قائمة الاسئلة

امتحان نهاية الفصل الدراسي الثاني - للعام الجامعي 1446 هـ - الموافق -2025/2024م-كلية الحاسوب وتكنولوجيا المعلومات :: إدارة امن م

د.عبدالرحمن الصبري

1) Risk Management is commonly understood as all of the following EXCEPT:
   1) - Analyzing and assessing risk
   2) - Identifying risk
   3) - Accepting or mitigation of risk
   4) + Likelihood of a risk occurring
2) Which of the following computer recovery sites is only partially equipped with processing equipment?
   1) - hot site.
   2) - rolling hot site.
   3) + warm site.
   4) - cold site
3) Which of the following recovery plan test results would be most useful to management?
   1) - elapsed time to perform various activities.
   2) - list of successful and unsuccessful activities.
   3) + amount of work completed.
   4) - description of each activity.
4) Which of the following provides enterprise management with a prioritized list of time-critical business processes, and estimates a recovery time objective for each of the time critical processes and the components of the enterprise that support those processes?
   1) + Business Impact Assessment
   2) - Current State Assessment
   3) - Risk Mitigation Assessment.
   4) - Business Risk Assessment
5) Which of the following steps is NOT one of the eight detailed steps of a Business Impact Assessment (BIA):
   1) - Notifying senior management of the start of the assessment.
   2) - Creating data gathering techniques.
   3) - Identifying critical business functions.
   4) + Calculating the risk for each different business function.
6) A site that is owned by the company and mirrors the original production site is referred to as a?
   1) - Hot site.
   2) + Warm Site.
   3) - Reciprocal site.
   4) - Redundant Site.
7) Procedures implemented to define the roles, responsibilities, policies, and administrative functions needed to manage the control environment.
   1) - Integrity
   2) - Risk transfer
   3) - Compensating controls
   4) + Administrative controls
8) The percentage or degree of damage inflicted on an asset used in the calculation of single loss expectancy can be referred to as:
   1) + Exposure Factor (EF)
   2) - Annualized Rate of Occurrence (ARO)
   3) - Vulnerability
   4) - Likelihood
9) The absence of a fire-suppression system would be best characterized as a(n):

1) - Exposure

2) - Threat

3) + Vulnerability

4) - Risk

10) Risk Assessment includes all of the following EXCEPT:

1) + Implementation of effective countermeasures

2) - Ensuring that risk is managed

3) - Analysis of the current state of security in the target environment

4) - Strategic analysis of risk

11) What is the most common planned performance duration for a continuity of operations plan (COOP)

1) + 30 days

2) - 60 days

3) - 90 days

4) - It depends on the severity of a disaster

12) It is recommended that your disaster recovery plan (DRP) and business continuity plan (BCP) be tested at a minimum of what intervals?

1) - Six months

2) - When the systems and environment change

3) - Two years

4) + One year

13) Which of the following strategies used to minimize the effects of a disruptive eventon a company and is createdto preventinterruptions to normalbusiness activity

1) - Disaster Recovery Plan

2) + Business continuity plan

3) - continuity of operations plan

4) - coningency plan

14) What is the difference between quantitative and qualitative risk analysis?

1) - Qualitative analysis uses mathematical formulas and while quantitative analysis does not.

2) - Purely qualitative analysis is not possible, while purely quantitative is possible.

3) + Quantitative analysis provides formal cost/benefit information while qualitative analysis does not.

4) - There is no difference between qualitative and quantitative analysis.

15) If risk is defined as “the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets” the risk has all of the following elements except?

1) - An impact of assets based on threats and vulnerabilities.

2) + Controls addressing the threats.

3) - Threats to and vulnerabilities of processes and/or assets.

4) - Probabilities of the threats.

16) Risk analysis allows you to do all of the following except:

1) - Quantify the impact of potential risks

2) - Create an economic balance between the impact of a risk and the cost of a countermeasure

3) - Provides a cost/benefit comparison

4) + Prevent risk

17) Which choice below is an accurate statement about standards?

1) - Standards are the high-level statements made by senior management in support of information systems security.

2) - Standards are the first element created in an effective security policy program.

3) + Standards are used to describe how policies will be implemented within an organization.

4) - Standards are senior management’s directives to create a computer security program

18) What should take place in order to restore a server, its files and data after a major system failure?
    1) + Restore from storage media backup
    2) - Perform a parallel test
    3) - Implement recovery procedures
    4) - Perform a check list test
19) What is the most critical factor in the development of a disaster recovery plan (DRP)?
    1) + Business impact analysis (BIA)
    2) - Annual testing
    3) - Participation from every department
    4) - Management support
20) Which of the following backup facility is most expensive?
    1) - Cold
    2) + Hot
    3) - Warm
    4) - Mobile
21) Which of the following BEST describes the fundamental purpose of an organization's security governance?
    1) - Implementing security technology
    2) - Compliance with legal regulations
    3) - Ensuring a secure organizational culture
    4) + Aligning security with business objectives
22) ISO/IEC 27001 is primarily concerned with what aspect of information security management?
    1) + Risk Management
    2) - Compliance Monitoring
    3) - Software Development
    4) - Physical Security
23) How does the application of a balanced scorecard benefit an organization’s security governance?
    1) - It ensures total regulatory compliance
    2) - It measures financial performance only
    3) + It balances security controls with business goals
    4) - It focuses exclusively on technological improvements
24) Your organization is evaluating the financial impact of a potential data breach. The asset value is $500,000, and the Exposure Factor (EF) is 60%. What is the Single Loss Expectancy (SLE)?
    1) - $30,000
    2) - $60,000
    3) + $300,000
    4) - $500,000
25) What is one of the first steps in developing a business continuity plan?
    1) - Identify a backup solution.
    2) - Perform a simulation test.
    3) + Perform a business impact analysis.
    4) - Develop a business resumption plan.
26) Which best describes a hot-site facility versus a warm- or cold-site facility?
    1) - A site that has disk drives, controllers, and tape drives
    2) + A site that has all necessary PCs, servers, and telecommunications
    3) - A site that has wiring, central air-conditioning, and raised flooring
    4) - A mobile site that can be brought to the company's parking lot
27) Which areas of a company are recovery plans recommended for?
    1) - The most important operational and financial areas
    2) - The areas that house the critical systems

3) + All areas

4) - The areas that the company cannot survive without

28) Business impact analysis is performed to identify:

1) - The impacts of a threat to business operations.

2) + The exposures to loss to the organization.

3) - The impacts of a risk on the company.

4) - The way to eliminate threats.

29) A business continuity plan should be updated and maintained:

1) - Immediately following an exercise.

2) - Bollowing a major change in personnel.

3) - After installing new software.

4) + All of the mentioned

30) An acceptable length of time a business function or process can be unavailable is known as_____.

1) - Recovery time objective (RTO)

2) - Maximum unavailability (MU)

3) - Total acceptable time (TAT)

4) + Maximum tolerable downtime (MTD)

31) Recovery Controls: Controls implemented to restore conditions to normal after a security incident.

1) + TRUE.

2) - FALSE.

32) Risk Management: The practice of passing on the risk in question to another entity, such as an insurance company.

1) - TRUE.

2) + FALSE.

33) COBIT is a framework aimed at documenting Organizational IT Security.

1) + TRUE.

2) - FALSE.

34) Guidelines is one of the policy hierarchies but not mandatory

1) + TRUE.

2) - FALSE.

35) The right time to develop an Incident Response plan is after an incident occurs.

1) - TRUE.

2) + FALSE.

36) Once policies are created, they should not be changed.

1) - TRUE.

2) + FALSE.

37) For policies to be effective, they must first be developed using generally-accepted practices.

1) + TRUE.

2) - FALSE.

38) An issue-specific security policy sets the strategic direction, scope, and tone for all of an organization's security efforts.

1) - TRUE.

2) + FALSE.

39) Policies comprise a set of rules that dictates acceptable and unacceptable behavior within an organization.

1) + TRUE.

2) - FALSE.

40) During the implementation phase of the policy development SecSDLC, the development team creating the information security policy should make sure that the policy is written at a reasonable reading level.

1) + TRUE.

2) - FALSE.