JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY
UNIVERSITY EXAMINATION 2012/2013

2ND YEAR 1ST SEMESTER EXAMINATION FOR THE DEGREE

OF MSC IN IT SECURITY AND AUDIT

KISUMU LEARNING CENTRE

COURSE CODE: IIT 5212

TITLE: ADVANCE INFO AUDIT & CONTROL

DATE: 16/4/2013 TIME: 9.00-12.00NOON

DURATION: 3 HOURS

INSTRUCTIONS

1. **This paper contains TWO sections**
2. **Answer ALL questions in section A (Compulsory) and ANY other 2 Questions in section B**
3. **Write all answers in the booklet provided**

SECTION B: ANSWER <u>ANY TWO</u> QUESTIONS

SECTION A

Q1. Mixed True/False, Fill-in and Multiple Choice (1 Mark Each)

1. Which of the following provides the strongest authentication for physical access control?

   A. Sign-in logs
   B. Dynamic passwords
   C. Key verification
   D. Biometrics

2. What is an effective countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off?

   Choose the BEST answer.
   A. Employee security awareness training
   B. Administrator alerts
   C. Screensaver passwords
   D. Close supervision

3. Who is ultimately accountable for the development of an IS security policy?

   A. The board of directors
   B. Middle management
   C. Security administrators
   D. Network administrators

4. If senior management is not committed to strategic planning, how likely is it that a company's implementation of IT will be successful?

   A. IT cannot be implemented if senior management is not committed to strategic planning.
   B. More likely.
   C. Less likely.
   D. Strategic planning does not affect the success of a company's implementation of IT.

5. Which of the following are effective controls for detecting duplicate transactions such as payments made or received?

   A. Concurrency controls
   B. Reasonableness checks
   C. Time stamps

D. Referential integrity controls

6. Which of the following is a guiding best practice for implementing logical access controls?

A. Implementing the Biba Integrity Model
B. Access is granted on a least-privilege basis, per the organization's data owners
C. Implementing the Take-Grant access control model
D. Classifying data according to the subject's requirements

7. Why would an information security policy require that communications test equipment be controlled?
A. The equipment is susceptible to damage
B. The equipment can be used to browse information passing on a network
C. The equipment must always be available for replacement if necessary
D. The equipment can be used to reconfigure the network multiplexers

8. Which of the following would provide the highest degree of server access control?

A. A mantrap-monitored entryway to the server room
B. Host-based intrusion detection combined with CCTV
C. Network-based intrusion detection
D. A fingerprint scanner facilitating biometric access control

9. Step-by-step instructions used to satisfy control requirements is called a
A. policy
B. standard
C. guideline
D. procedure

10. The preliminary steps to security planning include all of the following EXCEPT
A. establish objectives.
B. list planning assumptions.
C. establish a security audit function.
D. determine alternate courses of action

11. What physical characteristics does a retinal scan biometric device measure?
A. The amount of light reaching the retina.
B. The amount of light reflected by the retina.
C. The size, curvature, and shape of the retina.
D. The pattern of blood vessels at the back of the eye.

12. Which of the following could lead to an unintentional loss of confidentiality?

Choose the BEST answer.

A. Lack of employee awareness of a company's information security policy

B. Failure to comply with a company's information security policy
C. A momentary lapse of reason
D. Lack of security policy enforcement procedures

13. What are used as the framework for developing logical access controls?

A. Information systems security policies
B. Organizational security policies
C. Access Control Lists (ACL)
D. Organizational charts for identifying roles and responsibilities

14. One purpose of a security awareness program is to modify
A. Employee’s attitudes and behaviors.
B. Management’s approach.
C. Attitudes of employees with sensitive data.
D. Corporate attitudes about safeguarding data.

15. Which of the following measures would be the BEST deterrent to the theft of corporate information from a laptop which was left in a hotel room?
A. Store all data on disks and lock them in an in room safe.
B. Remove the batteries and power supply from the laptop and store them separately from the computer.
C. Install a cable lock on the laptop when it is unattended.
D. Encrypt the data on the hard drive.

16. Which one of the following individuals has PRIMARY responsibility for determining the classification level of information?
A. Security manager
B. User
C. Owner
D. Auditor

17. The Internet Activities Board characterizes which of the following as unethical behavior for Internet users?
A. Writing computer viruses.
B. Monitoring data traffic.
C. Wasting computer resources.
D. Concealing unauthorized accesses.

18. Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. True or false?

A. True
B. False

19. An example of a(n) _____ is a software defect in an operating system that allows an unauthorized user to gain access to a computer without a password

A. vulnerability
B. threat
C. threat agent
D. asset exploit (AE)

20. The _____ is primarily responsible for assessment, management, and implementation of security.

A. Chief Information Security Officer (CISO)
B. security manager
C. security administrator
D. security technician

SECTION B

Q2.

a) In information security audit and control – what do you understand by term audit standards? **(4 Marks)**

b) In information security audit and control what role does SAS 70 audits play? List some of the common terminology used with SAS 70. **(10 Marks)**

c) Under SAS 70 auditing, differentiate between Type I and Type II audits? **(3 Marks)**

d) What are pros and con about SAS 70 auditing? **(3 Marks)**

Q3

a) In IT security and audit why is COSO Framework important? **(3 Marks)**

b) In IT security and audit why is COBIT important? **(6 Marks)**

c) In IT security and audit why is it important that you perform IT testing? **(6 Marks)**

d) In IT security and audit why does auditing and certification go hand-in-hand? **(5 Marks)**

Q4.

a) In IT security and audit what do you understand by term Risk Framework? **(8 Marks)**

b) Which areas do Technical Frameworks for IT Audits covers? **(12 Marks)**

Q5.

a) Define internal audit. **(4 Marks)**

b) Briefly explain what is an IT Audit Role? **(6 Marks)**

c) How would you undertake IT Audit Process **(6 Marks)**

d) What do you need to do to prepare for an IT Audit? **(4 Marks)**

Q6.

a) What do you understand by term IT control? **(2 Marks)**

b) What is the importance of IT control? **(4 Marks)**

c) Under IT control how are roles and responsibilities apportioned? **(3 Marks)**

d) Under IT controls briefly explain the following: **(5 Marks)**

e) As an IT Audit specialist, how can you determine if the Internal Controls in your area are adequate? **(6 Marks)**