



TOIT TRAINING LLC

Certified Information Systems Auditor (CISA)

Overview: Our CISA Certified Information Systems Auditor Series provides the student with the knowledge and proficiency to prepare for the globally recognized CISA certification exam. The CISA certification has become very popular since it originated in 1978, and is a benchmark for IS audit, security, control, and assurance personnel to validate their skill set. This course will immerse the student into the subject, with in-depth coverage of the information covering the five domains that make up the “Body of Knowledge” for the CISA exam and will provide the student the tools to build their technical skills to develop, manage, and perform IT security audits.

The CISA designation is a globally recognized certification for IS audit control, assurance and security professionals. Being CISA-certified showcases your audit experience, skills and knowledge, and demonstrates you are capable to assess vulnerabilities, report on compliance and institute controls within the enterprise. The CISA certification is sought by those who audit, control, monitor and assess an enterprise’s information technology and business systems. CISAs are recognized internationally as professionals with the assurance, knowledge, skills, experience and credibility to leverage standards, manage vulnerabilities, ensure compliance, offer solutions, institute controls and deliver value to the enterprise.

1001 Wilshire Boulevard #1071
Los, Angeles, CA 90017
support@toittraining.com
(909) 760-0217
(909) 760-0218 Fax
<https://toittraining.com>

Course Modules:

Module 01 – The Process of Auditing Information Systems

(Duration: 3h 44m)

1. Workbook (Pdf)
2. Lesson 1: Management of the Audit Function
3. Organization of the IS Audit Function
4. IS Audit Resource Management
5. Audit Planning
6. Effect of Laws and Regulations on IS Audit Planning
7. Lesson 2: ISACA IT Audit and Assurance Standards and Guidelines
8. ISACA IT Audit And Assurance Standards And Guidelines
9. ISACA IT Audit And Assurance Standards Framework
10. Auditing Standards
11. Audit Guidelines
12. Audit and Assurance Tools and Techniques
13. Relationship Among Standards, Guidelines, and Tools and Techniques
14. Information Technology Assurance Framework
15. Information Technology Assurance Framework Components
16. ITAF General Standards (Section 2200)
17. ITAF Performance Standards (Section 2400)
18. Reporting Standards (Section 2600)
19. IT Assurance Guidelines (Section 3000)
20. Lesson 3: Risk Analysis

1001 Wilshire Boulevard #1071
Los, Angeles, CA 90017
support@toittraining.com
(909) 760-0217
(909) 760-0218 Fax
<https://toittraining.com>



TOIT TRAINING LLC

21. Risk Analysis
22. Lesson 4: Internal Controls
23. Internal Control Objectives
24. IS Control Objectives
25. COBIT
26. General Controls
27. IS Controls
28. Lesson 5: Performing An IS Audit
29. Performing an IS Audit
30. Classification of Audits
31. Audit Programs
32. Audit Methodology
33. Fraud Detection
34. Risk-Based Auditing
35. Audit Risk and Materiality
36. Risk Assessment and Treatment
37. Risk Assessment Techniques
38. Audit Objectives
39. Compliance Versus Substantive Testing
40. Evidence
41. Interviewing and Observing Personnel in the Performance Of Their Duties
42. Sampling
43. Using The Services Of Other Auditors And Experts
44. Computer-Assisted Audit Techniques (CAAT)
45. Evaluation Of Audit Strengths And Weaknesses
46. Communicating Audit Results
47. Management Implementation Of Recommendations
48. Audit Documentation
49. Lesson 6: Control Self-Assessment
50. Objectives of CSA
51. Benefits of CSA
52. Disadvantages of CSA
53. Auditor Role in CSA

1001 Wilshire Boulevard #1071
Los, Angeles, CA 90017
support@toittraining.com
(909) 760-0217
(909) 760-0218 Fax
<https://toittraining.com>

- 54. Technology Drivers for CSA
- 55. Traditional Versus CSA Approach
- 56. Lesson 7: The Evolving IS Audit Process
- 57. Automated Work Papers
- 58. Integrated Auditing
- 59. Continuous Auditing
- 60. Module 01 Review
- 61. **Review Quiz (Number of attempts allowed: Unlimited)**

Module 02 – Governance and Management of IT

(Duration: 3h 40m)

- 1. Workbook (Pdf)
- 2. Lesson 1: Corporate Governance
- 3. Corporate Governance
- 4. Lesson 2: IT Governance
- 5. IT Governance
- 6. Lesson 3: IT Monitoring and Assurance Practices for Board and Senior Management
- 7. IT Monitoring and Assurance Practices for Board and Senior Management
- 8. Best Practices for IT Governance
- 9. IT Governance Frameworks
- 10. Audit Role in IT Governance
- 11. IT Strategy Committee
- 12. IT Balanced Scorecard
- 13. Information Security Governance
- 14. Importance of Information Security Governance
- 15. Outcomes of Security Governance



TOIT TRAINING LLC

16. Effective Information Security Governance
17. Roles and Responsibilities of Senior Management and Board of Directors
18. Enterprise Architecture
19. Lesson 4: Information Systems Strategy
20. Strategic Planning
21. Steering Committee
22. Lesson 5: Maturity and Process Improvement Models
23. Maturity and Process Improvement Models
24. Lesson 6: IT Investment and Allocation Practices
25. IT Investment and Allocation Practices
26. Implement IT Portfolio Management
27. IT Portfolio Management Versus Balanced Scorecard
28. Lesson 7: Policies and Procedures
29. Policies
30. Information Security Policy
31. Procedures
32. Lesson 8: Risk Management
33. Risk Management
34. Developing a Risk Management Program
35. Risk Management Process
36. Risk Analysis Methods
37. Lesson 9: IS Management Practices
38. Human Resource Management
39. Organizational Change Management
40. Financial Management Practices
41. Quality Management
42. Information Security Management
43. Performance Optimization
44. Lesson 10: IS Organizational Structure and Responsibilities
45. IS Roles and Responsibilities
46. Segregation of Duties
47. Segregation of Duties Controls
48. Compensating Controls for Lack of Segregation

1001 Wilshire Boulevard #1071
Los, Angeles, CA 90017
support@toittraining.com
(909) 760-0217
(909) 760-0218 Fax
<https://toittraining.com>

49. Lesson 11: Auditing IT Governance Structure and Implementation
50. Reviewing Documentation
51. Reviewing Contractual Commitments
52. Lesson 12: Business Continuity Planning
53. IS Business Continuity Planning
54. Disasters and Other Disruptive Events
55. Business Continuity Planning Process
56. Business Continuity Policy
57. Business Impact Analysis
58. Classification of Operations and Criticality Analysis
59. Development of Business Continuity Plans
60. Other Issues and Plan Development
61. Components of a BCP
62. BCP Testing
63. BCP Maintenance
64. Summary of BCP
65. Module 02 Review
66. Review Quiz (**Number of attempts allowed: Unlimited**)

Module 03 – Information Systems Acquisition, Development and Implementation

(Duration: 3h 12m)

1. Workbook (Pdf)

1001 Wilshire Boulevard #1071
Los, Angeles, CA 90017
support@toittraining.com
(909) 760-0217
(909) 760-0218 Fax
<https://toittraining.com>



TOIT TRAINING LLC

2. Lesson 1: Business Realization
3. Portfolio/Program Management
4. Business Case Development and Approval
5. Benefits Realization Techniques
6. Lesson 2: Project Management Structure
7. Project Context and Environment
8. Project Organizational Forms
9. Project Communication and Culture
10. Project Objectives
11. Roles and Responsibilities of Groups and Individuals
12. Lesson 3: Project Management Practices
13. Initiation of a Project
14. Project Planning
15. Example of Project Management for New Software
16. Software Size Estimation
17. Lines of Source Code
18. Function Point Analysis (FPA)
19. Function Points
20. Cost Budgets
21. Software Cost Estimation
22. Scheduling and Establishing the Timeframe
23. Critical Path Methodology
24. Gantt Charts
25. Program Evaluation Review Technique (PERT)
26. Time Box Management
27. General Project Management
28. Project Controlling
29. Management of Resource Usage
30. Management of Risk
31. Closing a Project
32. Lesson 4: Business Application Development
33. Traditional SDLC Approach
34. SDLC Phases

1001 Wilshire Boulevard #1071
Los, Angeles, CA 90017
support@toittraining.com
(909) 760-0217
(909) 760-0218 Fax
<https://toittraining.com>



TOIT TRAINING LLC

35. SDLC
36. Integrated Resource Management Systems
37. Description of SDLC Phases
38. Risks Associated with Software Development
39. Lesson 5: Business Application Systems
40. Electronic Commerce
41. E-Commerce Models
42. E-Commerce Architectures
43. E-Commerce Risks
44. E-Commerce Requirements
45. E-Commerce Audit and Control Issues or Best Practices
46. Components of PKI
47. Electronic Data Interchange
48. General Requirements of EDI
49. Traditional EDI
50. Web Based EDI
51. EDI Risks and Controls
52. Controls in EDI Environment
53. E-Mail
54. E-Mail Security Issues
55. Standards for E-Mail Security
56. Point-Of-Sale Systems (POS)
57. Electronic Banking
58. Risk Management Challenges in E-Banking
59. Risk Management Controls for E-Banking
60. Electronic Finance
61. Payment Systems
62. Electronic Money Model
63. Electronic Checks Model
64. Electronic Transfer Model
65. Electronic Funds Transfer
66. Controls in an EFT Environment
67. Automated Teller Machines

1001 Wilshire Boulevard #1071
Los, Angeles, CA 90017
support@toittraining.com
(909) 760-0217
(909) 760-0218 Fax
<https://toittraining.com>



TOIT TRAINING LLC

68. Image Processing
69. Business Intelligence
70. Decision Support System (DSS)
71. DSS Frameworks
72. Customer Relation Management (CRM)
73. Supply Chain Management (SCM)
74. Lesson 6: Alternative Forms of Software Project Organization
75. Agile Development
76. Prototyping
77. Rapid Application Development (RAD)
78. Lesson 7: Alternative Development Methods
79. Data Oriented System Development
80. Object Oriented System Development
81. Component-Based Development
82. Web-Based Application Development
83. Software Reengineering
84. Reverse Engineering
85. Lesson 8: Infrastructure Development/Acquisition Practices
86. Project Phases of Physical Architecture Analysis
87. Planning Implementation of Infrastructure
88. Critical Success Factors
89. Hardware Acquisition
90. Acquisition Steps
91. System Software Acquisition
92. System Software Implementation
93. System Software Change Control Procedures
94. Lesson 9: Information Systems Maintenance Practices
95. Change Management Process Overview
96. Deploying Changes
97. Documentation
98. Testing Changed Programs
99. Auditing Program Changes
100. Emergency Changes

1001 Wilshire Boulevard #1071
Los, Angeles, CA 90017
support@toittraining.com
(909) 760-0217
(909) 760-0218 Fax
<https://toittraining.com>

101. Change Exposures (Unauthorized Changes)
102. Configuration Management
103. Lesson 10: System Development Tools And Productivity Aids
104. Code Generators
105. Computer Aided Software Engineering
106. Fourth-Generation Languages (4GL)
107. Lesson 11: Business Process Reengineering And Process Change Projects
108. Business Process Reengineering And Process Change Projects Continued
109. Benchmarking Process
110. The Benchmarking Process
111. ISO 9126
112. Software Capability Maturity Model
113. ISO 15504
114. Lesson 12: Application Controls
115. Inputs Controls
116. Processing Procedures And Controls
117. Processing Controls
118. Data File Control Procedures
119. Output Controls
120. Business Process Control Assurance
121. Lesson 13: Auditing Application Controls
122. Risk Assessment Model To Analyze Application Controls
123. Observing And Testing User Performing Procedures
124. Data Integrity Testing
125. Example Of Referential And Relational Integrity
126. Data Integrity In Online Transaction Processing Systems
127. Test Application Systems
128. Continuous Online Auditing
129. Online Auditing Techniques
130. Lesson 14: Auditing Systems Development, Acquisition And Maintenance
131. Project Management
132. Feasibility Study
133. Requirements Definition

- 134. Software Acquisition Process
- 135. Detailed Design And Development
- 136. Testing
- 137. Implementation Phase
- 138. Post Implementation Review
- 139. System Change Procedures And The Program Migration Process
- 140. Module 03 Review
- 141. **Review Quiz (Number of attempts allowed: Unlimited)**

Module 04 – Information Systems Operations, Maintenance and Support

(Duration:2h 47m)

- 1. Workbook (Pdf)
- 2. Lesson 1: Information Systems Operations
- 3. Management of IS Operations
- 4. Service Management
- 5. Service Level
- 6. Infrastructure Operations
- 7. Scheduling
- 8. Monitoring Use of Resources
- 9. Process of Incident Handling
- 10. Problem Management
- 11. Detection, Documentation, Control, Resolution and Reporting of Abnormal Conditions
- 12. Support/Helpdesk
- 13. Change Management Process

1001 Wilshire Boulevard #1071
Los, Angeles, CA 90017
support@toittraining.com
(909) 760-0217
(909) 760-0218 Fax
<https://toittraining.com>



TOIT TRAINING LLC

14. Release Management
15. Information Security Management
16. Media Sanitization
17. Lesson 2: Information Systems Hardware
18. Computer Hardware Components and Architecture
19. Common Enterprise Backend Devices
20. Specialized Devices
21. Risks
22. Security Control
23. Radiofrequency Identification
24. RFID Applications
25. RFID Risks
26. RFID Security Control
27. Hardware Maintenance Program
28. Hardware Monitoring Procedures
29. Capacity Management
30. Lesson 3: IS Architecture and Software
31. Operating Systems
32. Software Integrity Issues
33. Activity Logging and Reporting Options
34. Data Communication Software
35. Data Management
36. File Organization
37. Database Management Systems
38. Example of Data in DBMS
39. DBMS Architecture
40. DBMS Metadata Architecture
41. Database Structure
42. Relational Database
43. Database Models
44. Relational Database Model
45. Database Controls
46. Tape and Disk Management Systems

1001 Wilshire Boulevard #1071
Los, Angeles, CA 90017
support@toittraining.com
(909) 760-0217
(909) 760-0218 Fax
<https://toittraining.com>



TOIT TRAINING LLC

47. Utility Programs
48. Software Licensing Issues
49. Digital Rights Management
50. Lesson 4: Network Infrastructure
51. Enterprise Network Architecture
52. Types of Networks
53. Network Services
54. Network Standards and Protocols
55. OSI Architecture
56. OSI Layers
57. Application of the OSI Model in Network Architectures
58. Local Area Network
59. Network Physical Media Specifications
60. Implementation of WANs
61. LAN Media Access Technologies
62. LAN Components
63. OSI Layer Diagram
64. LAN Technology Selection Criteria
65. Wide Area Networks
66. WAN Message Transmission Techniques
67. WAN Devices
68. WAN Technologies
69. Wireless Networks
70. Wireless Wide Area Networks
71. Wireless Local Area Networks
72. Wireless Security
73. Wireless Application Protocol
74. Risks of Wireless Communications
75. World Wide Web Services
76. General Internet Terminology
77. Network Administration and Control
78. Network Performance Metrics
79. Network Management Issues

1001 Wilshire Boulevard #1071
Los, Angeles, CA 90017
support@toittraining.com
(909) 760-0217
(909) 760-0218 Fax
<https://toittraining.com>

80. Network Management Tools
81. Client/Server Technology
82. Lesson 5: Disaster Recovery Planning
83. Recovery Point Objective and Recovery Time Objective
84. Recovery Strategies
85. Application Disaster Recovery Methods
86. Data Storage Disaster Recovery Methods
87. Telecommunication Networks Disaster Recovery Methods
88. Methods for Network Protection
89. Development of Disaster Recovery Plans
90. Organization and Assignment Of Responsibilities
91. Backup and Restoration
92. Off-Site Library Controls
93. Types of Backup Devices and Media
94. Periodic Backup Procedures
95. Frequency of Rotation
96. Backup Schemes
97. Module 04 Review
98. **Review Quiz (Number of attempts allowed: Unlimited)**

Module 05 – Protection of Information Assets

(Duration: 2h 30m)

1. Workbook (Pdf)
2. Lesson 1: Importance Of Information Security

1001 Wilshire Boulevard #1071
Los, Angeles, CA 90017
support@toittraining.com
(909) 760-0217
(909) 760-0218 Fax
<https://toittraining.com>



TOIT TRAINING LLC

3. Key Elements of Information Security Management
4. Information Security Management Roles and Responsibilities
5. Inventory and Classification of Information Assets
6. System Access Permission
7. Mandatory and Discretionary Access Controls
8. Privacy Management Issue and the Role of IS Auditors
9. Critical Success Factors to Information Security Management
10. Information Security and External Parties
11. Identification of Risks Related to External Parties
12. Addressing Security When Dealing with Customers
13. Addressing Security and Third-Party Agreements
14. Human Resources Security and Third Parties
15. Computer Crime Issues and Exposures
16. Types of Computer Crimes
17. Peer to Peer, Instant Messaging, Data Leakage and Web-Based Technologies
18. Security Incident Handling and Response
19. Lesson 2: Logical Access
20. Logical Access Exposures
21. Familiarization with the Enterprise IT Environment
22. Paths of Logical Access
23. General Points of Entry
24. Logical Access Control Software
25. Identification and Authentication
26. Features of Passwords
27. Identification and Authentication Best Practices
28. Token Devices, One-Time Passwords
29. Management of Biometrics
30. Single Sign-On
31. Authorization Issues
32. Access Control Lists
33. Logical Access Security Administration
34. Remote Access Security
35. Common Connectivity Methods

1001 Wilshire Boulevard #1071
Los, Angeles, CA 90017
support@toittraining.com
(909) 760-0217
(909) 760-0218 Fax
<https://toittraining.com>



TOIT TRAINING LLC

36. Remote Access Using PDAs
37. Access Issues with Mobile Technology
38. Access Rights to System Logs
39. Tools for Audit Trail Analysis
40. Use of Intrusion Detection
41. Storing, Retrieving, Transporting and Disposing of Confidential Information
42. Lesson 3: Network Infrastructure Security
43. LAN Security
44. Virtualization
45. Client/Server Security
46. Wireless Security Threats and Risks Mitigation
47. Internet Threats and Security
48. Network Security Threats
49. Internet Security Control Audits
50. Firewall Security Systems
51. Common Attacks Against a Firewall
52. Examples of Firewall Implementation
53. Intrusion Detection
54. Describing IDS and IPS Deployment
55. Encryption
56. Uses of Encryption
57. Viruses
58. Technical Controls Against Viruses
59. AV Software
60. Voice Over IP
61. Private Branch Exchange
62. Lesson 4: Auditing Information Security Management Framework
63. Auditing Logical Access
64. Techniques for Testing Security
65. Lesson 5: Auditing Network Infrastructure Security
66. Auditing Remote Access
67. Network Penetration Test
68. Types of Penetration Tests

1001 Wilshire Boulevard #1071
Los, Angeles, CA 90017
support@toittraining.com
(909) 760-0217
(909) 760-0218 Fax
<https://toittraining.com>



TOIT TRAINING LLC

- 69. Full Network Assessment Reviews
- 70. Development and Authorization of Network Changes
- 71. Unauthorized Changes
- 72. Computer Forensics
- 73. Chain of Evidence
- 74. Lesson 6: Environmental Exposures and Controls
- 75. Lesson 7: Physical Access Exposures and Controls
- 76. Physical Access Exposures
- 77. Physical Access Controls
- 78. Auditing Physical Access
- 79. Lesson 8: Mobile Computing
- 80. Module 05 Review
- 81. Course Closure
- 82. **Review Quiz (Number of attempts allowed: Unlimited)**

This course includes

- about 15.56 hours on-demand video
- 5 downloadable Pdf Workbooks
- Unlimited time access (During Membership)
- Access on mobile and Desktop
- Certificate of Completion

1001 Wilshire Boulevard #1071
Los, Angeles, CA 90017
support@toittraining.com
(909) 760-0217
(909) 760-0218 Fax
<https://toittraining.com>