Module 4 – Final Quiz: Risk Management and Security Policies

1 - What does “cybersecurity risk” mean?

A) Any situation that improves system performance
B) The potential for loss or damage due to threats exploiting vulnerabilities
C) A scheduled software patch
D) A backup plan for data

2 - Which best describes the difference between a threat and a vulnerability?

A) A threat is a weakness; a vulnerability is an external danger
B) A threat is an external danger; a vulnerability is an internal weakness
C) Both terms mean the same thing
D) A vulnerability always prevents risk

3 - Which formula best captures the concept of risk?

A) Risk = Vulnerability × System Speed
B) Risk = Threat × Vulnerability × Impact
C) Risk = Encryption ÷ Likelihood
D) Risk = Control × Awareness

4 - Why does risk management matter in cybersecurity?

A) It makes systems run faster
B) It ensures risks are identified, prioritized, and mitigated before damage occurs
C) It replaces the need for antivirus software
D) It guarantees 100% security

5 - Which method focuses on measuring likelihood and impact with numbers and costs?

A) Qualitative risk assessment
B) Quantitative risk assessment
C) Threat modeling only
D) Subjective analysis

6 - Which is an example of a qualitative risk assessment?

A) Estimating downtime in dollars per hour
B) Ranking risks as “High, Medium, Low”
C) Calculating annualized loss expectancy (ALE)
D) Performing a cost-benefit analysis

7 - Which of the following is a risk assessment framework?

A) TCP/IP model
B) NIST RMF
C) WPA3 standard
D) RAID levels

8 - Which of these is NOT a type of security control?

A) Preventive
B) Detective
C) Corrective
D) Expansive

9 - Which example best represents a preventive control?

A) Installing a firewall to block malicious traffic
B) Using intrusion detection logs
C) Restoring data from backups
D) Reviewing security audit reports

10 - Which control type includes intrusion detection systems (IDS)?

A) Preventive
B) Detective
C) Corrective
D) Administrative

11 - What is a security policy?

A) A set of guidelines defining acceptable use, responsibilities, and protections
B) A technical control that encrypts traffic
C) A hardware-based access rule
D) A temporary workaround during an incident

12 - Who is typically responsible for security governance?

A) Only end-users
B) Senior management and designated governance bodies
C) Technical support teams only
D) Third-party contractors

13 - Which is NOT part of the security policy lifecycle?

A) Drafting
B) Enforcement
C) Archiving without updates
D) Review and revision

14 - Why are security awareness programs important?

A) Technology alone cannot address human error
B) They eliminate all phishing attacks
C) They guarantee compliance automatically
D) They are optional and rarely effective

15 - Which is an example of a training method for awareness programs?

A) Simulated phishing exercises
B) Installing stronger firewalls
C) Updating OS patches
D) Encrypting emails

Lab 4.1 – Building a Risk Register

16 - What is a risk register?

A) A log of firewall rules
B) A structured document tracking risks, likelihood, and impact
C) A backup storage system
D) An antivirus database

17 - Which of the following is a core column in a risk register?

A) Risk description, likelihood, impact, controls
B) Employee satisfaction, cost savings, productivity
C) Font size, table style, formatting rules
D) Server uptime percentage only

18 - In the example risk entry, “phishing email,” what makes this a valid risk register item?

A) It only tracks cost
B) It links a threat (phishing) to vulnerabilities and possible impacts
C) It only lists the likelihood
D) It ignores human factors

19 - Why does scoring risk help?

A) It replaces the need for policies
B) It prioritizes which risks need urgent action
C) It makes risk management optional
D) It eliminates vulnerabilities automatically

20 - Which of the following is a strategic use of a risk register?

A) Prioritizing risks for leadership and tracking changes over time
B) Encrypting sensitive files
C) Monitoring CPU performance
D) Training only system administrators

Answer Key

1. **B** – Cyber risk = potential for harm when threats exploit vulnerabilities.
2. **B** – Threat = danger; vulnerability = weakness exploited.
3. **B** – Standard definition of risk in cybersecurity.
4. **B** – Goal is prioritizing/mitigating risks before incidents.
5. **B** – Quantitative uses measurable numbers, costs.
6. **B** – Qualitative uses relative scales (e.g., High/Medium/Low).
7. **B** – NIST RMF is a risk management framework.
8. **D** – Expansive is not a control category.
9. **A** – Firewalls are preventive.
10. **B** – IDS = detective control.
11. **A** – Policies = written rules and expectations.
12. **B** – Governance is a senior management responsibility.
13. **C** – Archiving without updates is not part of lifecycle.
14. **A** – People are the first line; awareness reduces human error.
15. **A** – Simulated phishing is a classic training method.
16. **B** – Risk register = structured tracking of risks.
17. **A** – Risk description, likelihood, impact, controls are core fields.
18. **B** – Example ties phishing threat to vulnerabilities/impact.
19. **B** – Scoring helps rank/prioritize risks.
20. **A** – Register is used strategically for prioritization & reporting.