C. Ensures data is not altered during transmission
- D. Verifies the identity of a user at login

Question 20**HARD**

According to ISC2, what is the CORRECT order of the phases in a Business Continuity Plan (BCP) lifecycle?

- A. Develop → Test → Implement → Maintain
- B. Project initiation → BIA → Strategy selection → Plan development → Training and testing → Maintenance
- C. Risk assessment → Policy creation → Implementation → Audit
- D. Threat identification → Vulnerability analysis → Control selection → Documentation

Question 21**MEDIUM**

Which of the following BEST describes the 'need to know' principle?

- A. Users should know about all security incidents that occur
- B. Access to information is granted only when there is a legitimate business reason, regardless of clearance level
- C. Employees should be informed about the security policy
- D. Users with higher clearance can access all data at lower levels

Question 22**HARD**

What is the PRIMARY reason that security policies must have management support?

- A. IT staff will not implement controls without management approval
- B. Management support provides authority, resources, and enforcement capability needed for effective security
- C. Policies require legal review by senior management
- D. Regulations require CEO signature on all security documents

Question 23**MEDIUM**

An SLE for a web server is \$200,000 and the ARO is 0.25. What is the ALE?

- A. \$50,000
- B. \$200,000
- C. \$800,000
- D. \$25,000

Question 24**MEDIUM**

Which role is PRIMARILY responsible for determining the classification level of information?

- A. Custodian
- B. User
- C. Owner
- D. Security officer

Question 25**HARD**

A penetration test authorization letter limits testing to specific IP ranges. The tester discovers an unrelated critical vulnerability outside the authorized scope. What should the tester do FIRST?

- A. Immediately exploit the vulnerability to demonstrate impact
- B. Ignore it, as it is outside the scope of the engagement
- C. Stop testing and notify the client of the discovery without exploiting it
- D. Expand the scope unilaterally to fully test the vulnerability

Question 26**MEDIUM**

What is the purpose of a 'threat model'?

- A. To create a list of all organizational assets
- B. To identify, enumerate, and prioritize threats to a system based on how an attacker might view it
- C. To document security incidents that have occurred
- D. To assign risk ratings to vulnerabilities found during scanning

Question 27**HARD**

Which of the following represents a PRIMARY responsibility of a Chief Information Security Officer (CISO)?

- A. Implementing firewall rules
- B. Writing security patches for software
- C. Aligning the security program with business objectives and managing overall security risk
- D. Performing penetration testing

Question 28**MEDIUM**

SOC 2 Type II reports differ from SOC 2 Type I reports in that Type II reports:

- A. Cover a broader set of security domains
- B. Test controls over a period of time rather than at a point in time
- C. Are intended for internal use only
- D. Require assessment by a government auditor

Question 29**MEDIUM**

What is 'defense in depth' as applied to a security program?

- A. Using the most advanced firewall available
- B. Placing all sensitive data in a single, heavily protected location
- C. Implementing multiple layered security controls so no single failure leads to total compromise
- D. Training all employees to be security professionals

Question 30**HARD**

A company operates in multiple jurisdictions with conflicting data protection laws. The regulation in Country A requires data to be stored locally; Country B requires the same data to be accessible for law enforcement. What is the BEST approach?

- A. Follow whichever law is more stringent
- B. Ignore one country's law to comply with the other
- C. Engage legal counsel to evaluate options including data segregation, localization strategies, and regulatory exemptions
- D. Store the data in a neutral third country

Question 31**MEDIUM**

Which NIST document provides a framework for improving critical infrastructure cybersecurity?

- A. NIST SP 800-53
- B. NIST SP 800-37
- C. NIST Cybersecurity Framework (CSF)
- D. NIST SP 800-171

Question 32**MEDIUM**

What distinguishes a vulnerability from a threat?

- A. A vulnerability is external; a threat is internal
- B. A threat is a potential danger; a vulnerability is a weakness that can be exploited by a threat
- C. A vulnerability is intentional; a threat is accidental
- D. Threats are technical; vulnerabilities are physical

Question 33**HARD**

Which of the following actions would be considered a violation of 'due diligence'?

- A. Implementing a firewall without first assessing threats
- B. Failing to research current security threats and best practices before selecting controls
- C. Accepting a vendor's security claims without verification
- D. Both B and C

Question 34**MEDIUM**

Job rotation is PRIMARILY implemented to address which security concern?

- A. Employee burnout
- B. Fraud detection and prevention of collusion
- C. Skills development
- D. Compliance with labor laws

Question 35**MEDIUM**

According to the (ISC)² Code of Ethics, what is the FIRST canon a member must uphold?

- A. Act honorably, honestly, justly, responsibly, and legally
- B. Protect society, the common good, necessary public trust and confidence, and the infrastructure
- C. Provide diligent and competent service to principals
- D. Advance and protect the profession

Question 36**HARD**

What is the primary difference between a Recovery Time Objective (RTO) and a Recovery Point Objective (RPO)?

- A. RTO is about data; RPO is about systems
- B. RTO is the maximum time to restore a function; RPO is the maximum acceptable data loss measured in time
- C. RTO applies to hardware; RPO applies to software
- D. RTO and RPO are the same metric expressed differently

Question 37**MEDIUM**

Which of the following is an example of 'regulatory compliance' driving security requirements?

- A. A company encrypts data because it improves customer trust
- B. A healthcare provider implements access controls because HIPAA requires it
- C. A bank improves its firewall after a competitor is breached
- D. A CISO recommends MFA because it reduces risk

Question 38**HARD**

What does 'operational security (OPSEC)' primarily focus on?

- A. Securing operating systems against vulnerabilities
- B. Identifying and protecting critical information that could be used by adversaries to harm an organization
- C. Monitoring daily security operations in a SOC
- D. Ensuring backup and recovery procedures work correctly

Question 39**MEDIUM**

A company stores credit card data. Which compliance standard is MOST applicable?

- A. SOX
- B. HIPAA
- C. PCI DSS
- D. FERPA

Question 40**HARD**

What is 'aggregation' in the context of information security?

- A. Combining multiple low-sensitivity data items that together create a high-sensitivity disclosure
- B. Storing all sensitive data in a single location for easier protection
- C. Adding multiple users to a single access group
- D. Merging backup files to save storage space

Question 41**MEDIUM**

When should a penetration test authorization be obtained?

- A. After the test is complete
- B. Only when testing production systems
- C. Before ANY testing begins, regardless of the scope
- D. When requested by management after an incident

Question 42**HARD**

Which of the following BEST describes 'social engineering' as a security threat?

- A. Manipulating software to bypass security controls
- B. Exploiting human psychology to deceive people into divulging information or performing actions
- C. Engineering social media platforms to gather intelligence
- D. A technical attack that mimics normal user behavior

Question 43**MEDIUM**

What is the PRIMARY output of a risk assessment?

- A. A list of security controls to implement
- B. A prioritized list of risks with their likelihood and impact
- C. A business continuity plan
- D. A security policy document

Question 44**HARD**

An employee's background check reveals a prior conviction for financial fraud. They are being considered for a role with access to financial systems. What is the MOST appropriate action?

- A. Automatically reject the candidate
- B. Evaluate the relevance, recency, and nature of the conviction against the specific role requirements in accordance with applicable employment law
- C. Hire the person but restrict their access completely
- D. Require the employee to sign an additional confidentiality agreement

Question 45**MEDIUM**

Which of the following is NOT typically included in a security policy?

- A. Statement of management intent
- B. Scope of the policy
- C. Step-by-step configuration instructions for firewalls
- D. Enforcement consequences for violations

Question 46**HARD**

What is the Annualized Rate of Occurrence (ARO) if a threat is expected to occur once every five years?

- A. 5.0
- B. 0.5
- C. 0.2
- D. 0.02

Question 47**MEDIUM**

Which of the following is the BEST definition of 'information security governance'?

- A. The technical implementation of security controls
- B. The set of responsibilities and practices by which the board and management provide strategic direction, ensure objectives are achieved, and manage risks
- C. The hiring of qualified security personnel
- D. The audit of security controls

Question 48**HARD**

A security team is evaluating whether to adopt ISO 27001 or NIST CSF. What is the PRIMARY distinguishing factor to consider?

- A. ISO 27001 is free; NIST CSF requires a paid license
- B. ISO 27001 offers third-party certification; NIST CSF is a voluntary framework without formal certification
- C. NIST CSF applies only to U.S. government agencies
- D. ISO 27001 requires annual penetration testing; NIST CSF does not

Question 49**MEDIUM**

What is the purpose of a 'data retention policy'?

- A. To determine who can access data
- B. To specify how long data must be kept and when it must be securely destroyed
- C. To classify data by sensitivity level
- D. To establish backup frequency requirements

Question 50**HARD**

Which of the following BEST describes 'privacy' as distinct from 'confidentiality' in information security?

- A. Privacy is a technical control; confidentiality is a policy requirement
- B. Privacy concerns an individual's right to control information about themselves; confidentiality concerns preventing unauthorized disclosure of information
- C. Confidentiality applies to all data types; privacy applies only to medical data
- D. Privacy and confidentiality are interchangeable terms in security

AK

ANSWER KEY WITH DETAILED EXPLANATIONS

The explanations are the most valuable part of this test bank. Read every explanation carefully — including for questions you answered correctly. Understanding the concept behind each answer is what prepares you for the real exam.

1 Answer: B An organization is selecting a risk treatment option for a vulnerability that would cost \$500,000 to remediate but ...

WHY: When the cost of remediation (\$500,000) significantly exceeds the potential loss (\$50,000), risk acceptance is the most cost-effective response. Spending more to fix a risk than the risk is worth is economically irrational.

2 Answer: B What is the PRIMARY purpose of a Business Impact Analysis (BIA)?

WHY: A BIA identifies critical business functions, determines the Maximum Tolerable Downtime (MTD), and establishes recovery time objectives — forming the foundation for business continuity planning.

3 Answer: B Which formula correctly represents Annual Loss Expectancy (ALE)?

WHY: $ALE = \text{Single Loss Expectancy (SLE)} \times \text{Annualized Rate of Occurrence (ARO)}$. SLE itself equals $\text{Asset Value} \times \text{Exposure Factor}$. ALE represents the expected yearly loss from a specific threat.

4 Answer: B Which of the following BEST describes the concept of 'due care'?

WHY: Due care means doing what a reasonable person would do to protect assets — implementing appropriate controls. Due diligence is the research and planning phase; due care is the ongoing action. Both are needed to avoid negligence liability.

5 Answer: C An organization has a policy that two employees must be present when accessing the safe. This is an example of whic...

WHY: Two-person integrity (dual control) requires two people to be present simultaneously to perform an action. Separation of duties splits a task so no single person can complete it alone. Both reduce insider threat but through different mechanisms.

6 Answer: C Which type of law creates duties between private parties and provides for civil remedies?

WHY: Tort law is civil law governing private wrongs between parties. Negligence is a common tort claim in security breach cases. Criminal law involves government prosecution; administrative/regulatory law involves government agency rules.

7 Answer: B What does the term 'residual risk' mean?

WHY: Residual risk is what remains after controls are applied. $\text{Total risk (inherent risk)} - \text{controls applied} = \text{residual risk}$. Management must formally accept residual risk through a risk acceptance process.

8 Answer: A Which of the following is the CORRECT order of data classification sensitivity from highest to lowest in a U.S. gov...

WHY: U.S. government data classification levels from highest to lowest: Top Secret, Secret, Confidential, Sensitive But Unclassified (SBU), and Unclassified. 'Classified' is not a specific level — it is a general term for Top Secret, Secret, and Confidential.

9

Answer: B

A security manager wants to compare the cost of a control against its benefit. Which analysis method is MOST appropriate?

WHY: A cost-benefit analysis directly compares the cost of implementing a control against the benefit (risk reduction). The control is justified when $ALE \text{ (before)} - ALE \text{ (after)} - \text{Annual Cost of Control} > 0$.

10

Answer: C

Which of the following describes 'privacy by design'?

WHY: Privacy by design, developed by Ann Cavoukian, requires that privacy protections be integrated into system design from the start — not bolted on afterward. It is proactive rather than reactive and a core principle in GDPR and modern privacy frameworks.

11

Answer: B

Under GDPR, what is the maximum fine for the most serious violations?

WHY: GDPR has a two-tier penalty structure. Tier 1: up to €10 million or 2% of global annual turnover (lower-level violations). Tier 2: up to €20 million or 4% of global annual turnover (serious violations, including core principles and data subject rights). The higher amount applies.

12

Answer: B

Which framework is specifically designed to align IT security controls with business objectives and is widely used?

WHY: COBIT (Control Objectives for Information and Related Technology) is specifically designed for IT governance and management, aligning IT with business goals. ISO 27001 is an ISMS standard; NIST 800-53 is a U.S. government control catalog; PCI DSS is for payment card security.

13

Answer: B

What is the PRIMARY difference between a policy and a standard in an information security program?

WHY: Security policies express high-level management intent and direction. Standards are mandatory, specific requirements that support the policy. Guidelines are recommended (optional). Procedures are step-by-step implementation instructions.

14

Answer: D

An organization purchases cyber liability insurance to cover the cost of a potential data breach. This is an example of which risk management strategy?

WHY: Risk transference (or sharing) shifts the financial consequences of risk to a third party — most commonly through insurance. The risk still exists, but the financial impact is transferred. Cyber liability insurance is the textbook example.

15

Answer: C

Which regulation specifically governs the protection of health information in the United States?

WHY: HIPAA (Health Insurance Portability and Accountability Act) governs Protected Health Information (PHI) in the U.S. GLBA covers financial data; FERPA covers student education records; SOX covers financial reporting controls for public companies.

16

Answer: C

What is the MAIN goal of a security awareness training program?

WHY: The primary goal of security awareness training is behavioral change — reducing human-related risks such as phishing susceptibility, password misuse, and social engineering. Compliance is a secondary benefit, not the primary goal.

17 Answer: D

A company decides to stop offering an online service because the security risks are too high and cannot be adequate...

WHY: Risk avoidance eliminates the risk entirely by discontinuing the activity that creates it. Stopping the service removes the associated threat surface. This is distinct from mitigation (reducing risk) and acceptance (acknowledging and accepting the remaining risk).

18 Answer: B

Which of the following is a key characteristic of quantitative risk analysis compared to qualitative risk analysis?

WHY: Quantitative risk analysis uses specific numerical values — dollar amounts, percentages, frequencies — to measure risk (e.g., ALE). Qualitative analysis uses descriptive scales (high/medium/low). Quantitative is more objective but requires more data and time.

19 Answer: B

In the context of information security, what does 'non-repudiation' provide?

WHY: Non-repudiation ensures that a party cannot deny performing an action (sending a message, signing a document). Digital signatures provide non-repudiation because only the holder of the private key could have created the signature.

20 Answer: B

According to ISC2, what is the CORRECT order of the phases in a Business Continuity Plan (BCP) lifecycle?

WHY: The BCP lifecycle per ISC2: (1) Project initiation/scope, (2) Business Impact Analysis (BIA), (3) Recovery strategy selection, (4) Plan development, (5) Training and testing, (6) Maintenance. The BIA is always performed before strategy selection because priorities cannot be set without knowing critical function dependencies.

21 Answer: B

Which of the following BEST describes the 'need to know' principle?

WHY: Need to know means that even if a user has the clearance level to access information, they must also have a specific operational need for it. Clearance is necessary but not sufficient. A general with Top Secret clearance still cannot read a compartmented program they have no need to know about.

22 Answer: B

What is the PRIMARY reason that security policies must have management support?

WHY: Without senior management support, security programs lack authority to enforce policies, budget for controls, and cultural influence. Management 'tone from the top' drives security culture. This is not merely procedural — it determines whether the program will succeed.

23 Answer: A

An SLE for a web server is \$200,000 and the ARO is 0.25. What is the ALE?

WHY: $ALE = SLE \times ARO = \$200,000 \times 0.25 = \$50,000$. An ARO of 0.25 means the event is expected once every four years (25% annual probability).

24 Answer: C

Which role is PRIMARILY responsible for determining the classification level of information?

WHY: The data owner (typically a senior business manager) is responsible for determining the classification level and acceptable use of data. The custodian (often IT) implements the controls the owner specifies. The security officer advises but does not own the classification decision.

25 Answer: C A penetration test authorization letter limits testing to specific IP ranges. The tester discovers an unrelated cri...

WHY: Professional ethics and most penetration testing standards (including PTES) require testers to notify the client of significant out-of-scope findings without exploiting them. Proceeding without authorization would be unauthorized access (illegal). The client can then decide whether to expand scope formally.

26 Answer: B What is the purpose of a 'threat model'?

WHY: Threat modeling (e.g., using STRIDE, PASTA, or DREAD methodologies) systematically identifies potential threats to a system from an attacker's perspective. It is performed early in the design phase to inform security requirements before implementation.

27 Answer: C Which of the following represents a PRIMARY responsibility of a Chief Information Security Officer (CISO)?

WHY: The CISO is an executive role focused on strategic alignment of security with business goals, risk management, governance, and communication with the board. Implementation tasks belong to security engineers and analysts. The CISO is responsible TO the business, not just for technical security.

28 Answer: B SOC 2 Type II reports differ from SOC 2 Type I reports in that Type II reports:

WHY: SOC 2 Type I assesses whether controls are suitably designed at a specific point in time. SOC 2 Type II assesses whether those controls operated effectively over a period (typically 6–12 months). Type II provides stronger assurance because it tests actual operation, not just design.

29 Answer: C What is 'defense in depth' as applied to a security program?

WHY: Defense in depth applies multiple, overlapping security controls (preventive, detective, corrective) at different layers. If one control fails, others limit the damage. It reflects the assumption that any single control can be bypassed or fail.

30 Answer: C A company operates in multiple jurisdictions with conflicting data protection laws. The regulation in Country A req...

WHY: Conflicting international legal requirements are a complex governance issue requiring legal expertise. A security professional's role is to escalate to legal counsel, not to make unilateral legal interpretations. Solutions might include data localization, contractual mechanisms, or regulatory exemption applications.

31 Answer: C Which NIST document provides a framework for improving critical infrastructure cybersecurity?

WHY: The NIST Cybersecurity Framework (CSF) organizes security activities into five functions: Identify, Protect, Detect, Respond, Recover. It is voluntary but widely adopted. SP 800-53 is the control catalog; SP 800-37 is the Risk Management Framework (RMF); SP 800-171 covers CUI in non-federal systems.

32 Answer: B What distinguishes a vulnerability from a threat?

WHY: A threat is any potential danger that could exploit a vulnerability to harm an asset. A vulnerability is a weakness or gap in protection efforts. Risk exists at the intersection of threat, vulnerability, and asset value: Risk = Threat × Vulnerability × Asset Value.

33 **Answer: D** Which of the following actions would be considered a violation of 'due diligence'?

WHY: Due diligence requires research, investigation, and ongoing assessment — understanding threats, evaluating vendors, verifying claims. Accepting vendor claims without verification and failing to research threats both constitute failure of due diligence. Due care is the implementation; due diligence is the investigation that informs it.

34 **Answer: B** Job rotation is PRIMARILY implemented to address which security concern?

WHY: Job rotation serves as a detective control against fraud and collusion. When employees rotate roles, any irregularities or unauthorized activities by the previous occupant are more likely to be discovered. It also prevents over-reliance on a single employee who might become a single point of failure.

35 **Answer: B** According to the (ISC)² Code of Ethics, what is the FIRST canon a member must uphold?

WHY: The ISC2 Code of Ethics canons in order: (1) Protect society, the common good, public trust, and infrastructure. (2) Act honorably, honestly, justly, responsibly, and legally. (3) Provide diligent and competent service to principals. (4) Advance and protect the profession. Society comes first.

36 **Answer: B** What is the primary difference between a Recovery Time Objective (RTO) and a Recovery Point Objective (RPO)?

WHY: RTO: how long can we be without this system? (time to recover). RPO: how much data can we afford to lose? (acceptable backup age). Example: RTO=4 hours means we must restore within 4 hours. RPO=1 hour means backups must be taken at least hourly. Both are outputs of the BIA.

37 **Answer: B** Which of the following is an example of 'regulatory compliance' driving security requirements?

WHY: Regulatory compliance means implementing controls because a law or regulation mandates them. HIPAA mandates access controls for PHI — the healthcare provider has no choice. The other options are driven by business judgment, threat intelligence, or customer expectations — not regulatory mandate.

38 **Answer: B** What does 'operational security (OPSEC)' primarily focus on?

WHY: OPSEC is a process that identifies critical information that might be observed and exploited by an adversary, then implements countermeasures. Originally a military concept, it protects the 'pieces of the puzzle' that, when combined, could reveal sensitive plans, capabilities, or intentions.

39 **Answer: C** A company stores credit card data. Which compliance standard is MOST applicable?

WHY: PCI DSS (Payment Card Industry Data Security Standard) applies to any organization that stores, processes, or transmits payment card data. It is a contractual standard set by card brands (Visa, Mastercard, etc.), not a government regulation, but non-compliance results in fines and loss of card processing privileges.

40 **Answer: A** What is 'aggregation' in the context of information security?

WHY: Aggregation is a security threat where combining multiple pieces of individually non-sensitive information creates a sensitive disclosure. Example: name + employer + neighborhood + physical description + daily schedule individually may be public, but combined creates a privacy risk enabling stalking or targeting.

41 **Answer: C** When should a penetration test authorization be obtained?

WHY: Written authorization must be obtained before any penetration testing begins. Without authorization, even well-intentioned testing is unauthorized access — a criminal offense. The authorization (Rules of Engagement) should define scope, permitted techniques, escalation procedures, and the contact person.

42 **Answer: B** Which of the following BEST describes 'social engineering' as a security threat?

WHY: Social engineering exploits human nature — trust, helpfulness, authority, fear, urgency — rather than technical vulnerabilities. It is often the easiest attack path because humans are typically the weakest security link. Awareness training is the primary countermeasure.

43 **Answer: B** What is the PRIMARY output of a risk assessment?

WHY: A risk assessment identifies, analyzes, and evaluates risks — producing a prioritized list with likelihood and impact assessments. The output informs risk treatment decisions and control selection. It does not itself prescribe controls; that is the risk treatment/response phase.

44 **Answer: B** An employee's background check reveals a prior conviction for financial fraud. They are being considered for a role...

WHY: Employment decisions based on criminal history must comply with applicable law (which varies by jurisdiction) and consider the relevance and recency of the offense to the role. Blanket rejection policies may be discriminatory and illegal. The decision should be role-specific and legally reviewed, not automatic.

45 **Answer: C** Which of the following is NOT typically included in a security policy?

WHY: Security policies contain high-level management intent, scope, roles, and enforcement statements. Step-by-step technical configurations belong in procedures or standards — not policies. Policies must be stable over time; technical specifics change frequently and should be maintained separately.

46 **Answer: C** What is the Annualized Rate of Occurrence (ARO) if a threat is expected to occur once every five years?

WHY: $ARO = 1 / \text{number of years between occurrences} = 1/5 = 0.2$. An ARO of 0.2 means there is a 20% probability the event will occur in any given year, or equivalently, once every five years on average.

47 **Answer: B** Which of the following is the BEST definition of 'information security governance'?

WHY: Information security governance is the oversight responsibility of the board and executive management — setting direction, allocating resources, managing risk, and measuring performance. It is distinct from security management (operational) and security administration (technical implementation).

48 **Answer: B** A security team is evaluating whether to adopt ISO 27001 or NIST CSF. What is the PRIMARY distinguishing factor to ...

WHY: ISO 27001 is a certifiable standard — organizations can achieve formal third-party certification after an accredited audit. NIST CSF is a voluntary reference framework with no formal certification body. ISO 27001 certification can be required by contracts or regulators; NIST CSF adoption is self-assessed.

49 **Answer: B** What is the purpose of a 'data retention policy'?

WHY: A data retention policy defines the minimum and maximum periods for keeping different types of data, the storage requirements, and the destruction method when retention ends. It is driven by legal requirements, business needs, and privacy considerations. Retaining data longer than necessary increases risk and storage costs.

50 **Answer: B** Which of the following BEST describes 'privacy' as distinct from 'confidentiality' in information security?

WHY: Confidentiality protects data from unauthorized disclosure — it is about the data itself. Privacy is a broader concept — an individual's right to control what information about them is collected, used, and shared. You can maintain confidentiality without respecting privacy (e.g., keeping data secret but using it in ways the person didn't consent to).

READY FOR THE FULL CISSP?

Upgrade to the Threatnexus CISSP Premium Test Bank for complete exam coverage.

FEATURE	FREE EDITION	PREMIUM EDITION
Questions	50	300
Domain Coverage	1 Domain	All 8 Domains
Explanations	Standard	Advanced + Distractor Analysis
Scenario Questions	—	Included
Quick Reference Sheet	—	Formulas, Models, Crypto
Format	PDF	PDF (Print-Ready)

threatnexus.com

Visit to unlock the CISSP Premium Test Bank

© 2025 Threatnexus. All rights reserved. This document is licensed for individual personal exam preparation use only. Reproduction, redistribution, or commercial use is prohibited.