MASTER OF SCIENCE IN INFORMATION TECHNOLOGY SECURITY AND AUDIT

1. INTRODUCTION

Today's globalization and worldwide technology transfer and electronic business transactions have accelerated the demand for secure information systems. In order to compete effectively in the new global economy that demands a 24/7 response capability, organizations require continuous access to technological expertise that can ensure the integrity and security of their systems and availability and confidentiality of their data and information is guaranteed at all times. A better understanding of IT security audit ensures that information security solutions are better managed using best practices that are regularly audited. IT security auditing involves conducting audits in key areas where organizations are at risk to loss of information, thereby, leading to lose in confidence by business partners and customers. IT security administration addresses design architecture choices based on ISO, disaster recovery and project management best practices. Digital forensic expertise and cybercrime investigators are also required to figure-out what went wrong when enterprise security defense gets compromised. This Master of Information Technology Security and Audit is designed with this goal in mind.

2. OBJECTIVES

The overall objectives of the course is to train IT graduates who are skilled, knowledgeable and motivated to manage enterprise network resources security needs. The specific objectives are:

To develop the security needs of computer and network systems,

To assess, recommend and develop safeguard solutions, and

To manage the implementation and maintenance of security devices, systems, and procedures including security auditing best practices.

3. ADMISSION REQUIREMENTS

To qualify for admission into the Master Degree candidates shall be:

(a) Holders of at least an upper second class honours degree in Computer Science or Information Technology from Jaramogi Oginga Odinga University of Science and Technology or any other recognized University

(b) Holders of a lower second class honors degree of Jaramogi Oginga Odinga University of Science and Technology or any other recognized University and a Postgraduate Diploma in Computer Science from any other recognized University, or evidence of

extensive research experience as demonstrated by publications in peer reviewed journals.

(c) In addition to the above, applicants must meet the specific requirements of the Masters programme as approved by the Senate.

4. CREDITS TRANSFER

(a) A candidate may be exempted from some course units and credit(s) transferred from institutions recognized by the Senate, subject to the following conditions:

(b) Must have passed in similar course units at Master's level. Request for exemption should be made in writing to the Director, Board of Postgraduate Studies through the Dean of the School of Informatics and Innovative Systems and must be accompanied by officially endorsed supporting documents.

(c) Candidates may be allowed to transfer up to one third (1/3) of the total number of course units.

(d) Application for transfer will be processed only after payment of the prescribed fees.

5. COURSE STRUCTURE AND DURATION

The MSc (project option) course shall normally take two years covering 4 semesters offered by unit method.

Courses shall be offered in units. A course unit is defined as that part of a semester subject described by coherent syllabus and taught normally over a period of a semester. It is designated as a total of 42 hours of study in a semester. For this purpose, one 1-hour lecture is equivalent 2-hours tutorial or 3-hours practical or any combination as may be approved by the Board of the School of Informatics and Innovative Systems.

Part-time students shall be allowed to take not less than 50% of the courses prescribed for the year.

All course units will be taught for a total of 42 contact hours, including examinations except project work which will take 480 hours of practical work and project writing.

6. BASIC REQUIREMENTS

All core courses are compulsory; however, students can take additional electives courses up to a maximum of the six units.

7. EXAMINATIONS REGULATIONS

Jaramogi Oginga Odinga University of Science and Technology Examinations rules and regulation shall apply.

8. COURSE DISTRIBUTION

YEAR ONE: SEMESTER ONE

Course Code	Course Title	Contact Hours			Weight (Units)
		Lecture	Practical	Total	
IIT 5111	Computer Operating Systems & Virtualizations	28	14	42	1C
IIT 5112	Advanced Information Systems Security	28	14	42	1C
IIT 5113	TCP/IP Architecture and Enterprise Network	28	14	42	1C
IIT 5114	Securing an E-Commerce Infrastructure	28	14	42	1C
IIT 5115	Information Technology Law, Ethics and Society	28	14	42	1C
MBM 5113	Organizational Behaviour	42	0	42	1R
Total		**182**	**70**	**252**	**6**

YEAR ONE: SEMESTER TWO

Course Code	Course Title	Contact Hours			Weight (Units)
		Lecture	Practical	Total	
IIT 5121	Advanced Cryptography & Cyber-Security	28	14	42	1C

IIT 5122	Firewall Fundamentals	28	14	42	1C
IIT 5123	Advanced Network Security and Secure Network Communications	28	14	42	1C
IIT 5124	Risk Management	28	14	42	1C
IIT 5125	Research Methods	28	14	42	1C
MBM 5123	Financial Management	42	0	42	1R
Total		**182**	**70**	**252**	**6**

YEAR TWO: SEMESTER ONE

Course Code	**Course Title**	**Contact Hours**			**Weight (Units)**
		Lecture	**Practical**	**Total**	
IIT 5211	Security Policies, Standards, and Compliance Strategies	28	14	42	1C
IIT 5212	Advanced Information Systems Audit and Control	28	14	42	1C
IIT 5213	IT Security Planning Strategies and Project Management	28	14	42	1C
IIT 5214	Computer Digital Forensics	28	14	42	1C
IIT 5215	Advanced Cybercrime Investigation	28	14	42	1C
Total		**140**	**70**	**210**	**5**

ELECTIVES - Any one elective

Course Code	**Course Title**	**Contact Hours**			**Weight (Units)**
		Lecture	**Practical**	**Total**	
IIT 5216	Disaster Recovery Planning and Business	28	14	42	1E

	Continuity				
IIT 5217	Advances in Ethical Hacking and Penetration testing	28	14	42	1E
IIT 5218	HPC Cluster & Cloud Computing Technology	28	14	42	1E
IIT 5219	Network Management for Financial Management	28	14	42	1E

YEAR TWO: SEMESTER TWO

Course Code	**Course Title**	**Contact Hours**			**Weight (Units)**
		Lecture	**Practical**	**Total**	
IIT 5221	Project in Subject Area	0	480	480	1C

9. COURSE DESCRIPTION

YEAR ONE: SEMESTER ONE

IIT 5111 Computer Operating Systems & Virtualizations (42 hrs)

Introduction to hypervirtualization: Xen, VMware, Citrix XenServer, Windows 2008R2 Hyper-V or later, and Oracle VirtualBox. Introduction to major enterprise computer operating systems: Windows Server Active Directory security, policy and access controls. Secure Linux/UNIX powered servers using current CentOS/RHEL, Ubuntu and Mac OSX servers. DNS server and its implementation. LDAP (OpenLDAP) solution for identity management and Single-sign-on (SSO). OpenSSL for secure network communications (SSL/TLS). Secure messaging solutions using MS Exchange Server and open source Postfix and Sendmail mail servers.

IIT 5112 Advanced Information Systems Security (42 hrs)

Overview of IT security issues, policies, practices and procedures applicable to securing servers and networks. Code review, Security testing, Network testing and Penetration testing. Setup and maintenance of enterprise servers, firewalls and network devices. Network devices, servers and

clients: firmware, security fixes, and bug fixes. Host firewall, host intrusion detection (ID) and prevention systems (IPS). Host antivirus solutions.

IIT 5113 TCP/IP Architecture and Enterprise Network (42 hrs)

Current TCP/IP protocol suite: IP and protocols for address resolution, Internet control, routing, broadcasting, and multicasting. Private network interconnection: NAT, VPN. Network monitoring: packet analysis and data security. Network management and domain name systems. Bootstraps and autoconfiguration BOOTP, DHCP. Troubleshooting TCP/IP protocols. TCP/IP applications: telnet, file transfer, and simple mail transfer protocols. Secure complex Window and Linux/UNIX application servers. IP subnetting: simulate a network environment with capacity to accommodate thousands of devices (e.g., printers, servers, routers and network configuration). Designing a network. Security issues: firewall design, bastion machines, and proxies.

IIT 5114 Securing an E-Commerce Infrastructure (42 hrs)

Advances in e-commerce security: global internet-based online business. Latest techniques for securing the e-commerce infrastructure: concepts of SSL/TLS taking into account data architecture management, advanced network protocol, security techniques and online access and authentication controls. E-commerce environment: information security needs of organizations, privacy needs of customers and clients. Partners' requirements, government regulatory compliance and best practices in e-commerce domain.

IIT 5115 Information Technology Law, Ethics and Society (42 hrs)

Overview of International and Kenyan laws, legislation and legal issues relevant to information systems security profession. Social and ethical computer use: major social and ethical issues in computer science, impact of computers on society, and professional computer ethics. Impact of computers: applications, benefits, digital copyright, privacy, computer crime, constitutional issues, risks of computer failure, issues related to ethical hacking and penetration testing. Cloud computing: policy, security and privacy of data. Evaluating reliability of computer models, trade and communications in the global village, computers in the workplace.

MBM 5113 Organizational Behavior (42 hrs)

Concepts of organizational behavior. Individual Differences at work: Personality, attitude and intelligence. Motivation: Importance of motivation in work behaviour, approaches to motivation, content theories, process theories. Job analysis and Design: Approaches, job rotation, job enlargement, job design models. Communication: Types, transaction analysis, Johari windows. Training and Development: Training needs assessment, training techniques and training evaluation. Organizational Power, Politics and Conflict: Types, sources, conflict coping strategies. Leadership*:* Styles, theories and models. Performance appraisal: Need, methods and applications.

YEAR ONE: SEMESTER TWO

IIT 5121 Advanced Cryptography & Cyber-Security (42 hrs)

Principles of number theory, cryptographic algorithms and cryptanalysis techniques: Steganography and data hiding, block and stream ciphers encryption, secret key encryption (DES, RES, RE-N), primes, random numbers, factoring, integer factorization, and discrete logarithm problems. Public key encryption (RSA, Diffie-Helman, elliptical curve cryptography (ECC), ElGamal, N'TRU). Secure key management and key distribution solutions; Hash functions (MD5, SHA-1, RIPEMD-160, HMAC) and their applications; Digital signatures, certificates and authentication protocols. Cryptanalytic methods (known, chosen plaintext etc.) for secret and public key schemes (linear and differential cryptanalysis; Integer factorization techniques: Pollard's rho method, number field sieve, etc.). Secure communications.

IIT 5122 Firewall Fundamentals (42 hrs)

Firewall theory and architecture, technology and the implementation in routed IPv4 based TCP/IP networks. IPv6 based protocols in relation to IPv4. Firewall fundamentals: firewall network architecture, the firewall's role in a network, firewall types, firewall performance attributes, and firewall protection. Firewall installation: plan, design, deploy, implement, maintain and support secure enterprise network defense. Some of the software-based firewall/router/UTMs: Astaro SG and Vyatta router. Install and configure Cisco hardware firewall/UTMs. Test and evaluate firewall for security weaknesses and network defense mechanism using pen-test.

IIT 5123 Advanced Network Security and Secure Network Communications (42 hrs)

Advances in network environment security: firewalls, proxy servers, and other enterprise resources considerations for planning network connectivity and security. Planning and installing secure web servers, FTP server, Samba server, DNS server and messaging servers in a lab environment; implementing appropriate updates, bug fixes and patches to ensure network protection to the desired standards and best practices. Working with advance security tools: network scanning, web application penetration testing, log management, DLP, file integrity management etc. Test and evaluate network for security weaknesses and network defense mechanism using pen-test.

IIT 5124 Risk Management (42 hrs)

Best practices for conducting vulnerability assessments and countermeasures techniques. Advances in risk assessment tools; Establish cost benefit analysis for specific safeguards to organization's assets, confidentiality, availability and integrity of data and network resources. Risk management plan, Incidence response plan, Risk registry and best practices. Trends and latest advances in risk management plan and incidence response techniques via capstone research.

IIT 5125 Research Methods (42 hrs)

Formulating a research question or research problem, determining research design, assessing data collection methods, determining a sampling framework, types of data analyses and interpreting data. Determine specific areas of interest and develop a research plan and research proposal which will later be used (if approved) as the basis to proceed to the project work.

MBM 5123 Financial Management (42 hrs)

Introduction: financial management theory and financial statement analysis. Objectives and functions of financial management: time value of money, concept of risk and return. Capital Budgeting: Data requirements; evaluation techniques, pay back, internal rate of return, net present value, capitalization & capital structure, computation of specific and weighted cost of capital. Working capital management: determination of working capital cash management, receivables management and inventory management. Financial Decision: Relationship between dividend policy and value of a firm, dividend policy in practice, factors affecting dividend policy, legal and procedural aspects of dividend policy.

YEAR TWO: SEMESTER ONE

IIT 5211 Security Policies, Standards, and Compliance Strategies(42 hrs)

Advances in security management principles: defining security requirements, planning and documenting security policies, asset identification and control, system access control and Internet security. Security techniques to formulate, administer, audit, manage and evaluate network security policies and standards based on best practices and standards e.g., ISO 17799/27001, Payment Card Industry (PCI) Data Security Standard, Sarbanes-Oxley (SOX) Act for corporate financial accountability, HIPPA for healthcare industry accountability; GLBA for privacy and security of non-public information; best practices for security auditing (COBIT) and the protection of private information. Best practices to implement IT Infrastructure Library (ITIL) for service delivery support and management. NIST and KEBS security policies and standards.

IIT 5212 Advanced Information Systems Audit and Control (42 hrs)

Cryptographic algorithms, protocols and applications. Secure e-commerce. Cryptosystems: hash checksums, symmetrical and asymmetrical cryptography algorithms, advanced protocols and standards like RSA, ECC, AES and SSL, digital signatures and digital cash, the concept of a PKI and X509 certificates, and various crypto-software applications. Computer security and controls to information systems: authentication and access control, protection against malicious code and coders, database security, formal models, and policy issues. Concepts of layered protection mechanisms for secure web-based client/server systems on the Internet. Computer auditing transaction databases: auditing methodology, and evaluation of secure financial transaction.

IIT 5213 IT Security Planning Strategies and Project Management (42 hrs)

Advances in Project Management strategies: project planning, resources, costs, as well as project execution and progress tracking. The IT security project management process; project management methodologies and tools; IT project management standards; change management; Case studies: current issues in IT security project management; Disaster management and business continuity.

IIT 5214 Computer Digital Forensics (42 hrs)

Fundamentals and advances in computer forensics, cyber-crime scene investigations and analysis: digital data collection, preservation, presentation and preparation of computer based evidence for the purposes of criminal law enforcement or civil litigation. Formulation and implementation of organizational computer forensics preparedness policies; Determine the necessity for forensic procedures, extend governance processes to allow for proper future forensic investigations, and participation to computer forensics investigation teams.

IIT 5215 Advanced Cybercrime Investigations (42 hrs)

Advances in cybercrimes investigations: unauthorized access, mischief to data, possession of hacking tools, illegal drug trades; money laundry, human trafficking, possession of child pornography, identity theft and bank fraud detection. Legal aspects: institutional organizations, Kenyan judicial system, computer crime laws, bills of right, common law, mutual legal assistance treaty, search warrants, production and assistance orders, international laws, upcoming legal changes; Investigation process: search planning, acquisition methods, environment recognition, evidence identification. Reporting process: investigation and analysis reports, notes taking; Authority of seizure; Digital Forensics, Interviews; Computer crime trials: witness preparation, court sentencing, rebuttal witness, cross-examination, testimony, credibility attacks; Case studies: Capstone research project on cybercrime activities in Kenya and laws that govern it.

IIT 5216 Disaster Recovery Planning and Business Continuity (42 hrs)

Disaster recovery planning techniques: prevention, detection and recovery. Business continuity planning and management: identify the organization’s exposure to internal and external threats; hard and soft assets; provide effective prevention and recovery plan. System and data recovery plan: data backup and recovery best practices; offsite backup; comparison between hot, warm

and cold backup. Risk management standards and best practices in disaster recovery and business continuity strategies.

IIT 5217 Advances in Ethical Hacking and Penetration Testing (42 hrs)

Latest trends and advances in ethical hacking and penetration testing. Securing information systems against cyber-attacks. Application of concepts learned in previous classes to both defend and compromise a system. Various advanced tools for managing and compromising systems, safeguarding ancillary systems to prevent collateral damage during testing procedures. Legal and ethical issues associated with penetration testing.

IIT 5218 HPC Cluster & Cloud Computing Security (42 hrs)

Advances in High Performance Computing (HPC) technology: Virtualization, HPC Cluster, and Cloud Computing and security of data on the cloud. Virtualization technology: building HPC Cluster mimicking supercomputers. Design and build private and public cloud computing solutions using Ubuntu Enterprise Cloud Computing, Eucalyptus Cloud Systems and OpenNebula Cloud Computing solutions.

IIT 5219 Network Management for Financial Management (42 hrs)

Advances in management of network technologies in business applications. Telecommunications technologies: data communications, and networking technologies; components and topologies; network planning and management; network security, policy and access control; management issues: risk management; backup and recovery; privacy and ethics; networking legal issues; and emerging technologies and trends. Provisioning network technologies, and management of technical staff in networking.

YEAR TWO: SEMESTER TWO

IIT 5221 Project in Subject Area (480 hrs)

Each student will conduct his or her research with the approval and under the direction of the designated Departmental Course Coordinator. Prerequisites: Successful completion of all core ITSA courses.