CISA TIMETABLE (4 DAYS)

ISACA-CISA

Day 1

9.00	**9.30**	Welcome, Introductions, Coffee
9.30	**11.00**	About the CISA Exam **Domain 1 - The Process of Auditing Information Systems** Learning objectives Domain Task and Knowledge Statements Auditing ▪ Types of Audits ▪ Audit Methodology
11.00	**11.15**	Break
11.15	**12.00**	Risk-Based Auditing ▪ Risk Assessment Process ▪ A Risk-Based Audit Approach Internal Controls Audit Planning ▪ Effect of Laws and Regulations on IS Audit Planning ▪ Steps to determine compliance with external requirements
12.00	**13.00**	Lunch break
13.00	**16.15**	Performing the Audit ▪ Standards, Guidelines, Tools and Techniques ▪ ISACA IT Audit and Assurance Tools and Techniques ▪ ISACA IT Audit and Assurance Standards Framework ▪ Evidence Sampling ▪ Attribute sampling ▪ Variable sampling ▪ Statistical sampling terms ▪ Compliance vs. Substantive Testing ▪ Integrated Auditing Audit Analysis and Reporting ▪ Audit Documentation ▪ Automated Work Papers ▪ Evaluation of Audit Strengths and Weaknesses ▪ Computer-Assisted Audit Techniques ▪ Communicating Audit Results Control Self-Assessment (CSA) ▪ Objectives of Control Self-Assessment ▪ Benefits of Control Self-Assessment ▪ Disadvantages of Control Self-Assessment ▪ Continuous Auditing ▪ Continuous Auditing IT techniques ▪ Continuous Auditing Advantages & Disadvantages ISACA Code of Professional Ethics
16.15	**16.30**	Break
16.30	**17.00**	**Sample questions**

Day 2

9.00	**9.30**	
9.30	**11.00**	**Domain 2 - Governance and Management of IT** Learning objectives Domain Task and Knowledge Statements Governance and Management of IT ▪ Corporate Governance ▪ IT Governance ▪ Best Practices for IT Governance ▪ Information Security Governance Strategic Planning and Models ▪ IS Strategy ▪ IT Strategy Committee ▪ Standard IT Balanced Scorecard ▪ Enterprise Architecture ▪ Maturity and Process Improvement Models ▪ Auditing IT Governance Structure and Implementation
11.00	**11.15**	Break
11.15	**12.00**	Policies, Standards and Procedures ▪ Policies ▪ Procedures ▪ Standards Risk Management ▪ Risk Management Process ▪ Risk Analysis methods / techniques categories ▪ Qualitative Risk Analysis methods ▪ Quantitative Risk Analysis methods ▪ Quantitative vs. Qualitative ▪ Risk Response Options Resource Management ▪ IS Roles and Responsibilities ▪ Segregation of Duties Within IS ▪ Human Resource Management ▪ Personnel Security Principles ▪ Insider Threats ▪ Sourcing Practices
12.00	**13.00**	Lunch break
13.00	**16.15**	Management of IT Functional Operations ▪ Organizational Change Management ▪ Quality Management ▪ Performance Optimization Business Continuity Planning (BCP) ▪ IS Business Continuity Planning ▪ Disasters and Other Disruptive Events ▪ Business Continuity Planning Process ▪ BIA discovery techniques ▪ Business Impact Analysis (BIA) ▪ Business Continuity Plan

		▪ Components of a Business Continuity Plan ▪ Disaster Recovery **Sample questions**
16.15	**16.30**	Break
16.30	**17.00**	**Domain 3 - Information Systems Acquisition, Development, and Implementation** Learning objectives Domain Task and Knowledge Statements Program and Project Management ▪ Project / Program / Portfolio ▪ Project / Program / Portfolio Management ▪ Business Case Development and Approval ▪ Benefits Realization Techniques ▪ Project Communication ▪ Roles and Responsibilities of Groups and Individuals ▪ Project Planning ▪ Project Risk
Day 3		
9.00	**9.30**	
9.30	**11.00**	Systems Development Lifecycle (SDLC) ▪ Business Application Development ▪ Traditional SDLC Approach ▪ Boehm's Spiral Model ▪ Rapid Application Development (RAD) Model ▪ DSDM Atern & AgilePM ▪ Structured Analysis, Design and Development Techniques ▪ Alternative Development Methods ▪ Agile Development Types of Specialized Business Applications ▪ Electronic Commerce ▪ Electronic Data Interchange (EDI) ▪ Electronic Mail ▪ Electronic Banking ▪ Electronic Finance ▪ Electronic Funds Transfer (EFT) ▪ Automated Teller Machine (ATM) ▪ Business Intelligence (BI) Acquisition ▪ Infrastructure Development / Acquisition Practices ▪ Hardware Acquisition ▪ System Software Acquisition ▪ Auditing Systems Development Acquisition Application Controls ▪ Input/Origination Controls ▪ Processing Procedures and Controls ▪ Output Controls ▪ Auditing Application Controls ▪ System Change Procedures and the Program Migration Process **Sample questions**

11.00	**11.15**	Break
11.15	**13.00**	**Domain 4 - Information Systems Operations, Maintenance and Support** Learning objectives Domain Task and Knowledge Statements Auditing System Operations and Maintenance ▪ Information Security Management ▪ Information Systems Operations ▪ Infrastructure Operations ▪ Support / Help Desk ▪ Change Management Process ▪ Release Management System and Communications Hardware ▪ Computer Hardware Components and Architectures ▪ Security Risks with Portable Media ▪ Capacity Management ▪ IS Architecture and Software ▪ Operating Systems ▪ Database Management System (DBMS) ▪ Tape and Disk Management Systems ▪ Software Licensing Issues ▪ Digital Rights Management (DRM)
12.00	**13.00**	Lunch break
13.00	**16.15**	Auditing Networks ▪ Types of Data Network Structures ▪ Network Services ▪ OSI Architecture ▪ Types of Data Networks Topology ▪ Network Components (LAN / WAN devices) ▪ Communications Technologies ▪ Wireless Networking ▪ Risks Associated with Wireless Communications ▪ Auditing of Network Management Auditing Job Scheduling ▪ Job Scheduling Reviews ▪ Personnel Reviews Business Continuity and Disaster Recovery Plans ▪ Auditing of Business Continuity Plans ▪ Business Continuity Strategies ▪ Elements of Recovery ▪ Recovery Alternatives ▪ Hot Site ▪ Warm Site ▪ Cold Site ▪ Mirror Site or Multiple Processing Centers Auditing of Business Continuity Plans
16.15	**16.30**	Break
16.30	**17.30**	**Sample questions**

Day 4

9.00	**9.30**	
9.30	**11.00**	**Domain 5 - Protection of Information Assets** Learning objectives Domain Task and Knowledge Statements Information Security Management ▪ Importance of Information Security Management ▪ Key Elements of Information Security Management ▪ CSFs to Information Security Management ▪ Privacy Management Issues and the Role of IS Auditors ▪ Social Media Risks Access Controls ▪ System Access Permission ▪ Mandatory and Discretionary Access Controls ▪ IAAA ▪ Authentication ▪ Authorization ▪ Challenges with Identity Management ▪ Technical exposures include ▪ Logical Access Control Software ▪ Centralized vs. Decentralized Access ▪ Single Sign On (SSO) ▪ Remote Access ▪ Auditing Remote Access **Sample questions**
11.00	**11.15**	Break
11.15	**12.00**	Equipment and Network Security ▪ Security of Portable Media ▪ Mobile Device Security ▪ Network Infrastructure Security ▪ LAN Security Issues ▪ Client-server Security ▪ Wireless Security Threats ▪ Internet Threats and Security (active attacks) ▪ Firewalls ▪ Honeypots and Honeynets ▪ Intrusion Detection and Prevention Systems ▪ Network-based IPS (N-IPS) ▪ Network-based IDS (N-IDS) ▪ Host-based IDS (H-IDS) ▪ VoIP security issues Encryption • Strength of Encryption • Symmetric Encryption • Symmetric Key Cryptography • Asymmetric Algorithms • Asymmetric Key Cryptography • Hashing Algorithms • Digital Signatures

12.00	**13.00**	Lunch break
14.00	**16.15**	Malware • Malicious Code Threats • Unauthorized Software • Viruses Protection Incident Handling and Evidence • Security Incident Handling and Response • Evidence Handling Physical and Environmental Controls ▪ Locks ▪ Entrance Protection ▪ Closed-circuit television (CCTV) ▪ Security guards ▪ Lighting ▪ Electrical Power Supply ▪ Electrostatic Discharge ▪ HVAC ▪ Fire Suppression Systems ▪ Fire / Smoke Detection ▪ Controls for Environmental Exposures
16.15	**16.30**	Break
16.30	**17.00**	**Sample questions**
		That's all folks!