COLLEGE OF ENGINEERING AND APPLIED SCIENCES

NCIS309-INFORMATION SYSTEMS AUDIT AND CONTROL

END OF FIRST SEMESTER EXAMINATIONS

NOVEMBER 2024

LECTURER: MRS L FUNDISI

DURATION: 3 HOURS

INSTRUCTIONS

Section A: **compulsory, answer all**

Section B: Answer any 4 (four) questions

All question carries equal marks (20)

Begin your answer to each question on a fresh page

Logical answering, smartness and use of examples will earns more marks

Section A

1. **An audit charter should:**
A. be dynamic and change often to coincide with the changing nature of technology and the audit profession.
B. clearly state audit objectives for, and the delegation of, authority to the maintenance and review of internal   controls.
C. document the audit procedures designed to achieve the planned audit objectives.
D. outline the overall authority, scope and responsibilities of the audit function.

2. **In an Organization Audit charter is approved by**
A. Board of directors or Audit Committee.
B. Board of directors or Senior Management.
C. Board of directors and Audit Committee.
D. Senior Management and Audit Committee.

3. **Which of the following is the MOST critical step to perform when planning an IS audit?**
A. Review findings from prior audits.
B. Develop plans to conduct a physical security review of the data center facility.
C. Review IS security policies and procedures.
D. Perform a risk assessment.

4. **During the planning stage of an IS audit, the PRIMARY goal of an IS auditor is to:**
A. address audit objectives.
B. collect sufficient evidence
C. specify appropriate tests.
D. minimize audit resources.

5. **While planning an audit, an assessment of risk should be made to provide:**
A. reasonable assurance that the audit will cover material items.
B. definite assurance that material items will be covered during the audit work.
C. reasonable assurance that all items will be covered by the audit.
D. sufficient assurance that all items will be covered during the audit work

6. **Which of the following is the FIRST step performed prior to creating a risk ranking for the annual internal IS audit   plan?**
A. Prioritize the identified risk.
B. Define the audit universe.
C. Identify the critical controls.
D. Determine the testing approach

7. **The knowledge base of an expert system that uses questionnaires to lead the user through a series of choices before a conclusion is reached is known as:**
A. Rules

B. Semantic nets
C. Decision trees
D. Dataflow diagram

8. Value delivery from IT to the business is MOST effectively achieved by:
A. Aligning the IT strategy with the enterprise strategy
B. Embedding accountability in the enterprise.
C. Providing a positive return on investment.
D. Establishing an enterprise wide risk management process.

9. Involvement of senior management is MOST important in the development of:
A. Strategic plans.
B. IT policies.
C. IT procedures.
D. Standards and guidelines.

10. Effective IT governance will ensure that the IT plan is consistent with the organization's:
A. business plan.
B. audit plan.
C. security plan.
D. investment plan.

11. Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?
A. System owners
B. System users
C. System designers
D. System builders

12. Which of the following is the MOST efficient way to test the design effectiveness of a change control process?
A. Test a sample population of change requests
B. Test a sample of authorized changes
C. Interview personnel in charge of the change control process
D. Perform an end-to-end walk-through of the process

13. Which of the following is the MOST important requirement for a robust change management process?
A. Chain of custody
B. Individual accountability
C. Data entry controls
D. Segregation of duties

14. Which of the following is MOST important to ensure business continuity?
A. Current contact information for key employees
B. Backup data
C. Access to funds for short-term needs

D. Alternate processing site

15. **Which of the following would have the HIGHEST priority in a business continuity plan (BCP)?**
A. Resuming critical processes
B. Recovering sensitive processes
C. Restoring the site
D. Relocating operations to an alternative site

16. **A hot site should be implemented as a recovery strategy when the:**
A. disaster tolerance is low.
B. recovery point objective (RPO) is high.
C. recovery time objective (RTO) is high.
D. disaster tolerance is high

17. **Which of the following risks represents a process failure to detect a serious error?**
A. Detective risk
B. Inherent risk
C. Sampling risk
D. Control risk

18. **The first step in the planning phase of an audit is:**
   A. Designing an audit program
   B. The allocation of audit resources
   C. Identification of key stakeholders
   D. Conducting a risk assessment

19. **The sampling method to be used when there is indication of fraud is:**
A. Attribute sampling
B. Variable sampling
C. Discovery sampling
D. Stop-or-go sampling

20. **Which sampling method that will be MOST meaningful for compliance testing?**
A. Attribute sampling
B. Variable sampling
C. Discovery sampling
D. Stop-or-go sampling

Section B
Question One
What is *risk management*, discuss the importance of risk assessment in the context of information systems auditing. [20]

Question Two

Describe the key components of an information systems audit process. What are the main stages involved in conducting an audit of information systems? [20]

Question Three

What are the typical functions and responsibilities of an IT steering committee, and how does it contribute to decision-making related to IT investments and priorities? [20]

Question Four

Briefly explain the following controls using examples: Preventive, Detective, Deterrent, Corrective

[20]

Question Five

Define the term "*business continuity planning*" and explain its relevance to ensuring business resilience in the face of disruptions. [20]

Question Six

Discuss the concept of "*change management*" in information systems operations. Why is change management important for controlling and managing changes to IT systems and infrastructure

[20]

Question Seven

Discuss the significance of security awareness and training programs in promoting a culture of security within an organization. How can organizations educate employees about security best practices to reduce the risk of security incidents? [20]

END OF EXAMINATION