# Information Security and Risk Management

1. Within the realm of IT security, which of the following combinations best defines risk?
   1. Threat coupled with a breach of security
   2. Threat coupled with a vulnerability
   3. Vulnerability coupled with an attack
   4. Threat coupled with a breach
2. Which of the following should be given technical security training?
   1. Senior managers, functional managers and business unit managers
   2. Security practitioners and information systems auditors
   3. IT support personnel and system administrators
   4. Operators
3. Preservation of confidentiality information systems requires that the information is not disclosed to:
   1. Authorized persons and processes
   2. Unauthorized persons or processes.
   3. Authorized person
   4. Unauthorized persons.
4. In Risk Modeling the focus is to obtain credible and usable portrayal of risks. Of the following, which is NOT a question used to perform this function?
   1. Is it credible?
   2. How bad would it be?
   3. What could happen?
   4. How often could it occur?
5. In a properly segregated environment, which of the following tasks is compatible with the task of security administrator?
   1. Data entry
   2. Systems programming
   3. Quality assurance
   4. Applications programming
6. Which of the following would be the first step in establishing an information security program?
   1. Development and implementation of an information security standards manual.
   2. Adoption of a corporate information security policy statement.
   3. Purchase of security access control software.
   4. Development of a security awareness-training program for employees.
7. Which choice below represents an application or system demonstrating a need for a high level of confidentiality protection and controls?
   1. Unavailability of the system could result in inability to meet payroll obligations and could cause work stoppage and failure of user organizations to meet critical mission requirements. The system requires 24-hour access.
   2. The application contains proprietary business information and other financial information, which if disclosed to unauthorized sources, could cause an unfair advantage for vendors, contractors, or individuals and could result in financial loss or adverse legal action to user organizations.
   3. Destruction of the information would require significant expenditures of time and effort to replace. Although corrupted information would present an inconvenience to the staff, most information, and all vital information, is backed up by either paper documentation or on disk.
   4. The mission of this system is to produce local weather forecast information that is made available to the news media forecasters and the general public at all times. None of the information requires protection against disclosure.
8. In an organization, an Information Technology security function should:
   1. Be a function within the information systems function of an organization.
   2. Be independent but report to the Information Systems function.
   3. Be lead by a Chief Security Officer and report directly to the CEO.
   4. Report directly to a specialized business unit such as legal, corporate security or insurance.
9. Who should DECIDE how a company should approach security and what security measures should be implemented?
   1. Senior management
   2. Data owner
   3. Auditor
   4. The information security specialist
10. Step-by-step instructions used to satisfy control requirements is called a:
    1. procedure
    2. guideline
    3. standard
    4. policy