Course : Diploma in Information System Security Audit

I. Introduction to Information System Audit — Hours – Concept: 8.5 | Hands-On: 1.5

a. Definition and importance of information system audit
   i. Explanation of what an information system audit entails, including assessing the confidentiality, integrity, and availability of information systems. Also talking about privacy and security.
   ii. Importance of information system audits in ensuring regulatory compliance, risk management, and safeguarding organizational assets (including digital assets).

b. Evolution of auditing in the context of IT
   i. Historical overview of auditing practices and how they have adapted to incorporate IT systems.
   ii. Discussion on how advancements in technology have influenced auditing methodologies and practices.

c. Regulatory compliance and standards (e.g., SOX, GDPR, HIPAA)
   i. Overview of key regulations and standards that govern information system audits, such as Sarbanes-Oxley Act (SOX), General Data Protection Regulation (GDPR), and Health Insurance Portability and Accountability Act (HIPAA).
   ii. Explanation of the requirements imposed by these regulations and standards on organizations regarding information system audits – taking case study-based approach.

d. Objectives and scope of information system audit
   i. Identifying the primary objectives of information system audits, including assessing the effectiveness of controls, ensuring compliance with regulations, and identifying vulnerabilities.
   ii. Discussion on the scope of information system audits, including the systems and processes typically included in an audit.

e. Hands-on
   i. Provide a hypothetical scenario where candidates must assess the risks associated with a specific information system, considering factors such as the system's criticality, vulnerabilities, and potential impact on the organization.

II. Risk Assessment and Management — Hours – Concept: 12 | Hands-On: 1.5

a. Understanding risk in the context of information systems
   i. Definition of risk in the context of information systems, including potential threats, vulnerabilities, and impacts.
   ii. Explanation of different types of risks, such as security risks, operational risks, and compliance risks, also understanding classification of risks.

b. Risk assessment methodologies
   i. Overview of popular risk assessment frameworks and methodologies, such as COSO (Committee of Sponsoring Organizations of the Treadway Commission) and COBIT (Control Objectives for Information and Related Technologies).
   ii. Explanation of the steps involved in conducting a risk assessment, including risk identification, risk classification, risk analysis, and risk evaluation.

c. Risk management frameworks and practices
   i. Introduction to risk management frameworks, such as ISO 27001, NIST SP 800-30, and OCTAVE.
   ii. Discussion on risk treatment options, including risk acceptance, risk avoidance, risk mitigation, and risk transfer.

d. Identifying and prioritizing IT risks
   i. Techniques for identifying and documenting IT risks, such as risk registers, risk matrices, and risk heat maps.
   ii. Factors to consider when prioritizing IT risks, including likelihood, impact, and risk appetite.

e. Risk mitigation strategies
   i. Overview of risk mitigation strategies and controls, including preventive controls, detective controls, and corrective controls.
   ii. Discussion on implementing and monitoring risk mitigation measures to reduce the likelihood and impact of identified risks.

f. Hands-on
   i. Provide a hypothetical scenario where candidates must assess the risks associated with a specific information system, considering factors such as the system's criticality, vulnerabilities, and potential impact on the organization. Also, candidates will be identifying and prioritizing risks, documenting risk assessments, and proposing risk mitigation strategies.

III. IT Governance and Control Frameworks **Hours – Concept: 8.5 | Hands-On: 1.5**

a. Overview of Governance focusing on IT governance
   i. Introduction to IT governance frameworks such as COBIT (Control Objectives for Information and Related Technologies) and ITIL (Information Technology Infrastructure Library).
   ii. Explanation of the key principles and components of IT governance frameworks.

b. Control objectives and control activities
   i. Definition of control objectives and control activities in the context of IT governance.
   ii. Examples of common control objectives and activities related to information security, data privacy, and compliance.

c. Designing effective IT control frameworks
   i. Strategies for designing and implementing effective IT control frameworks, including defining control objectives, establishing control activities, and assigning responsibilities.
   ii. Considerations for tailoring control frameworks to meet the specific needs and objectives of an organization.

d. Monitoring and evaluating IT governance effectiveness
   i. Techniques for monitoring and evaluating the effectiveness of IT governance processes and controls.
   ii. Key performance indicators (KPIs) and metrics used to assess IT governance maturity and performance.

e. Hands-on
   i. Mapping control objectives to specific activities within a control framework and identifying gaps.

IV. Audit Planning and Execution **Hours – Concept: 8.5 | Hands-On: 1.5**

a. Planning an information system audit
   i. Steps involved in planning an information system audit, including scoping, risk assessment, and resource allocation.
   ii. Considerations for developing an audit plan, including objectives, scope, and methodology.

b. Conducting preliminary assessments
   i. Techniques for conducting preliminary assessments, including interviews, document reviews, and walkthroughs.
   ii. Identifying key stakeholders and obtaining necessary permissions and resources for the audit.

c. Developing audit programs and procedures
   i. Process for developing audit programs and procedures, including defining audit objectives, selecting audit techniques, and determining sampling methods.
   ii. Documentation requirements for audit programs and procedures.

d. Sampling techniques in information system audits
   i. Overview of sampling techniques used in information system audits, such as random sampling, stratified sampling, and judgmental sampling.

ii. Introducing CAAT Tools, Log Management, etc.

e. Documenting audit findings and conclusions

i. Guidelines for documenting audit findings, conclusions, and recommendations.

ii. Introducing ITAF (Information Technology Assurance Framework)

f. Hands-on

i. Provide candidates with a fictitious audit scenario (e.g., auditing a financial system) and relevant documentation (e.g., audit scope, objectives) and ask them for developing an audit program outlining the audit procedures, testing methodologies, and sampling techniques to be employed during the audit.

V. SDLC & It's Audit **Hours – Concept: 8.5 | Hands-On: 1.5**

a. Overview of SDLC Phases and Processes:

i. Provide candidates with an overview of the various phases of the SDLC, including requirements gathering, design, development, testing, deployment, and maintenance.

ii. Discuss key processes, methodologies (e.g., Agile, Waterfall), and best practices associated with each phase.

b. SDLC Control Objectives and Standards:

i. Introduce candidates to control objectives and standards relevant to SDLC audits, such as ISO/IEC 12207 (Software Life Cycle Processes), CMMI (Capability Maturity Model Integration), and OWASP ASVS (Application Security Verification Standard).

ii. Discuss compliance requirements, security considerations, and quality assurance measures throughout the SDLC.

c. Security Assessment of Development Tools and Environments:

i. Introducing DevSecOps and Threat Modelling

ii. Introduce candidates to common development tools and environments used in software development (e.g., IDEs, version control systems, issue tracking systems).

d. Hands-On Exercise: SDLC Process Evaluation:

i. Provide candidates with a case study or documentation of a software development project and let them evaluating the project's SDLC processes, including requirements management, change control, testing procedures, identifying potential vulnerabilities (e.g., insecure configurations, lack of access controls) and recommending security controls to mitigate risks.

VI. Application Controls and Security **Hours – Concept: 8.5 | Hands-On: 1.5**

a. Understanding application controls

i. Definition of application controls and their role in ensuring the integrity, confidentiality, and availability of data processed by applications.

ii. Classification of application controls into input controls, processing controls, and output controls.

b. Authentication and access controls

i. Explanation of authentication mechanisms (e.g., passwords, biometrics, multi-factor authentication) and access control techniques (e.g., role-based access control, discretionary access control).

ii. Best practices for implementing strong authentication and access controls to protect sensitive information.

c. Data integrity and validation controls

i. Overview of data integrity controls, including data validation, data reconciliation, and data integrity checks.

ii. Techniques for implementing data validation controls to prevent data entry errors and ensure data accuracy.

d. Encryption and cryptographic controls

i. Introduction to encryption techniques and cryptographic algorithms used to protect data in transit and at rest.

- ii. Considerations for implementing encryption and cryptographic controls to safeguard sensitive information from unauthorized access.

e. Security best practices for applications and databases
- i. Best practices for securing applications and databases, including secure coding practices, patch management, and database encryption.
- ii. Strategies for mitigating common security threats, such as SQL injection, cross-site scripting (XSS), and data breaches.

f. Hands-on
- i. Provide candidates with access to a demo application or sandbox environment and asking the for conducting a security assessment of the application, identifying security vulnerabilities (e.g., injection flaws, broken authentication) using tools like OWASP ZAP or Burp Suite, and proposing remediation measures.

VII. Physical and Environmental Security **Hours – Concept: 4.5 | Hands-On: 1.5**

a. Physical Security Controls
- i. Understand the need and requirements of Securing Physical Access to Facilities by Implementing physical access controls (e.g., locks, access cards, biometrics).
- ii. Designing secure entry points and monitoring access, using surveillance cameras and monitoring systems.

b. Environmental Security Controls
- i. Assessing the need for Protecting Against Environmental Threats including natural disasters (e.g., floods, earthquakes, fires).
- ii. Implementing measures to mitigate environmental risks (e.g., fire suppression systems, flood barriers).

c. Hands-On
- i. Provide candidates with a case study of a SOC facility layout and security policies and let candidates performing a physical and environmental security assessment, identifying vulnerabilities, and recommending improvements.

VIII. Network Security **Hours – Concept: 8.5 | Hands-On: 1.5**

a. Securing network infrastructure
- i. Overview of network security principles and techniques, including firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).
- ii. Considerations for designing and implementing secure network architectures to protect against external and internal threats.

b. Firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS)
- i. Explanation of how firewalls, IDS, and IPS work to monitor and control network traffic.
- ii. Deployment considerations and best practices for configuring firewalls, IDS, and IPS to detect and respond to security incidents.

c. Virtual private networks (VPNs) and secure sockets layer (SSL)
- i. Overview of VPN technologies and SSL encryption protocols used to secure remote access and data transmission over public networks.
- ii. Considerations for implementing VPNs and SSL to protect confidential communications and data privacy.

d. Network segmentation and zoning
- i. Benefits of network segmentation and zoning in reducing the attack surface and containing security breaches.
- ii. Strategies for implementing network segmentation and zoning to isolate critical assets and enforce access controls.

e. Hands-on
- i. Provide candidates with network diagrams and configurations of a simulated network environment and let them review the network configurations, identifying security weaknesses (e.g., open ports, misconfigured firewalls), and recommending improvements to enhance network security posture.

IX. Disaster recovery and business continuity planning **Hours – Concept: 6.5 | Hands-On: 1.5**

a. Key concepts of Disaster Recovery, Business Continuity Plan and Business Continuity Management
   - i. Understanding Incident Response, Continuity Management, Crisis Management, Importance of disaster recovery (DR) and business continuity planning (BCP) in ensuring the resilience of IT systems and operations.
   - ii. Components of DR and BCP strategies, including backup and recovery procedures, different data replication methods, and alternate site arrangements.

b. Testing and implementation of BCP
   - i. Considering the importance of testing a plan and different testing methodologies.
   - ii. Understanding the process of implementing a BCP/DR plan and importance of engaging an expert consultant in doing so.

c. BC/DR Planning and Standards
   - i. Understanding BC/DR principles and standards (e.g., ISO 22301).
   - ii. Developing comprehensive BC/DR plans and documents.

d. Hands-On
   - i. Developing and auditing BC/DR plans and conducting simulations and testing BC/DR readiness.

X. Audit Tools and Techniques **Hours – Concept: 6.5 | Hands-On: 2**

a. Overview of audit tools and software
   - i. Introduction to various audit tools and software used in information system audits, such as vulnerability scanners, penetration testing tools, and audit management platforms.
   - ii. Explanation of the functionalities and capabilities of different audit tools and their role in facilitating audit processes including some AI Tools.

b. Using data analytics for audit purposes
   - i. Importance of data analytics in information system audits for identifying patterns, trends, and anomalies in large datasets.
   - ii. Techniques for applying data analytics tools and methodologies to audit processes, such as data mining, statistical analysis, and visualization.

c. Continuous auditing and monitoring techniques
   - i. Definition of continuous auditing and monitoring and their benefits in providing real-time insights into the effectiveness of controls and detecting anomalies.
   - ii. Strategies for implementing continuous auditing and monitoring programs, including automated data collection, exception reporting, and continuous risk assessment.

d. Automated audit tools and their applications
   - i. Overview of automated audit tools and their role in streamlining audit processes, improving efficiency, and reducing manual effort.
   - ii. Examples of automated audit tools, such as audit management software, compliance management systems, and data analytics platforms, and their applications in different audit functions.

e. Hands-on
   - i. Case studies illustrating the use of audit tools and techniques in real-world audit scenarios, such as assessing security controls, analysing financial transactions, and evaluating compliance with regulatory requirements.

XI. Compliance and Legal Considerations **Hours – Concept: 6.5 | Hands-On: 1.5**

a. Legal and regulatory requirements for information system audits
   - i. Overview of legal and regulatory requirements that govern information system audits, including data protection laws, industry regulations, and international standards.
   - ii. Discussion on the implications of non-compliance with legal and regulatory requirements and potential consequences for organizations.

b. Privacy laws and regulations

  i. Explanation of privacy laws and regulations, such as the General Data Protection Regulation (GDPR), Digital Personal Data Protection Act, and Health Insurance Portability and Accountability Act (HIPAA).
  ii. Requirements imposed by privacy laws on organizations regarding data protection, consent management, data subject rights, and breach notification.

c. Intellectual property protection and digital rights management
  i. Importance of intellectual property protection and digital rights management in safeguarding proprietary information and content assets.
  ii. Strategies for implementing intellectual property protection measures, including copyright registration, trademark enforcement, and digital rights management systems.

d. Ethical considerations in information system auditing
  i. Discussion on ethical principles and professional standards that guide information system auditors in conducting their work with integrity, objectivity, and professionalism.
  ii. Case studies and scenarios highlighting ethical dilemmas in information system auditing and strategies for addressing ethical challenges in practice.

e. Hands-on
  i. Provide candidates with a Privacy Impact Assessment (PIA) template and a fictional scenario involving the processing of personal data and ask them for conducting a PIA, assessing the privacy risks associated with the data processing activities, and proposing controls to mitigate those risks.

XII. Emerging Technologies and Audit Considerations **Hours – Concept: 8 | Hands-On: 0**

a. Cloud computing security and audit challenges
  i. Overview of cloud computing, security risks and audit considerations, including data security, compliance, and vendor management.
  ii. Strategies for assessing and mitigating cloud computing risks through security controls and assurance mechanisms.

b. Internet of Things (IoT) security considerations
  i. Introduction to IoT security challenges, including device vulnerabilities, data privacy concerns, and ecosystem complexity.
  ii. Audit considerations for assessing IoT security risks and ensuring the integrity and confidentiality of IoT data.

c. Blockchain technology and its implications for audits
  i. Explanation of blockchain technology and its applications in securing transactions and digital assets.
  ii. Audit considerations for blockchain implementations, including smart contract audits, consensus mechanisms, and cryptographic controls.

d. Artificial intelligence (AI) and machine learning (ML) in auditing
  i. Opportunities and challenges of using AI and ML technologies in auditing, including automation, data analysis, and anomaly detection.
  ii. Considerations for auditing AI and ML algorithms, including transparency, fairness, and accountability.

e. Data Analytics & it's impact on technological landscape
  i. Understanding data analysis, types and Leveraging data analytics for audit processes.
  ii. Identifying patterns, anomalies, and risks using data analytics tools.

f. Robotics Process Automation
  i. What is RPA and Understanding the role of RPA through a case study
  ii. Assessing the impact of RPA on audit efficiency and accuracy.

XIII. India-Oriented Information System Topics and Compliances **Hours – Concept: 8 | Hands-On: 0**

a. Indian Information Technology Act (IT Act) and Amendments:
  i. Overview of the Indian Information Technology Act, its amendments, and associated regulations governing electronic transactions, digital signatures, and cybersecurity.

   ii. Examination of key provisions, such as data protection, electronic records retention, and liability of intermediaries, and their implications for information system audits.

b. Digital Personal Data Protection Act:
   i. Analysis of the DPDP Act and its implications for data protection and privacy in India.
   ii. Understanding the rights and obligations of data fiduciaries and data principals under the DPDP Act and compliance requirements for organizations handling personal data.

c. Reserve Bank of India (RBI) Guidelines on Information Security:
   i. Exploration of RBI guidelines and circulars related to information security, cybersecurity, and data protection for banks, financial institutions, and payment service providers.
   ii. Compliance requirements for implementing robust information security frameworks, incident reporting mechanisms, and cybersecurity controls in the financial sector.

d. Goods and Services Tax (GST) Compliance and IT Systems:
   i. Overview of GST compliance requirements and implications for IT systems, including invoicing, tax reporting, and compliance monitoring.
   ii. Considerations for auditing IT systems to ensure compliance with GST regulations, including GSTN integration, e-way bill generation, and reconciliation of GST returns.

e. Unique Identification Authority of India (UIDAI) Guidelines for Aadhaar Authentication:
   i. Understanding UIDAI guidelines for Aadhaar authentication and compliance requirements for entities using Aadhaar-based authentication services.
   ii. Audit considerations for assessing the security, privacy, and accuracy of Aadhaar authentication processes and systems.

f. Cybersecurity Framework for Critical Information Infrastructure (CII):
   i. Overview of the cybersecurity framework for critical information infrastructure (CII) sectors, as mandated by the Indian government.
   ii. Audit requirements for assessing the cybersecurity posture of critical infrastructure sectors, such as energy, transportation, banking, and healthcare, and ensuring compliance with CII cybersecurity guidelines.

g. Information Systems Audit and Certification by CERT-In:
   i. Explanation of information systems audit and certification processes conducted by the Indian Computer Emergency Response Team (CERT-In) for government organizations and critical infrastructure sectors.
   ii. Audit methodologies, assessment criteria, and compliance requirements for achieving CERT-In certification and accreditation.

h. National Cyber Security Strategy and Initiatives:
   i. Examination of India's National Cyber Security Strategy and government initiatives aimed at enhancing cybersecurity resilience, capacity-building, and public-private collaboration.
   ii. Role of information system audits in supporting national cybersecurity objectives, including risk assessment, incident response readiness, and cybersecurity awareness.

i. Data Localization and Cross-Border Data Transfer Regulations:
   i. Overview of data localization requirements and cross-border data transfer regulations in India, including restrictions on storing and transferring sensitive personal data outside the country.
   ii. Audit considerations for assessing compliance with data localization requirements, data sovereignty principles, and cross-border data transfer mechanisms.

j. IT Governance Frameworks and Compliance Standards:
   i. Adoption of international IT governance frameworks and compliance standards, such as COBIT, ISO/IEC 27001, and NIST Cybersecurity Framework, in the Indian context.
   ii. Alignment of IT governance practices with regulatory requirements and industry-specific compliance standards applicable to organizations operating in India.