PRELIM REVIEWER (MODULE 1-4) IT 3217

Main goal of a SETA program: Protect information assets.
Long-term security learning: Security education.
Security awareness mainly targets: Daily behavior.
Short, simple, repeated reminders: Security awareness.
Security training focuses on: Practical skills.
Example of security awareness activity: Poster about phishing.
Who should be covered by SETA: All employees.
A semester-long security course: Security education.
Importance of SETA: Reduce human risks.
Who needs deeper security education: Security/IT staff.
Goal of contingency planning: Keep systems available.
First step in contingency planning: Risk assessment.
Who manages incident response and recovery: CPMT (Contingency Planning Management Team).
SDLC phase that finds requirements: Analysis.
Why add continuity in SDLC design: Build resilience in systems.
SDLC phase that installs the system: Implementation.
Study of critical processes and impact of downtime: Business impact analysis.
Why test the contingency plan often: Prove it works and find weaknesses.
What supports continuity: Offsite backups.
SDLC phase that applies fixes and patches: Maintenance.
Comparing your security to standards and peers: Benchmarking.
Main benefit of benchmarking: Find gaps and improve.
Most important for an online store: Protect customer data.
HTTPS with valid certificates gives: Strong encryption and checks.
Ten Immutable Laws focus on: People and basic security truths.
Fixed minimum set of controls: Baselining.
Why use a baseline: Easier to see abnormal activity.
Good security position in organization should: Support business goals.
All staff sign rules for system use: Acceptable use policy.
Future security analyst needs: Skills, ethics, and growth.
Original readable message: Plaintext.
Encrypted unreadable data: Ciphertext.
Controls encryption and decryption: Cryptographic key.
One secret key for both encrypt and decrypt: Symmetric encryption.
Public key encrypts and private key decrypts: Asymmetric encryption.
Encrypts data byte by byte: Stream cipher.
Encrypts data in fixed blocks: Block cipher.
Fixed-length value to check changes: Hash function.
Attacker between two parties altering traffic: Man-in-the-middle attack.
Using common words to guess passwords: Dictionary attack.

SETA program helps reduce user-related security risks in an organization. (True)
Security awareness is usually short and simple, not long highly technical courses. (False)
Security training should give users hands-on experience with secure behavior. (True)
Security education is more formal and long-term than training. (True)
Posters and short videos are common tools for security awareness. (True)
Only IT staff need to be included in SETA. (False)
A strong SETA program supports the organization’s security policies. (True)
An employee who understands phishing is less likely to click a malicious link. (True)
Security awareness should be repeated regularly, not just once. (True)
SETA programs have no connection to ethical and legal responsibilities. (False)
Contingency planning helps maintain critical services during disruptions. (True)
The CPMT is responsible only for marketing activities. (False)
A contingency planning timeline includes assessment, strategy, testing, maintenance. (True)
Integrating continuity into the SDLC is unnecessary. (False)
The analysis phase of the SDLC focuses on understanding system requirements. (True)
Offsite backups support business continuity when the main site is damaged. (True)
Testing contingency plans helps reveal weaknesses before real incidents. (True)
The maintenance phase includes applying patches and improvements. (True)
Contingency planning is only useful for natural disasters. (False)
CPMT members should understand both business needs and technical issues. (True)
Benchmarking compares your security to standards or others. (True)
Baselining sets minimum controls. (True)

An online store can ignore customer data. (False)
The Ten Immutable Laws show how users can weaken security. (True)
A baseline helps detect unusual activity. (True)
Policies may include background checks and use rules. (True)
Security staff placement should support business goals. (True)
Security pros do not need lifelong learning. (False)
Benchmarking can show weak areas. (True)
Good security work needs skill and ethics. (True)
Plaintext is readable data before encryption. (True)
Ciphertext is decrypted data. (False)
Symmetric uses the same key for both directions. (True)
Asymmetric uses a public and a private key. (True)
Hash functions are easy to reverse. (False)
Stream ciphers work bit or byte at a time. (True)
Block ciphers work on fixed-size chunks. (True)
Man-in-the-middle can change messages. (True)
Dictionary attacks use common words for guessing. (True)
Ethical cryptography respects privacy and law. (True)

Matching Type:
Short reminders about risks → Security awareness.
Combined education, training, awareness → SETA program.
Long-term security learning → Security education.
Practical skill exercises → Security training.
Rules for system use → Policy.
Daily actions of people → User behavior.
Fake message to steal data → Phishing.
Shared security values and habits → Security culture.
Written record of a security event → Incident report.
Rules about creating and using passwords → Password policy.
Check threats and vulnerabilities → Risk assessment.
Team for planning, response, recovery → CPMT.
Steps for handling disruptions → Contingency plan.
Study of effects of interruptions → Business impact analysis.
Deploy system to users → Implementation phase.
Life cycle of a system → SDLC.
Storage at another site → Offsite backup.
Target time to restore a service → Recovery time objective.
Extra server ready to take over → Redundant server.
Phase for updates and fixes → Maintenance phase.
Compare to standards or other orgs → Benchmarking.
Recommended way to do a task → Best practice.
Minimum security settings → Baselining.
Site for orders and payment → Online trade website.
Basic security truths and warnings → Ten Immutable Laws of Security.
Rules for system and network use → Acceptable use policy.
Review of history before hiring → Background check.
Person leading security efforts → Security officer.
Give only needed access rights → Least privilege.
Split tasks between different people → Separation of duties.
Original readable data → Plaintext.
Encrypted data → Ciphertext.
Value for encryption/decryption → Key.
Same key for both directions → Symmetric encryption.
Public and private key pair → Asymmetric encryption.
Encrypts data bit by bit/byte by byte → Stream cipher.
Encrypts data in blocks → Block cipher.
Gives fixed-length output → Hash function.
Attacker between two parties → Man-in-the-middle attack.
Tries common words as passwords → Dictionary attack.