CISA TOC

The current CISA syllabus (2016) is divided into 5 domains. These domains are all examinable with different weighting in the exam. The exam has 150 multiple choice questions to be completed within a 4-hour period.

Following is a summary of the CISA domains:

Domain	Topic	Exam Weightage	Approximate number of Questions
Domain 1	The Process of Auditing Information Systems	21%	32
Domain 2	Governance and Management of IT	16%	24
Domain 3	Information Systems Acquisition, Development and Implementation	18%	27
Domain 4	Information Systems Operations, Maintenance and Service Management	20%	30
Domain 5	Protection of Information Assets	25%	37
Total		**100%**	**150 Question**

Task statements are what a CISA candidate is expected to know how to perform.
Knowledge statements are those a CISA student should have a good grasp to perform the tasks.
Task and Knowledge statements establish and maintain the process of auditing information systems. Tasks can be mapped to more than one knowledge statement.

Domain-1: Process of Auditing Information system

S. No	Topics
1.	Information Tech Assurance Framework (ITAF)
2.	Standards
3.	Guidelines
4.	Professional Ethics IPS PC DE
5.	CobiT
6.	Audit
7.	Risk
8.	Internal Control
9.	Performing IS Audit
10.	IS Control Objectives
11.	IS control procedures include-
12.	Audit Program
13.	Audit Procedure
14.	Audit Methodology
15.	Risk Based Audit
16.	Gap Analysis
17.	Assurance Definitions

18.	Risk Assessment Technique
19.	Compliance testing vs. substantive testing
20.	Audit evidence gathering Techniques
21. `	Sampling
22.	Balanced Score Card
23.	Evidence
24.	Audit Documentation
25.	Computer Assisted Audit Techniques (CAATs)
26.	Working Paper
27.	Communication of Audit Results
28.	The Report
29.	Control self-assessment (CSA)
30.	Continuous Audit
31.	Audit Charter
32.	Audit Trail

Domain 2: Governance and Management of IT

S. No	Topics
1.	IT Governance
2.	Quality Management System
3.	Information technology Monitoring and assurance practices
4.	Various levels of Organization
5.	Audit role in IT Governance
6.	Monitoring and Reporting IT Performance
7.	BSC (balanced score board) CB FG
8.	Key Performance Indicator(KPI)
9.	IS strategic planning:
10.	Maturity and Process improvement models
11.	IT investment and allocation process
12.	Policy and procedures
13.	Risk Management
14.	Risk analysis methods:
15.	IS Management practices
16.	Employee Roles and Duties
17.	The duties that should be segregated are:
18.	Reviewing Audit Documents
19.	Reviewing contractual commitment s
20.	Business Impact Analysis Related to Business Continuity Planning
21.	Business Continuity Plan (BCP)
22.	Invoking the BCP/DRP
23.	Enterprise Risk Management
24.	Ways of Quality Assurance
25.	Quality Management
26.	Resource Allocation

Domain 3: Acquisition, Development and Implementation

S. No	Topics
1.	Overview
2.	Project Governance Mechanism
3.	When purchasing or acquiring hardware and software from a vendor, consider the following:
4.	Terms
5.	CMM
6.	Project organization forms
7.	Project objectives
8.	Project Culture
9.	object breakdown structure (OBS)
10.	Software Cost Estimation
11.	Software size estimation methods
12.	Scheduling
13.	Project risks
14.	Resource Usages Management
15.	Closing a Project
16.	Requirement Analysis
17.	Enterprise Architecture
18.	SDLC
19.	Software baseline
20.	Software testing process
21.	Classification of Testing
22.	Other types of testing
23.	Data conversion
24.	Changeover (cutover or go-live technique)
25.	Post implementation review
26.	EDI (electronic data interchange)
27.	DSS(Decision support system)
28.	Alternative forms of software project organization
29.	Prototyping
30.	Rapid application development (RAD)
31.	Alternative system development methods
32.	Proof of concept
33.	Configuration management
34.	CMMI (capability maturity model integration)
35.	Application controls
36.	Input controls
37.	Data processing controls and procedures
38.	Output controls
39.	Tasks of IS Auditor in application controls
40.	Important controls for data validation and editing
41.	Important controls for data files
42.	Data integrity tests
43.	Data integrity in online transaction

44.	Continuous online auditing
45.	Online auditing techniques:
46.	Release Management
47.	Change Management
48.	Project Success
49.	System Migration and Infrastructure Development
50.	Important points to remember

Domain 4: Information System operations, Maintenance and Service Management

S. No	Topics
1.	IS operation management
2.	Enterprise Architecture
3.	Technology Concepts
4.	Hardware Auditing
5.	Operating System Integrity
6.	Access Control Software
7.	Types of Network
8.	Wireless Network Security
9.	System Resiliency
10.	Sites and Spares
11.	Backup
12.	Software Licensing Issues
13.	Job Scheduling
14.	Control Techniques for Interface Integrity
15.	Systems Performance Monitoring Processes, Tools and Techniques
16.	Data backup
17.	Risks and Controls for End-User computing
18.	Regulatory issues and DRP
19.	Disaster recovery
20.	Disaster Recovery
21.	RFID (Radio frequency identification)
22.	Capacity Planning and Related Monitoring Tools and Techniques
23.	IS architecture
24.	Data communication software
25.	Database management system (DBMS)
26.	Data Quality
27.	Types of data structure
28.	Important table properties of relational database:
29.	Important points about database: (Just like vlookup process)
30.	Disk and tape management
31.	Digital right management (DRM)
32.	Physical Media for LAN
33.	WAN implementation methods are:
34.	Important LAN components:

35.	WAN (wide area network)
36.	Some popular WAN technologies that are used to establish the connection are:
37.	Virtual private network(VPN)
38.	WAP (Wireless application protocol)
39.	CGI (common gateway interface)
40.	Applet
41.	Servlets
42.	Telnet (Remote terminal control protocol)
43.	Network management tools
44.	Parity, Checksum and CRC
45.	On Demand Computing (ODC) or Utility Computing
46.	Important Points

Domain 5: Protection of Information Assets

S. No	Topics
1.	Overview
2.	External Requirements
3.	Privacy Policy
4.	Data Leakage
5.	End User Computing
6.	Security Awareness Program
7.	Attack Methods
8.	Prevention and Detection
9.	Network Infrastructure security
10.	Security Testing
11.	Security Incidents
12.	Forensics
13.	Fraud
14.	Email Fraud
15.	Maintenance and Monitoring of Security Controls
16.	Physical Control
17.	DAC (Discretionary logical access) MAC (Mandatory logical access)
18.	Data Owner Data Custodian Security Administrator
19.	Types of DOS (denial of service attacks)
20.	Wireless (Wi-Fi Security)
21.	Other Types of Attacks
22.	Logical Access Control
23.	Operating System Issues
24.	Hardware Security
25.	Database Activity Monitoring
26.	Virtual System

27.	Mobile and Wireless
28.	Open V. Close Operating System
29.	Laptop Security
30.	Bring Your Own Device
31.	Voice Communications Security
32.	Private Branch Exchange (PBX)
33.	Security Devices
34.	Protocols
35.	Firecall ID
36.	Biometrics
37.	SSO (single sign-on):
38.	Disadvantages of VPN
39.	NAS (network access server)
40.	Audit Trail(logs)
41.	Network Infrastructure Security
42.	SEIM(Security information and event management)
43.	Dial back modem control
44.	Active Attack and Passive Attack
45.	Firewall types
46.	Firewall implementation methods
47.	Penetration testing phases
48.	Computer forensic
49.	Encryption
50.	Elements of PKI
51.	Digital Signature
52.	X.509 Certificates
53.	Peer-to-peer, IM, and Web
54.	Various security risks in using social networking sites:
55.	Data Classification Standards
56.	Store, Retrieve, Transport, and Dispose of Confidential Information
57.	Destruction of Confidential Data
58.	IPsec (Internet protocol security)
59.	SSH-secure shell
60.	Environmental exposures and controls
61.	Storing, retrieving, Transporting and Disposing of Confidential Information
62.	Important Points
63.	Other Imp points