UNIVERSITI UTARA MALAYSIA

FINAL EXAM
INTERSESSION SEMESTER 2005/2006

CODE/COURSE NAME: KAS5033 – INFORMATION SYSTEMS CONTROL AND AUDIT
DATE: 5 JULY 2006
TIME: 9.00AM – 12.00PM (3 HOURS)
VENUE: FPK413

INSTRUCTION:
1. This book script contains TWO (2) sections and THIRTY TWO (32) questions in EIGHT (8) printed pages.
2. Answer ALL the questions.

For internal use only:
Section A
Section B
Total

MATRIK NO: ____________________________  (in word)  (in number)
IC/PASSPORT NO: ________________________
INSTRUCTOR NAME: ______________________
GROUP: _______  DESK NO: _______

PLEASE DO NOT OPEN THIS EXAM BOOK
UNTIL YOU ARE TOLD TO DO SO

Private & Confidential
SECTION A (40 Marks)

1. Which of the following would NOT be a use of generalized software programs?
   A. Verifying calculations and totals
   B. Performing intricate calculations
   C. Selecting data that an auditor defines as unusual
   D. Producing multiple reports and machine-readable output files

2. The risk that an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when, in fact, they do, is an example of:
   A. Inherent Risk
   B. Control Risk
   C. Detection Risk
   D. Audit Risk

3. Which of the following would NOT be considered a security threat to Internet web sites?
   A. Hackers
   B. Crackers
   C. Virus writers
   D. Asynchronous attacks

4. Which of the following would NOT protect a system from computer viruses?
   A. Write-protect all diskettes, once they have been virus-checked.
   B. Scan any new software before it is installed.
   C. Boot only from diskettes that were initially checked for viruses.
   D. Do not allow vendors to run demonstration on company owned machines.

5. Anti-virus software should be used as a:
   A. Detective control.
   B. Preventive control.
   C. Corrective control.
   D. Compensating control.

6. Which of the following should be considered the BEST example of a proper password for use in system access?
   A. XWA3
   B. LARRY2
   C. TWC2H
   D. TYRC45OPB

7. Automated Teller Machines (ATMs) are specialized form of point of sale terminal which:
   A. Allow cash withdrawal and financial deposits only.
   B. Are usually located in populous areas to deter theft or vandalism.
   C. Utilize protected telecommunications lines for data transmissions.
   D. Must provide high levels of logical and physical security.
8. Edit controls are considered to be:
   A. Detective control.
   B. Preventive control.
   C. Corrective control.
   D. Compensating control.

9. Software that maintains audit trails for an application system may pose control concerns if:
   A. User-ids are recorded in audit trail.
   B. The details cannot be amended by the security administrator.
   C. Date time stamps are recorded indicating when actions occurred.
   D. Users can amend audit trail records when correcting systems errors.

10. Disaster recovery planning for a company's computer system usually focuses on:
    A. Operations turnover procedures.
    B. Strategic long-range planning.
    C. The probability that a disaster will occur.
    D. Alternative procedures to process transactions.

11. Which of the following processes would be performed FIRST by the system when logging-on to an on-line system?
    A. Initiation.
    B. Verification.
    C. Authorization.
    D. Authentication.

12. In which of the following phases of the system development life cycle of a new application system is it the MOST important for the IS Auditor to participate?
    A. Design.
    B. Testing.
    C. Programming.
    D. Implementation.

13. An IS Auditor performing an audit of the company's information system strategy would be LEAST likely to:
    A. Assess IS security procedures
    B. Review both short and long term IS strategies.
    C. Interview appropriate corporate management personnel.
    D. Ensure that the external environment has been considered.

14. From an IS audit perspective, which of the following is the MOST valuable asset in an information systems facility:
    A. Hardware
    B. Database
    C. Personnel
    D. Software
15. In a computer system, the audit trail is:
   A. Still always present in some type of hard copy form
   B. Disappearing as more on-line, real-time update systems are used
   C. Produced automatically by software during the update process
   D. Sometimes more extensive than the audit trail in manual system if it is designed properly

16. The primary advantage of a derived PIN is:
   A. It is easy to remember
   B. It does not have to be stored so preserving privacy is easier
   C. Lost or forgotten PINs can be replaced without having to change the account number
   D. Changing the cryptographic key has no implications for existing PINs

17. The control information that prevents undetected removal of the last page of the last report is the:
   A. Page number
   B. End-of-job marker
   C. Security classification
   D. Page title

18. Computer abuse is BEST defined as:
   A. Malicious damage carried out to hardware and software
   B. Any incident associated with computer technology whereby a victim suffered loss and perpetrator gained
   C. A fraud perpetrated by modifying software or hardware
   D. Any incident whereby a hacker breaches controls in a computer system and destroys software or data

19. Which of the following would NOT be a reason why an IS Auditor would prepare a formal audit program?
   A. To structure the IS Auditor’s own planning
   B. To guide assistants in performing planned procedures
   C. To provide documentation for review reference
   D. To access the overall risk of operations within the organization

20. Creation of Digital Signature:
   A. Encrypts the message
   B. Verifies where the message came from
   C. Cannot be compromised when using a private key
   D. Cannot be used with e-mail systems
SECTION B (60 Marks)

1. Define IS Audit. (5 Marks)

2. Why controls are still needed to protect hardware, software and personnel, even though substantial insurance coverage might have been taken out by the organizations? (5 Marks)
3. Define the concept of a control.  

4. Why must auditors focus on controls as a system?
5. Discuss how an IT audit is different from a financial statement audit. (5 Marks)

6. Discuss the considerations of a disaster recovery plan. (5 Marks)
7. What are the disadvantages of using electronic working papers? (5 Marks)

8. What are some typical problems with passwords? (5 Marks)

9. Describe the two (2) objectives IT Governance. (5 Marks)
10. Gives five (5) measures of system quality. (5 Marks)

11. Output controls ensure that output is not lost, misdiredcted, or corrupted and that privacy is not violated. What are some output exposures or situations where output is at risk? (5 Marks)

12. Give two (2) ways in which utility software might be used to facilitate auditors' assessment of operational efficiency in an application system. (5 Marks)

- END OF QUESTIONS -