

Risk Management, Information Security and Audit based on ISO / IEC 27002

ISACA Kenya will conduct a three day Risk Management, Information Security and Audit course following the two day E-Commerce Conference. The course will equip participants with the skills to oversee and provide assurance of the safe operations of e-commerce; m-banking, internet-banking and other e-commerce transactions.

The course is based on the ISO / IEC 27002 standard, which is part of the ISO/IEC 27000 family of standards.

The ISO 27002 is a code of practice, which provides best practice recommendations on information security management or use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS) In e-commerce. It outlines controls and control mechanisms, which may be implemented, to secure the Enterprise Information Assets.

The standard requires that management systematically examines the organization's information security risks, taking account of the threats, vulnerabilities and impacts; designs and implements a coherent comprehensive suite of controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that it deems unacceptable, and adopts a process to ensure information controls continue to meet the organization's security needs on an ongoing basis.

The course is targeted at I S Auditors, IS Managers, IS Regulators, IS Security personnel, Those in charge of compliance Regulators In charge.

The course is mapped to ISO / IEC 27002 Foundation Certification.

Course Cost KSh. 47,500

Optional Examination KSh. 16,000

Course Duration: 3 Days (15th -17th September 2010)

1 Information and security

1.1 The concept of information

- Data
- Informatics
- Information
- Information analysis
- Information architecture
- Storage medium
- Information management
- Information system
- Infrastructure

1.2 Value of information

- Asset
- Production factor

1.3 Reliability aspects

- Availability
 - Continuity
 - Robustness
 - Timeliness
- Integrity
 - Authenticity

- Verifiability
- Correctness
- Validity
- Precision
- Nonrepudiation
- Completeness
- Confidentiality
 - Exclusivity
 - Privacy

2 Threats and risks

2.1 Threat and risk

- Security measure
 - Preventive
 - Detective
 - Repressive
 - Corrective
- Threat
- Hacking
- Vulnerability
- Phishing
- Risk
- Risk assessment (Dependency & Vulnerability analysis)
- Risk analysis
 - Qualitative risk analysis
 - Quantitative risk analysis
- Risk management
- Risk strategy
 - Risk bearing
 - Risk neutral
 - Risk avoiding
- Damage
 - Direct damage
 - Indirect damage
- Spam
- Spyware
- Virus
- Worm

3 Approach and Organization

3.1 Security policy and security organization

- Security Policy
- Security Organization
- Category
- Impact
- Priority
- Urgency

3.2 Components

- Code of Conduct

3.3 Incident Management

- Security incident
- Escalation
 - Functional escalation
 - Hierarchical escalation
- Incident cycle
- ISO/IEC 20000:2005

4 Measures

4.1 Importance of measures

- Classification (grading)

4.2 Physical measures

- Authentication
- Biometrics
- Clean desk policy
- Interference
- Uninterruptible Power Supply (UPS)

4.3 Technical measures

- Access control
- Backup
- Botnet
- Certificate
- Cryptography
- Digital signature
- Encryption
- Hoax
- Logical access management
- Malware
- Maintenance door
- Patch
- Personal firewall
- Public Key Infrastructure (PKI)
- Rootkit
- Key
- Social engineering
- Trojan
- Validation
- Virtual Private Network (VPN)

4.4 Organizational measures

- Authorization
- Business Continuity Management (BCM)
- Business Continuity Plan (BCP)
- Disaster
- Disaster Recovery Plan (DRP)
- Segregation of duties

- Identification
- Stand-by arrangement
- Change Management

5 Legislation and regulations

5.1 Legislation and regulations

- Public records legislation
- Audit
- Copyright legislation
- Code of practice for information security (ISO/IEC 27002:2005)
- Compliance
- Security regulations for the government
- Security regulations for special information for the government
- Personal data protection legislation
- Computer criminality legislation