MIT(CS)-201

Information Security Assurance : Framework, standards and Industry best practices

Block-I

UNIT-I

UNIT I: INFORMATION SECURITY STANDARDS

INTRODUCTION, Elements of Information Security Policy, INFORMATION SECURITY STANDARDS, ISO/IEC 27001:2013 (Information Security Management System), Structure of the standard, Changes from the 2005 standard, New controls in 27001:2013, Controls, ISO/IEC 27002:2013 (Code of Practice for Information Security Management), Outline for ISO27002:2005, Implementation example of ISO/IEC 27002, Career path with ISMS ISO27001:2013, Bullets to improve security posture of organization, From network protection point of view, From data protection point of view.

UNIT II: INFORMATION SECURITY REGULATIONS

INTRODUCTION, Regulations related to Information Security- SOX, IT ACT, Against an Individual, Individual Property, Against Organisation, Against Society at Large, Amendments, SARBANES-OXLEY ACT (SOX), Background about SOX, Why SOX was born?, Key requirements/provisions, What should SOX implementers do in real-time?, PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS), CHILDRES'S ONLINE PRIVACY PROTECTION ACT (COPPA), HIPPA, GLBA, FISMA, Purpose for FISMA, FIPS, FFIEC, CYBER SECURITY, SECURITY CONTROLS, Information security standards and control frameworks, International information security standards, U.S. Federal Government information security standards, COMMON PITFALLS OF INFORMATIN SECURITY PROGRAM, COMMON ELEMENTS OF COMLPINANCE .

Unit III: Industry best practices

ISO/IEC 15408 (EVALUATIN CRITERIA FOR IT SECURITY), Target of Evaluation (TOE), How do the Common Criteria work?, ISO/IEC 13335 (IT SECURITY MANAGEMENT), PAYMENT CARD INDUSTRY DATA SECURITY STANDATDS (PCI DSS), About PCI History, Requirement of PCI, Best Practices for Implementing PCI DSS into Business-as-Usual Processes, COBIT, DOMAINS, ITIL (OR ISO/IEC 20000 SERIES), ITIL(Information Technology Infrastructure Library), Changes and characteristics of the 2011 edition of ITIL, Services Desk, What ITIL is not?.

UNIT IV: INDUSTRY BEST PRACTICES

NIST, Scope/Objective, NIST-SP800-50 (Building an Information Technology Security Awareness and Training Program), NIST-SP800-50 (Building an Information Technology Security Awareness and Training Program), Risk Assessment methodology described in SP 800-30, SANS (SysAdmin, Audit, Networking, and Security), Computer Security Training & Certification, Information Security Research, OWASP (OPEN WEB APPLICATION SECURITY PROJECT), Code of Ethics, Projects, Partial project list, Principles, OWASP Top Ten (Widely used Methodology), What is OWASP Top Ten, What are Application Security Risks?, OWASP Top 10 Application Security Risks – 2010, A1-Injection, A2-Cross Site Scripting (XSS) A3-Broken Authentication and Session Management, A4-Insecure Direct Object References, A5-Cross Site Request Forgery (CSRF), A6-Security Misconfiguration, A7-Insecure Cryptographic Storage, A8-Failure to Restrict URL Access, A9-Insufficient Transport Layer Protection, A10-Unvalidated Redirects and Forwards, OWASP Top 10 Application Security Risks –2007, 2010 and 2013.

Block- II

UNIT I: MANAGING INFORMATION SECURITY

INTRODUCTION, INFORMATION SECURITY MANAGEMENT SYSTEM, ISMS PLANNING, ISMS documentation, Asset identification, Risk assessment, Risk Treatment Plan, ISMS DOCUMENTATION, Context, Scope and Information Security Policy, Statement of Applicability (SoA), Mandatory documents and records required by ISO 27001:2013, Non-mandatory documents- ISO 27001:2013, INFORMATION SECURITY POLICY, Hierarchical policy scheme, Policy Development, PLAN-DO-CHECK-DO (PDCA) CYCLE, ISO/IEC 27001 - PDCA Cycle.

UNIT II: INFORMATION SECURITY MANAGEMENT SYSTEM - ISO STANDARDS

INTRODUCTION, BENEFITS OF INTERNATIONAL STANDARDS, STANDARDS DEVELOPMENT, POPULAR ISO STANDARDS, ISO/IEC 27001 - Information security management, ISO 9000 - Quality management, ISO 14000 - Environmental management, Country Codes - ISO 3166, ISO 50001 - Energy management, ISO 22000 - Food safety management, ISO 31000 - Risk management, Related Standards, Language codes - ISO 639, ISO 27K SERIES OF STANDARDS, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC TR 27008, ISO/IEC 27010, ISO/IEC 27011, ISO/IEC 27013, ISO/IEC 27014, ISO/IEC 27015, ISO/IEC TR 27016, ISO/IEC 27031, ISO/IEC 27032, ISO/IEC 27033, ISO/IEC 27034, ISO/IEC 27035, ISO/IEC 27036, ISO/IEC 27037, ISO/IEC 27038.

UNIT III: ISO/IEC 27001 AND 27002 FOR INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

INTRODUCTION, ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, Structure and format of ISO/IEC 27002:2013, Contents of ISO/IEC 27002:2015, ISO/IEC 27001 CERTIFICATION PROCESS, NIST CYBER SECURITY FRAMEWORK AND ISO 27001.

UNIT IV: INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) AUDITING

INTRODUCTION, CONCEPT OF AUDITING, Type of Audits, Purpose of Auditing, ISMS Auditing, AUDIT ACTIVTIES, ISMS INTERNAL AUDIT, GUIDELINES FOR AUDITORS/AUDITING ORGANIZATIONS, People or Auditors, Technical, Process, GUIDELINES FOR AUDITEE, Audit components and characteristics, Auditor Organization Responsibilities, Auditee Organization Responsibilities, Auditee expectations, General guidelines, Technical Competence of the auditing team, Relationship auditee & auditor

BLOCK III

UNIT I: SECURITY AUDIT

SECURITY AUDIT, The audit process, Audit Planning & Preparation, Establishing audit objectives, Performing the review, Issuing the review report, THE AUDITED SYSTEMS, Encryption and IT audit, Logical security audit, Physical security audit, Security Audit Checklist, Specific tools used in network security, SECURITY AUDIT STANDARDS, COBIT-Control Objectives for Information and related Technology, FISCAM (Federal Information Systems Control Audit Manual), ISO: 17799, Outline for ISO27002:2013, Outline for ISO27002:2005, HIPAA-Health Insurance Portability and Accountability Act Of 1996, Sarbanes Oxley Act of 2002, History of SOX, SOX Act & Healthcare, Major elements, AUDITING APPLICATION SECURITY, Segregation of duties, Computer Assisted Audit Techniques, SECURITY AUDIT PLANNING, Previous audit results, Site surveys and questionnaire, Consult with the client, Entry Briefing, Security Audit Fieldwork, Interviews, Software tools and system logs, Network Discovery, Vulnerability Assessment, Analysis, SECUITY AUDIT REPORTING, AUDIT EVENT REPORTING, Traditional Logging, Modern Auditing Services.

UNIT II: INFORMATION SECURITY

INTRODUCTION, WHY IS INFORMATION SECURITY IMPORTANT, WHAT IS INFORMATION?, DEFINITIONS, KEY CONCEPTS, Confidentiality, Integrity, Availability, Non-repudiation, RISK MANAGEMENT, CONTROLS, Administrative, Logical, Physical, DEFENSE IN DEPTH, SECURITY CLASSIFICATION FOR INFORMATION, ACCESSCONTROL, Identification, Authentication, Authorization, PROTECTING COMPANY INFORMATION, Taking Action as a User, Taking Action as an Organization, Frameworks, Standards, and Compliance, CRYPTOGRAPHY, THE PURPOSE OF CRYPTOGRAPHY, TYPES OF CRYPTOGRAPHIC ALGORITHMS, Secret Key Cryptography, Public-Key Cryptography, Hash Functions, PROCESS, Security governance, Incident response plans,

Change management, BUSINESS CONTINUITY, Disaster recovery planning, LAWS AND REGULATIONS.

UNIT III: DISASTER RECOVERY

INTRODUCTION, THE DEVELOPMENT OF DISASTER RECOVERY, What is Disaster recovery Plan?, Importance of Disaster Recovery Plan, Don't ignore it until it's too late, Benefits, CLASSIFICATION OF DISASTERS, Natural disasters and Man-made disasters, Man-made Disasters, RELATIONSHIP TO THE BUSINESS CONTINUITY PLAN, IT DISASTER RECOVERY CONTROL MEASURES, DISASTER RECOVERY PLANNING METHODOLOGY, Obtaining top management commitment, Establishing a planning committee, Performing a risk assessment, Establishing priorities for processing and operations, Determining recovery strategies, Collecting data, Organizing and documenting a written plan, Developing testing criteria and procedures, Testing the plan, Obtaining plan approval, CAVEATS/CONTROVERSIES, Lack of buy-in, Incomplete RTOs and RPOs, Systems myopia, Lax security, Outdated plans.

UNIT IV: BUSINESS CONTINUITY PLANNING AND MANAGEMENT

INTRODUCTION, WHAT IS BUSINESS CONTINUITY PLANNING?, Why is business continuity planning important?, CREATING A BUSINESS COUNTINUITY PLAN, BCP Governance (Management), Business impact analysis, Identify the mandate and critical aspects of an organization, Prioritize critical services or products, Identify impacts of disruptions, Identify areas of potential, Identify intangible losses, Insurance requirements, Ranking, Identify dependencies, Plans for business continuity, Mitigating threats and risks, Analyze current recovery capabilities, Create continuity plans, Response preparation, Alternate facilities, Readiness procedures, Training, Exercises, Quality assurance techniques, Internal review, External audit, Maintenance, Information/targets, Technical, Testing and verification of recovery procedures, Recovery requirement, Threat and risk analysis (TRA), Impact scenarios, What to do when a disruption occurs, Response, ContinuationRecovery and restoration.