MAKERERE UNIVERSITY BUSINESS SCHOOL
FACULTY OF COMPUTING AND INFORMATICS
DEPARTMENT OF INFORMATION SYSTEMS
ACADEMIC YEAR 2024/25
BACHELOR OF BUSINESS COMPUTING

COURSE OUTLINE

Course Name:	**Information Security and Auditing**
Course Code:	**BUC3126**
Year of study:	**3**
Semester:	**1**
Credit Units:	**4**
Credit Hours:	**60**

FACILITATORS: Dr. Samali V. Mlay, Mr. Samuel Ssendi, Ms. Stella Kyalimpa

Course Description

Information technology (IT) has inspired the reengineering of traditional business operations. As global networks expand the interconnection of the world, the smooth operation of communication and computing systems becomes vital. The immediate need for organizations to protect critical information continues to increase. IT advances have introduced new risks that require unique internal controls and also have had great influences on auditing.

IS Auditing examines information systems in order to provide valuable information about the operations and security of information and information systems. This course will additionally give the learner essential information in order to conduct information systems audits. It exposes the learner to the different IT governance, acquisition reporting and compliance.

Course Objective

The course is intended to achieve the following objectives:

1. To introduce learners to information security practices implemented in IT companies worldwide.
2. To assess information security threats and vulnerabilities faced by organisations.
3. To review requirements of security controls and countermeasures
4. To introduce the learners to IS Audit process, standards and frameworks
5. To take learners through the planning and managing of IS audits
6. Illustrate to learners how to prepare audit reports and communication
7. Explain compliance and ethics in IS auditing.

Learning Outcomes

By the end of the course, students should be able to:

1. Describe information security practices implemented in IT companies.

2. Identify and prioritise information security threats and vulnerabilities faced by organisations.
3. Review requirements of security controls and countermeasures.
4. Describe the IS Audit process, standards and frameworks
5. Plan for and manage IS audits
6. Prepare audit reports and communication
7. Explain compliance and ethics in IS auditing

Detailed Course Content

No	Topic	Lesson Details	Hours
1.	Introduction to Information Security	a) The Information security CIA triangle b) Components of InfoSec c) Controlling IT environment d) Information Security Management System e) Steps for developing ISMS.	6
2	Information security threats, risks and cyber crimes	a) Information security threats b) Information security risks c) Introduction to cyber-crimes and attacks d) Information security measures	6
3	Information Security Policy and Standards	a) Information security principles b) Information security policy, policy definition and information security lifecycle. c) Types of Information security policies d) A structure and framework of compressive security e) Policy, policy infrastructure, policy design lifecycle and design processes, PDCA model, f) Security policy standards and practices- BS7799, ISO/IEC 17799, ISO27001	6
4	Domains of IT security	a) User/accepted usage/access, data access, physical access b) Internet access, e-mail, digital signature, c) Outsourcing, software development and acquisition, hardware acquisition d) Network and telecom, BCP and DRP, security organization structure. e) Domains related security-based case studies.	6
5	IT Governance and Management	a) IT Governance • Principles of IT governance • Assessing the effectiveness of IT governance frameworks b) IT Management and Operations	4

		• Evaluating IT policies, procedures, and controls • Change management and configuration control	
6	IS Auditing concepts	a) Overview of Information Systems Audit b) IS Audit Standards and Frameworks c) IS Auditing Planning and Management d) Techniques, methodologies, around and through computer, Controls – Concept objectives, types, risk. e) Auditing tools	10
7	Controls	a) Understanding Security & IT Audit Controls b) Categories of Controls (Administrative, Technical, Physical & Logical) c) Input, process, validation, output, logical access, physical access d) Classification of Controls (Preventive, Detective & Corrective) e) Database, network, environment, BCP, Evidence collection, evaluation and Reporting methodologies.	12
8	IS Audit Reporting and Communication	a) Audit Findings and Recommendations • Reviewing policies and procedures • Testing controls • Vulnerability assessment and penetration testing • Documenting and communicating audit findings • Providing actionable recommendations b) Audit Reporting • Developing clear and concise audit reports • Communicating findings to different stakeholders	4
9	Compliance and Ethics in IS Audit	a) Legal and Regulatory Compliance • Overview of relevant laws and regulations • Compliance audits and assessments b) Professional Ethics for IS Auditors • Code of Ethics and Professional Conduct for IS auditors • Ethical considerations in auditing practices	2
			60

Mode of Delivery

- Lectures (face to face and online)
- Case studies
- Demonstrations

Mode of Assessment

- Course work 30%
- End of semester examination 70%

The assignments will be given as follows;

Assignment 1: Take home
Assignment 2: Online real-time test (done in a controlled environment on campus)
Assignment 3: Practical test
Final Examination: Physical Exams

Learners are required to access the timetable and endeavor to sit for the exam as and when timetabled. Learners are required to attempt all three assignments and the final examination in order to complete the course. All assignments, including the take-home must be submitted on time. The pass mark score for the course is 50%. Therefore, any student who scores below that will be required to retake the examination when next offered.

Learning Management System

Learners are required to enroll themselves on MUBSEP; an online Moodle Online Learning Management System. All communication, teaching materials, assignments, results and discussion forum will be done on that forum.

Role of the student and Participation

Every learner is required to attend at least 75% of the classes to fulfil the minimum requirements to sit for the final examination. Learners must use their official full names when logging on for the online classes. This is a class that depends in large part on your participation and interaction for success. You are therefore, requested to actively participate and contribute in class and the discussion forums. Your input and questions will make this a better class. The more you put into the class, the more you will take from it. You are encouraged to keep time for class and stay the entire period. Learners are requested to keep their phones on silent mode during classes to avoid disruptions to themselves and other learners.

Role of the Facilitator

The facilitator shall not be a sage in class but rather will facilitate discussions and offer guidance to the learners. Students are welcome to make contributions in the different topics and share personal experience.

Statement of Academic Dishonesty

Academic dishonesty (e.g. cheating on assignments and examinations, plagiarism) is a serious offense. All work that you submit in this class must be your own. Each student is responsible for

being familiar with the MUBS policies on academic dishonesty. Any student engaging in academic dishonesty in this course will receive a fail grade (0) and appropriate disciplinary action will be taken.

Your submissions will be subjected to a similarity test using Turnitin antiplagiarism software. Therefore, you are advised to desist from plagiarism. Any plagiarized submission will be returned and you will be required to resubmit the assignment within 12 hours after the return time.

Reading List

1. Davis, C, Schiller, M., and Wheeler, K. (2011). IT Auditing Using Controls to Protect Information Assets. McGraw Hill Professional, 2nd Edition
2. Michael E. Whitman and Herbert J. Mattord (2003). Principles of Information Security. Thomson Course Technology, ISBN: 0619063181
3. Amjad Umar (2003). Information Security and Auditing in the Digital Age. Paperback. NGE Solutions.
4. The Art of Service (2021). IT Security Audit A Complete Guide - 2021 Ed. 4. The Art of Service