Domain 1 — Information System Auditing Process

- How can we Plan an audit to determine whether information systems are protected, controlled, and provide value to the organization?
- How can we Conduct an audit in accordance with IS audit standards and a risk-based IS audit strategy?
- How can we Communicate audit progress, findings, results and recommendations to stakeholders?
- How can we Conduct audit follow-up to evaluate whether risk has been sufficiently addressed?
- How can we Evaluate IT management and monitoring of controls?
- How can we Utilize data analytics tools to streamline audit processes?
- How can we Provide consulting services and guidance to the organization in order to improve the quality and control of information systems?
- How can we Identify opportunities for process improvement in the organization's IT policies and practices?

Domain 2 – Governance & Management of IT

- How can we Evaluate the IT strategy for alignment with the organization's strategies and objectives?
- How can we Evaluate the effectiveness of IT governance structure and IT organizational structure?
- How can we Evaluate the organization's management of IT policies and practices?
- How can we Evaluate the organization's IT policies and practices for compliance with regulatory and legal requirements?
- How can we Evaluate IT resource and portfolio management for alignment with the organization's strategies and objectives?
- How can we Evaluate the organization's risk management policies and practices?
- How can we Evaluate IT management and monitoring of controls?
- How can we Evaluate the monitoring and reporting of IT key performance indicators (KPIs)?
- How can we Evaluate whether IT supplier selection and contract management processes align with business requirements?
- How can we Evaluate whether IT service management practices align with business requirements?
- How can we Conduct periodic review of information systems and enterprise architecture?
- How can we Evaluate data governance policies and practices?
- How can we Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives?
- How can we Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices?

Domain 3 – Information Systems Acquisition, Development, & Implementation

- How can we Evaluate whether the business case for proposed changes to information systems meet business objectives?
- How can we Evaluate the organization's project management policies and practices?
- How can we Evaluate controls at all stages of the information systems development life cycle?
- How can we Evaluate the readiness of information systems for implementation and migration into production?
- How can we Conduct post-implementation review of systems to determine whether project deliverables, controls and requirements are met?

- How can we Evaluate change, configuration, release, and patch management policies and practices?

Domain 4 – Information Systems Operations and Business Resilience

- How can we Evaluate the organization's ability to continue business operations?
- How can we Evaluate whether IT service management practices align with business requirements?
- How can we Conduct periodic review of information systems and enterprise architecture?
- How can we Evaluate IT operations to determine whether they are controlled effectively and continue to support the organization's objectives?
- How can we Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the organization's objectives?
- How can we Evaluate database management practices?
- How can we Evaluate data governance policies and practices?
- How can we Evaluate problem and incident management policies and practices?
- How can we Evaluate change, configuration, release, and patch management policies and practices?
- How can we Evaluate end-user computing to determine whether the processes are effectively controlled?

Domain 5 – Protection of Information Assets

- How can we Conduct audit in accordance with IS audit standards and a risk-based IS audit strategy?
- How can we Evaluate problem and incident management policies and practices?
- How can we Evaluate the organization's information security and privacy policies and practices?
- How can we Evaluate physical and environmental controls to determine whether information assets are adequately safeguarded?
- How can we Evaluate logical security controls to verify the confidentiality, integrity, and availability of information?
- How can we Evaluate data classification practices for alignment with the organization's policies and applicable external requirements?
- How can we Evaluate policies and practices related to asset life cycle management?
- How can we Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives?
- How can we Perform technical security testing to identify potential threats and vulnerabilities?
- How can we Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices?

Domain 1 – Information Security Governance

- Could you please Explain the need for and the desired outcomes of an effective information security strategy?
- Could you please Create an information security strategy aligned with organizational goals and objectives?
- How can you Gain stakeholder support using business cases?
- How can you Identify key roles and responsibilities needed to execute an action plan?
- How can you Establish metrics to measure and monitor the performance of security governance?

Domain 2 – Information Risk Management

- Could you please Explain the importance of risk management as a tool to meet business needs and develop a security management program to support these needs?
- How can you Identify, rank, and respond to a risk in a way that is appropriate as defined by organizational directives?
- How can you Assess the appropriateness and effectiveness of information security controls?
- How can you Report information security risk effectively**?**

Domain 3- Information Security Program Development and Management

- How effectively you Align information security program requirements with those of other business function?
- How do you Manage the information security program resources?
- How do you Design and implement information security controls ?
- How do you Incorporate information security requirements into contracts, agreements and third-party management processes?

Domain 4 – Information Security Incident Management

- Could you please confirm concepts and practices of Incident Management?
- How do you Identify the components of an Incident Response Plan and evaluate its effectiveness?
- How do you make the key concepts of Business Continuity Planning, or BCP and Disaster Recovery Planning, or DRP?
- Please confirm techniques commonly used to test incident response capabilities?

Domain 1 — Risk Management

- How do you Collect and review environmental risk data?
- How do you Identify potential vulnerabilities to people, processes and assets?
- How do you Develop IT scenarios based on information and potential impact to the organization
- Identify key stakeholders for risk scenarios?
- How do you Establish risk register?
- How do you Gain senior leadership and stakeholder approval of the risk plan?
- How do you Collaborate to create a risk awareness program and conduct training?

Domain 2 – IT Risk Assessment

- How do you Analyze risk scenarios to determine likelihood and impact?
- How do you Identify current state of risk controls and their effectiveness ?
- How do you Determine gaps between the current state of risk controls and the desired state ?
- How to Ensure risk ownership is assigned at the appropriate level ?
- How do you Communicate risk assessment data to senior management and appropriate stakeholders ?
- How do you Update the risk register with risk assessment data ?

Domain 3 – Risk Response and Mitigation

- How do you Align risk responses with business objectives?
- How to Develop consult with and assist risk owners with development risk action plans?
- How to Ensure risk mitigation controls are managed to acceptable levels?
- How to Ensure control ownership is appropriately assigned to establish accountability?
- How to Develop and document control procedures for effective control?
- How do you Update the risk register?
- How do you Validate that risk responses are executed according to risk action plans?

Domain 4 – Risk and Control Monitoring and Reporting

- How do you do Risk and control monitoring and reporting?
- Define key risk indicators (KRIs) and identify key performance indicators (KPIs) to enable performance measurement key risk indicators (KRIs) and key performance indicators (KPIs)?
- How do you Determine the effectiveness of control assessments?
- How do you Identify and report trends/changes to KRIs/KPIs that affect control performance or the risk profile ?

- Securing Unstructured Data - What You Don't Know Can & Will Hurt You
- Auditing Big Data Systems
- Data Sharing Risks and Controls
- Protect Your Data Against Insider Threats
- Assessing Data Governance at Nationwide
- Physical Data Security
- Agile, DevOps & Compliance
- Why Companies Fail PCI DSS Assessments and What to Do About It
- Blockchain & Cryptocurrency Emerging Regulations in the USA
- The New Privacy: GDPR, California Consumer Privacy Act, and the Future of Data Regulation (panel discussion)
- Incorporating Security Practices into Business Practices
- What Senior Executives (And Others) Want to See in Security KPIs
- How to Operationalize Cybersecurity: Turning Policy into Action
- Preparing for the Security Audit: Is Your ERP Ready?
- Review & Secure an Email Server
- Safeguarding Web Applications: A Different Perspective
- Using Network Forensic Techniques to Detect Threats
- Identifying Critical Flaws in Hardened Active Directory Environments
- An Auditor’s Guide to Incident Response Plans
- How Secure Are Your Vendors? Third Party Risk Management in Information Security
- Secure Cloud Solutions
- How to Ensure Vendor Compliance & the Mitigation of Third-Party Risks
- Cloud Insecurity: The Need for Stronger Identity Management
- SOC Reports: Reducing the Risk of Service Providers
- AWS for Auditors

CPE on Demand: Data Security

Your bundle includes the following sessions:

- Securing Unstructured Data - What You Don't Know Can & Will Hurt You
- Auditing Big Data Systems
- Data Sharing Risks and Controls
- Protect Your Data Against Insider Threats
- Assessing Data Governance at Nationwide
- Physical Data Security

CPE on Demand: Emerging GRC Challenges
Your bundle includes the following sessions:

- Agile, DevOps & Compliance
- Why Companies Fail PCI DSS Assessments and What to Do About It
- Blockchain & Cryptocurrency Emerging Regulations in the USA
- The New Privacy: GDPR, California Consumer Privacy Act, and the Future of Data Regulation (panel discussion)

CPE on Demand: Security Practices for Business
Your bundle includes the following sessions:

- Incorporating Security Practices into Business Practices
- What Senior Executives (And Others) Want to See in Security KPIs
- How to Operationalize Cybersecurity: Turning Policy into Action
- Preparing for the Security Audit: Is Your ERP Ready?

CPE on Demand: Technical Security Insights
Your bundle includes the following sessions:

- Review & Secure an Email Server
- Safeguarding Web Applications: A Different Perspective
- Using Network Forensic Techniques to Detect Threats
- Identifying Critical Flaws in Hardened Active Directory Environments
- An Auditor's Guide to Incident Response Plans

CPE on Demand: Third-Party Services
Your bundle includes the following sessions:

- How Secure Are Your Vendors? Third Party Risk Management in Information Security
- Secure Cloud Solutions
- How to Ensure Vendor Compliance & the Mitigation of Third-Party Risks
- Cloud Insecurity: The Need for Stronger Identity Management
- SOC Reports: Reducing the Risk of Service Providers
- AWS for Auditors

1 Domain 01—Security and Risk Management

- 2 Objectives
- 3 Importance of Information Security and Risk Management0
- 4 Role and Importance of CIA in ISM
- 5 Confidentiality
- 6 Integrity
- 7 Availability
- 8 Information Security
- 9 Information Security Management
- 10 Information Security Governance
- 11 IT Security and Organizational Goals, Mission, and Objectives
- 12 Goals, Mission, and Objectives
- 13 Aligning Security with Goals, Mission, and Objectives
- 14 Business Scenario
- 15 Organizational Processes
- 16 Auditing
- 17 Control Framework
- 18 Due Care
- 19 Due Diligence
- 20 Security Controls
- 21 Service Level Agreements
- 22 Managing Third - Party Governance
- 23 Offshoring Privacy Requirements and Compliance
- 24 Business Scenario
- 25 Layers of Responsibility
- 26 Security Policies
- 27 Types of Security Policies
- 28 Security Policy Implementation
- 29 Policy Chart
- 30 Standards, Guidelines, Procedures, and Baselines
- 31 Business Scenario
- 32 Compliance—Need for Compliance
- 33 Regulatory Compliance
- 34 Compliance
- 35 Compliance (contd.)
- 36 Compliance (contd.)
- 37 Standards/Manuals/Guidelines for Compliance
- 38 Computer Crimes
- 39 Introduction to Computer Crimes
- 40 Categories of Computer Crimes
- 41 Business Scenarios
- 42 Major Legal Systems
- 43 Common Law and Civil Law
- 44 Customary Law and Religious Law0
- 45 Mixed Law
- 46 Business Scenario
- 47 Introduction to Intellectual Property (IP) Law
- 48 Types of Intellectual Property (IP) Law
- 49 Types of Intellectual Property (IP) Law (contd.)

- 50 Types of Intellectual Property (IP) Law (contd.)
- 51 Business Scenario
- 52 Import or Export Controls and Trans - Border Data Flow
- 53 Introduction to Privacy
- 54 U.S. Privacy Laws
- 55 U.S. Privacy Laws (contd.)
- 56 U.S. Guidelines for Managing Privacy
- 57 EU Council Directive (Law) on Data Protection
- 58 The U.S.-European Union Safe Harbor
- 59 Security Definitions
- 60 Information Risk Management
- 61 Business Scenario
- 62 Introduction to Risk Analysis
- 63 Goals of Risk Analysis
- 64 Risk Analysis Team
- 65 Steps for Risk Analysis
- 66 Information and Assets Valuation
- 67 Risk Analysis Types
- 68 Quantitative Risk Analysis—Steps
- 69 Quantitative Risk Analysis—Problem
- 70 Qualitative Risk Analysis
- 71 Delphi Technique
- 72 Quantitative vs.Qualitative
- 73 Hybrid Analysis
- 74 Countermeasure Selection—Problem
- 75 Countermeasure Selection—Other Factors
- 76 Handling Risk
- 77 Business Scenario
- 78 Threat Modeling
- 79 Need for Business Continuity Planning
- 80 Basic Concepts—Disruptive Events
- 81 Basic Concepts—Business Continuity Planning
- 82 Importance of Business Continuity Planning
- 83 Business Continuity Planning Phases
- 84 BCP/DRP Phase 1—Project Initiation and Scoping
- 85 BCP/DRP Phase 2—Business Impact Analysis (BIA)
- 86 BIA—Goals
- 87 BIA—Steps
- 88 BIA Steps—Business Unit Level
- 89 Maximum Tolerable Downtime (MTD)
- 90 Failure and Recovery Metrics
- 91 Failure and Recovery Metrics (contd.)
- 92 Stages of Failure and Recovery
- 93 BCP/DRP Phase 3—Identify Preventive Controls
- 94 Importance of Managing Personnel Security
- 95 Managing Personnel Security—Hiring Practices
- 96 Managing Personnel Security—Employee Termination
- 97 Vendor, Contractors, and Consultant Controls

- 98 Best Work Practices
- 99 Business Scenario
- 100 Importance of Security Awareness Training
- 101 Security Awareness Training: Awareness, Training, and Education
- 102 Implementation of Security Awareness Training Program
- 103 Importance of Content Updates
- 104 Importance of Managing Security Function
- 105 Best Practices—Budget and Establish Security Metrics
- 106 Best Practices—Resources and Develop and Implement Strategies
- 107 Best Practices—Completeness and Effectiveness of the Program
- 108 Business Scenario
- 109 (ISC)² Code of Ethics
- 110 Quiz
- 111 Summary
- 112 Conclusion
- 1 Domain 02 Asset Security
- 2 Objectives
- 3 Importance of Asset Security
- 4 Need for Information Classification
- 5 Information Classification Objectives
- 6 Government or Military Sector Classification
- 7 Commercial or Private Sector Classification
- 8 Information Classification Criteria
- 9 Data Classification Considerations
- 10 Role Responsible for Data Classification
- 11 Business Scenario
- 12 Data Management
- 13 Best Practices for Data Management
- 14 Data Policy
- 15 Data Ownership
- 16 Data Ownership Best Practices
- 17 Data Custodians
- 18 Data Custodians (contd.)
- 19 Data Quality
- 20 Data Quality—Aspects
- 21 Data Quality Assurance and Quality Control
- 22 Data Documentation
- 23 Data Documentation Practices
- 24 Data Standards
- 25 Data Control Lifecycle
- 26 Data Specification and Modeling
- 27 Database Maintenance
- 28 Data Audit
- 29 Data Storage and Archiving
- 30 Data Security
- 31 Data Access, Sharing, and Dissemination
- 32 Data Publishing
- 33 Data Handling Requirements

- 34 Media Resource Protection
- 35 Data Remanence
- 36 Business Scenario
- 37 Asset Management
- 38 Software Licensing
- 39 Equipment Lifecycle
- 40 Protecting Privacy
- 41 Ensuring Appropriate Retention
- 42 Data Security Controls
- 43 Data in Transit—Best Practices
- 44 Scoping and Tailoring
- 45 Scoping and Tailoring (contd.)
- 46 Standards Selection—US DoD
- 47 Standards Selection—International Standards
- 48 Standards Selection National Cyber Security Framework Manual
- 49 Standards Selection Center for Strategic and International Studies
- 50 Standards Selection Critical Security Controls
- 51 Standards Selection Security Content Automation Protocol0
- 52 Framework for Improving Critical Infrastructure Cybersecurity
- 53 Business Scenario

1 Domain 03 Security Engineering

- 2 Objectives
- 3 Security Architecture and Design - Case Study
- 4 Security Engineering
- 5 Architecture Framework
- 6 Zachman Framework
- 7 TOGAF
- 8 ITIL
- 9 Creating a Security Architecture
- 10 Enterprise Security Architecture
- 11 Common Security Services in ESA
- 12 SABSA Framework
- 13 SABSA Matrix
- 14 Business Scenario
- 15 ISO/IEC 27001:2013 Security Standards
- 16 ISO/IEC 27002 Code of Practice for Information Security Management
- 17 Security Models
- 18 State Machine Model
- 19 Multilevel Security Models
- 20 Matrix-Based Model
- 21 Non-Interference Model
- 22 Information flow model
- 23 Examples of Security Models: Bell–LaPadula Confidentiality Model
- 24 Examples of Security Models: Biba Integrity Model
- 25 Examples of Security Models: Clark–Wilson integrity model
- 26 Brewer Nash, Graham Denning, and Harrison Ruzzo Ullman models
- 27 Business Scenario
- 28 Evaluation Criteria

- 29 CSEC
- 30 Information Technology Security Evaluation Criteria0
- 31 Common Criteria
- 32 Common Criteria Evaluation Process
- 33 Common Criteria Levels
- 34 Payment Card Industry Data Security Standard
- 35 Certification and Accreditation
- 36 Certification and Accreditation Standards
- 37 SEI—CMMI0
- 38 SEI—CMMI Levels
- 39 Business Scenario
- 40 System Security Architecture
- 41 Mainframes and Other Thin Client Systems
- 42 Middleware and Embedded Systems
- 43 Pervasive Computing and Mobile Computing Devices
- 44 System Components Processors
- 45 System Components Memory
- 46 System Components Storage
- 47 System Components Trusted Computing Base (TCB)
- 48 System Components Reference Monitor
- 49 System Components—Trusted Platform Module (TPM)
- 50 System Components Peripherals and Other Input/Output Devices
- 51 System Components Operating System
- 52 System Components Ring Model
- 53 System Components System Kernel
- 54 Distributed Systems
- 55 Virtualization
- 56 Hypervisor
- 57 Cloud Computing
- 58 Service models
- 59 Grid Computing
- 60 Peer to Peer Networking (P2P)
- 61 Business Scenario
- 62 Security Threats and Countermeasures
- 63 Assessing and Mitigating Vulnerabilities and Threats
- 64 Assessing and Mitigating Vulnerabilities and Threats (contd.)
- 65 Assessing and Mitigating Vulnerabilities and Threats (contd.)
- 66 Best Practices
- 67 Best Practices (contd.)
- 68 Best Practices Techniques and Technologies
- 69 Best Practices Techniques and Technologies (contd.)
- 70 Best Practices Techniques and Technologies (contd.)
- 71 Best Practices Techniques and Technologies (contd.)
- 72 Best Practices Techniques and Technologies (contd.)
- 73 Introduction to Cryptography
- 74 Cryptographic Lifecycle
- 75 Algorithm or Protocol Governance
- 76 Cryptography Terms

- 77 Strength of a Cryptosystem
- 78 Cryptography Methods Substitution Cipher
- 79 Cryptography Methods Transposition Cipher
- 80 Cryptography Methods Book or Running Key Cipher
- 81 Cryptography Methods Concealment Cipher
- 82 Cryptography Methods Steganography and DRM
- 83 Business Scenario
- 84 Introduction to Symmetric Cryptography
- 85 Symmetric Key Ciphers
- 86 Block Cipher
- 87 Stream Cipher
- 88 Block Cipher Designs
- 89 Data Encryption Standard (DES)
- 90 DES Algorithm0
- 91 DES Operation Modes Electronic Code Book
- 92 DES Operation Modes Cipher Block Chainins
- 93 DES Operation Modes Cipher Feed Back
- 94 DES Operation Modes Output Feed Back
- 95 DES Operation Modes—Counter
- 96 Triple DES0
- 97 Advanced Encryption Standard (AES)0
- 98 AES Algorithm
- 99 AES Algorithm Key Expansion and Initial Round
- 100 Advanced Encryption Standard (AES) Algorithm—Rounds
- 101 AES Algorithm Final Round
- 102 Other Symmetric Systems
- 103 Other Symmetric Systems (contd.)
- 104 Business Scenario
- 105 Introduction to Asymmetric Cryptography
- 106 Introduction to Asymmetric Cryptography Diagram
- 107 Introduction to RSA Algorithm
- 108 RSA Algorithm Process
- 109 Other Types of Asymmetric Cryptography Elliptic Curve Cryptosystems
- 110 Other Types of Asymmetric Cryptography Diffie-Hellman Key Exchange
- 111 Public Key Cryptography
- 112 Symmetric vs. Asymmetric Cryptography
- 113 Advantages and Disadvantages
- 114 Introduction to Public Key Infrastructure
- 115 PKI Certification0
- 116 PKI Certification (contd.)
- 117 PKI Steps—Part 1
- 118 PKI Steps—Part 2
- 119 One-Way Hash
- 120 Hashing Algorithms
- 121 Hashing Algorithms (contd.)
- 122 Salting
- 123 Message Authentication Code (MAC)
- 124 Digital Signatures

- 26 Private Networks and Loopback Address
- 27 Types of IP Addressing
- 28 Routed and Routing Protocols
- 29 Types of Network Protocols
- 30 Transmission Control Protocol (TCP)
- 31 User Datagram Protocol (UDP)
- 32 Internet Protocol
- 33 Address Resolution Protocol
- 34 Internet Control Message Protocol (ICMP)
- 35 Hypertext Transfer Protocol (HTTP)
- 36 Implications of Multi-Layer Protocols
- 37 Distributed Network Protocol
- 38 LAN/Network Technologies
- 39 Transmission Media
- 40 Twisted Pair
- 41 Coaxial Cable Box
- 42 Fiber-Optic Cable Box
- 43 Network Topologies
- 44 Media Access Technologies
- 45 Carrier-Sense Multiple Access with Collision Detection
- 46 Carrier-Sense Multiple Access with Collision Avoidance
- 47 Flavors of LAN transmission methods
- 48 List of Networking Devices
- 49 VLANs
- 50 Gateways
- 51 Network Access Control Devices
- 52 Packet-Filtering and Application-Level
- 53 Circuit-Level and Stateful-Inspection
- 54 Firewall Architectures
- 55 Network Security Terms
- 56 Business Scenario
- 57 Networks
- 58 Types of Networks
- 59 WAN Technologies
- 60 WAN Switching and Devices
- 61 Network Address Translation and Frame Relay
- 62 Multi-Protocol Label Switching and VoIP
- 63 Fiber Channel over Ethernet and Internet Small Computer System Interface
- 64 Virtualized Networks
- 65 Introduction to Remote Access
- 66 VPN using PPTP and L2TP
- 67 Internet Security Protocol (IPsec)
- 68 Internet Security Protocol (IPsec) Modes of Operation
- 69 IPsec Security Protocols—Authentication Header (AH)
- 70 IPsec Security Protocols—Encapsulating Security Payload (ESP)
- 71 Components of the IPsec Process
- 72 Components of the IPsec Process (contd.)
- 73 IPsec Process

- 74 Secure Access Protocols
- 75 Secure Access Protocols (contd.)
- 76 Secure Access Protocols (contd.)
- 77 Remote Access Security Methods
- 78 Multimedia Collaboration
- 79 Wireless Technologies
- 80 IEEE Wireless Standards and Spread-Spectrum Technologies
- 81 Direct Sequence Spread Spectrum and Frequency-Hopping Spread Spectrum
- 82 WLAN Operational Modes
- 83 Bluetooth
- 84 Bluetooth Attack
- 85 Blue Jacking and Blue Snarfing
- 86 Blue Bugging, Backdoor Attacks, and Denial of Service Attacks
- 87 Wireless Security
- 88 Business Scenario
- 89 Network Attacks
- 90 Network Attacks (contd.)
- 91 Network Attacks—Countermeasures

Domain 05 - Identity and Access Management

- 1 Domain 05—Identity and Access Management
- 2 Objectives
- 3 Importance of Identity and Access Management in Information Security
- 4 Controlling Physical and Logical Access to Assets
- 5 Controlling Physical and Logical Access to Assets (contd.)
- 6 Access Subject Object and Access control
- 7 Identity and Access Management Policy
- 8 Identification Authentication and Authorization
- 9 Identity Management
- 10 Identity and Access Provisioning Lifecycle
- 11 Identity and Access Provisioning Lifecycle (contd.)
- 12 Guidelines for User Identification
- 13 Verifying Identification Information
- 14 Strong Authentication
- 15 Biometrics—Characteristics
- 16 Types of Biometrics
- 17 FRR FAR CER
- 18 Passwords
- 19 Password Types
- 20 Tokens
- 21 Token Device—Synchronous
- 22 Token Device—Asynchronous
- 23 Memory Cards and Smart Cards
- 24 Attacks on Smart Cards—Fault Generation and Micro-Probing
- 25 Access Criteria
- 26 Authorization Concepts
- 27 Identity Management Implementation
- 28 Password Management
- 29 Directory Management

- 30 Directory Technologies
- 31 Accounts Management
- 32 Profile Management
- 33 Web Access Management
- 34 Single Sign-On (SSO)
- 35 SSO Technologies
- 36 Kerberos
- 37 Kerberos Steps
- 38 Problems with Kerberos
- 39 Business Scenario
- 40 Access Control Types—Security Layer
- 41 Access Control Types—Functionality
- 42 Business Scenaris
- 43 Access Control Models—DAC
- 44 Access Control Models—MAC
- 45 Access Control Models—RBAC
- 46 Business Scenario
- 47 Access Control Concepts
- 48 Types of Access Control Administration
- 49 Remote Authentication Dial-In User Service (RADIUS)
- 50 TACACS and TACACS
- 51 DIAMETER
- 52 Accountability
- 53 Accountability (contd.)
- 54 Session Management
- 55 Registration and Proof of Identity
- 56 Credential Management Systems
- 57 Credential Management Systems—Risks and benefits
- 58 Federated Identity Management
- 59 Federated Identity Management Models
- 60 Federated Identity Management Models (contd.)
- 61 Federated Identity Management Models (contd.)
- 62 Identity as a Service
- 63 Identity as a Service—Functionality
- 64 Identity as a Service—Possible Issues
- 65 Integrate Third-Party Identity Services
- 66 Integrate Third-Party Identity Services (contd.)
- 67 Unauthorized Disclosure of Information
- 68 Threats to Access Control
- 69 Protection against Access Control Attacks
- 70 Access Control Best Practices
- 71 Access Control Best Practices (contd.)

Domain 06 - Security Assessment and Testing

- 1 Domain 06—Security Assessment and Testing
- 2 Objectives
- 3 Security Assessment and Testing—Introduction
- 4 Assessment and Test Strategies
- 5 Vulnerability Assessment

- 6 Penetration Testing
- 7 Log Management
- 8 Log Management—Advantages and Challenges
- 9 Log Management—Best Practices
- 10 Log Management—Operational Process
- 11 Logged Events
- 12 Synthetic Transactions
- 13 Reasons to Use Synthetic Transactions
- 14 Code Review and Testing
- 15 Testing Techniques
- 16 Security Testing in the SDLC
- 17 Software Product Testing Levels
- 18 Misuse Case Testing
- 19 Misuse Case Testing—Scenarios
- 20 Test Coverage Analysis
- 21 Interface Testing
- 22 API Testing (contd.
- 23 Interface Testing (contd.)
- 24 GUI Testing
- 25 Common Software Vulnerabilities
- 26 Business Scenario
- 27 Information Security Continuous Monitoring
- 28 Information Security Continuous Monitoring—Strategy and Process
- 29 Risk Evaluation and Control—Metrics
- 30 Security Controls Monitoring Frequencies
- 31 ISCM—Benefits
- 32 Key Performance and Risk Indicators
- 33 Internal and Third Party Audits
- 34 Audit Frequency and Scope
- 35 Statement on Auditing Standards No. 700
- 36 Service Organization Controls
- 37 SOC 1 Report
- 38 SOC 2 Report
- 39 SOC 2 Reports (contd.)
- 40 SOC 3 Report
- 41 SOC 1, SOC 2, and SOC 3 Comparison
- 42 Audit Process—Audit Preparation Phase
- 43 Audit Process—Audit Phases
- 44 Business Scnarios

Domain 07 - Security Operations

- 1 Domain 07—Security Operations
- 2 Objectives
- 3 Importance of Security Operations—Case Study
- 4 Introduction to Investigations
- 5 Investigation Challenges
- 6 Investigations—Primary Activities
- 7 Crime Scene
- 8 Forensic Investigation Guidelines

- 9 Incident Response Terminologies
- 10 Incident Response Goals
- 11 Incident Response Team
- 12 Incident Response Procedures
- 13 Incident Response Procedures (contd.)
- 14 Incident Response Procedures (contd.)
- 15 Incident Response Procedures (contd.)
- 16 Business Scenario
- 17 Evidence
- 18 Evidence Lifecycle
- 19 Chain of Evidence
- 20 Types of Evidence
- 21 Computer Forensics Procedure
- 22 Requirements for Investigation Types
- 23 Logging and Monitoring Activities
- 24 Intrusion Detection System
- 25 Intrusion Prevention System
- 26 Security Information and Event Management (SIEM)
- 27 Security Information and Event Management (SIEM)—Characteristics
- 28 Continuous Monitoring
- 29 Egress Filtering
- 30 Data Leak or Loss Prevention (DLP)
- 31 Steganography and Digital Watermarking
- 32 Business Scenario
- 33 Secure Provisioning of Resources through Configuration Management
- 34 Secure Provisioning of Resources through Configuration Management (contd.
- 35 Introduction to Security Operations
- 36 Security Operations Concepts
- 37 Security Operations
- 38 Effects of Operations Controls on C.I.A.
- 39 Business Scenario
- 40 Operational Resilience
- 41 Threats to Operations
- 42 Threats to Operations (contd.)
- 43 Vulnerabilities
- 44 Controls
- 45 Business Scenario
- 46 Need for Controlling Privileged Accounts
- 47 Identity and Access Management
- 48 Types of Accounts
- 49 Commonly Used Roles
- 50 Commonly Used Roles (contd.)
- 51 Monitoring Special Privileges
- 52 Service Level Agreements (SLAs)
- 53 Business Scenario
- 54 Protect Valuable Assets
- 55 Protecting Physical Assets
- 56 Protecting Information Assets

- 57 Protecting Resources
- 58 Controls for Protecting Assets—Hardware Controls
- 59 Controls for Protecting Assets—Software Controls
- 60 Controls for Protecting Assets—Media Controls
- 61 Controls for Protecting Assets—Administrative Controls
- 62 Cloud and Virtual Storage
- 63 Cloud and Virtual Storage Security Issues
- 64 Types of Virtualized Storage
- 65 Hard Copy Records
- 66 Business Scenario
- 67 Incident Management
- 68 Security Measurements, Metrics, and Reporting
- 69 Managing Security Technologies
- 70 Incident Management—Detection Phase
- 71 Intrusion Detection System
- 72 Security Information Event Management (SIEM)
- 73 Anti-Malware Systems
- 74 Monitoring Techniques—Violation Analysis
- 75 Incident Management—Other Phases
- 76 Trusted Recovery and System Recovery
- 77 Problem Management
- 78 Operating and Maintaining Preventive Measures
- 79 Patch Management
- 80 Vulnerability Management
- 81 Change Management
- 82 Change Control Process
- 83 Configuration Management
- 84 Configuration Management (contd.)
- 85 Business Scenario
- 86 Develop a Recovery Strategy
- 87 Types of Recovery—Business Recovery and Facility and Supply Recovery
- 88 Types of Recovery—User Recovery
- 89 Types of Recovery—Operational Recovery
- 90 Recovery Partners Strategy
- 91 Backup Sites
- 92 Backup Sites (contd.)
- 93 Backup Sites (contd.)
- 94 Backup Methods
- 95 Importance of Maintaining Resilient Systems
- 96 Redundancy and Fault Tolerance
- 97 Redundancy and Fault Tolerance Methods
- 98 Redundancy and Fault Tolerance Methods (contd.)
- 99 Best Practices for Backup and Recovery
- 100 Business Scenario
- 101 Disaster Recovery—Planning Design and Development
- 102 Planning Design and Development—Step 1 and Step 2
- 103 Planning Design and Development—Step 3 and Step 4
- 104 Disaster Recovery Phases—Implementation, Testing, and Training

- 105 Importance of Testing
- 106 Types of Testing
- 107 Types of Testing (contd.)
- 108 Types of Testing (contd.)
- 109 Training
- 110 Disaster Recovery Phases—Maintenance
- 111 Disaster Recovery Phases—Maintenance (contd.)
- 112 Business Scenario
- 113 Perimeter Security
- 114 Barriers
- 115 Fences
- 116 Gates
- 117 Walls and Bollards
- 118 Perimeter Intrusion Detection
- 119 Business Scenario
- 120 Importance of Lighting
- 121 Types of Lighting Systems
- 122 Types of Lights
- 123 Access Control
- 124 Types of Access Control Systems
- 125 Business Scenario
- 126 Building and Inside Security
- 127 Personnel Security
- 128 Business Scenario

Domain 08 - Software Development Security

- 1 Domain 08 - Software Development Security
- 2 Objectives
- 3 Importance of Software Development Security
- 4 System Environments
- 5 Distributed Environment
- 6 Client/Server Systems and Local Environment
- 7 Distributed Data Processing and Agents
- 8 Applets
- 9 Programming Concepts
- 10 Complier Vs Interpreter
- 11 Programming and Software
- 12 Threats in the Software Environment
- 13 Threats in the Software Environment (contd.)
- 14 Threats in the Software Environment (contd.)
- 15 Threats in the Software Environment (contd.)
- 16 Threats in the Software Environment (contd.)
- 17 Threats in the Software Environment (contd.)
- 18 Business Scenario
- 19 System Life Cycle and Systems Development
- 20 Systems Development Life Cycle
- 21 SDLC—Operation and Maintenance
- 22 Integrated Product Team (IPT)
- 23 DevOps

- 24 Software Testing Methods
- 25 Software Testing Levels
- 26 Application Controls
- 27 Software Development Methods
- 28 Software Development Methods (contd.)
- 29 Software Development Methods (contd.)
- 30 Software Development Methods (contd.)
- 31 Software Development Methods (contd.)
- 32 Java Security
- 33 Secure Software Development Best Practices
- 34 Business Scenario
- 35 Object - Oriented Programming Terms
- 36 Object - Oriented Programming Terms (contd.)
- 37 Object-Oriented Programming—Definition
- 38 Distributed Object-Oriented Systems
- 39 Object Request Brokers
- 40 COM—Component Object Model
- 41 DCOM—Distributed Component Object Model
- 42 CORBA—Common Object Request Broker Architecture
- 43 Software Security and Assurance
- 44 Software Security and Assurance (contd.)
- 45 Software Security and Assurance (contd.)
- 46 Software Security and Assurance (contd.)
- 47 Software Security and Assurance (contd.)
- 48 Software Security and Assurance (contd.)
- 49 Software Security and Assurance (contd.)
- 50 Software Security and Assurance (contd.)
- 51 Software Security and Assurance (contd.)
- 52 Software Security and Assurance (contd.)
- 53 Software Security and Assurance (contd.)
- 54 Software Security and Assurance (contd.)
- 55 Software Security and Assurance (contd.)
- 56 Software Security : XML and Security Assertion Markup Language
- 57 Software Security: SOA
- 58 Audit and Assurance Mechanisms
- 59 Assessing the Effectiveness of Software Security
- 60 Assessing the Effectiveness of Software Security (contd.)
- 61 Assessing the Security Impact of Acquired Software
- 62 Code Repositories and Application Programming Interfaces
- 63 Business Scenario
- 64 Database and Data Warehousing Environments
- 65 Database Terms
- 66 Types of Databases
- 67 Types of Databases (contd.)
- 68 Types of Databases (contd.)
- 69 Types of Databases (contd.)
- 70 Types of Databases (contd.)
- 71 Database—Threats and Vulnerabilities

- 72 Introduction to Data Warehousing
- 73 Data Warehousing Concepts
- 74 Database Normalization
- 75 DBMS Controls
- 76 Business Scenario
- 77 Malwares—Types
- 78 Malware Protection
- 79 Business Scenario
- 80 Importance and Role of Knowledge Management
- 81 Knowledge-Based System/Artificial Intelligence
- 82 Knowledge-Based System—Expert System
- 83 Knowledge-Based System—Neural Network
- 84 Web Application Environment—Threats and Vulnerabilities
- 85 Web Application Environment Security
- 86 Web Application Environment Security (contd.)
- 87 Web Application Environment Security (contd.)
- 88 Web Application Environment Security (contd.)
- 89 The Ten Best Practices for Secure Software Development—(ISC)2