

# C O N T E N T S

---

	PAGE
<i>Foreword</i>	I-3
<i>Author's Profile</i>	I-5
<i>Recommended Reading</i>	I-7
<i>Chapter-heads</i>	I-9

## A MODULE **IT SECURITY OVERVIEW**

### 1

#### **INTRODUCTION TO INFORMATION SECURITY**

◆ Objectives	3
◆ Introduction	3
◆ Data And Information	4
◆ Information Classification	6
◆ Need To Know	8
◆ Information Security	9
◆ Other Applicable Attributes of Information Security	12
◆ Physical Security	14
◆ Logical Security	14
◆ Know Your Progress	17
◆ Key Words	18

## 2

### **CORPORATE IT SECURITY**

◆ Objectives	20
◆ Meaning of Corporate IT Security	20
◆ Need for a Corporate IT Security Policy	21
◆ Legal requirements	22
◆ Essential features of Corporate IT Security Policy	23
◆ Methodology of framing an IT Security Policy	30
◆ Awareness Initiatives	32
◆ Know Your Progress	33
◆ Key Words	33

## 3

### **ORGANISATIONAL SECURITY AND RISK MANAGEMENT**

◆ Objectives	36
◆ Organisational Security	36
◆ Public Sector organisation	37
◆ Right to Information Act, 2005	38
◆ Risk Management	43
◆ Risk Metrics	48
◆ Downstream Liability	49
◆ Risk Management in Banking	49
◆ Know Your Progress	50
◆ Key Words	50

## 4

### **SECURITY GOVERNANCE**

◆ Objectives	53
◆ Policies	54
◆ Framework	54
◆ Key Responsibility Areas	55

	PAGE
◆ Security Governance in Public Sector Undertakings	55
◆ Security Governance in Banks	56
◆ Compliance to Policies is a must in any organization	58
◆ Monitoring	58
◆ Know Your Progress	60
◆ Key Words	60

## 5

### **PHYSICAL AND ENVIRONMENTAL SECURITY**

◆ Objectives	63
◆ Physical security equipment	67
◆ Intrusion Prevention Systems (IPSs)	71
◆ Environmental Security	72
◆ Know Your Progress	74
◆ Key Words	74

## 6

### **HARDWARE SECURITY**

◆ Objectives	77
◆ Hardware	77
◆ Network related devices like routers, switches, hubs	81
◆ Know Your Progress	88
◆ Key Words	88

## 7

### **SOFTWARE AND OPERATIONAL SECURITY**

◆ Objectives	91
◆ Cloud Computing	97
◆ Operational Security	98
◆ Banking	99
◆ Telecom Industry	100
◆ IT Industry	101
◆ BPO and KPO Industries	101



- ◆ User Level Controls
- ◆ Know Your Progress
- ◆ Key Words

8

**SECURITY STANDARDS AND BEST PRACTICES**

- ◆ Objectives 106
- ◆ Introduction 106
- ◆ ISO 27000 standards 108
- ◆ ISO – ISMS 109
- ◆ What are the benefits of ISO 27001? 110
- ◆ COBIT-Control Objectives in IT 112
- ◆ Know Your Progress 115
- ◆ Key Words 115

B MODULE

**IT SECURITY CONTROLS**

9

**ASSET CLASSIFICATION AND CONTROLS**

- ◆ Introduction 121
- ◆ Asset Classification and Control 121
- ◆ Protection of Information Assets 122
- ◆ Control of Hardware equipment 123
- ◆ Control of Software Assets 128
- ◆ Know Your Progress 131
- ◆ Key Words 131

10

**PHYSICAL & ENVIRONMENTAL SECURITY CONTROLS**

- ◆ Introduction 135
- ◆ Environment Controls 138
- ◆ E-Wastes 141
- ◆ Know Your Progress 144
- ◆ Key Words 145

**11****SOFTWARE SECURITY CONTROL**

◆ Objectives	148
◆ Operating Systems (OS)	150
◆ Windows Security	152
◆ Databases	153
◆ Application Level Security	154
◆ Mobile Banking	161
◆ Internet Banking	163
◆ Credit Cards	164
◆ Know Your Progress	166
◆ Key Words	167

**12****NETWORK CONTROLS**

◆ Introduction	170
◆ Controls in a layered network	172
◆ IP Security	173
◆ VLANs	174
◆ Communication Channels	176
◆ Protocols used in Network	179
◆ Intrusion Detection System (IDS)	183
◆ Firewalls	185
◆ Unified Threat Management	187
◆ Know Your Progress	190
◆ Key Words	191

**13****CONTROLS IN SOFTWARE DEVELOPMENT & MAINTENANCE**

◆ Introduction	195
◆ Software Development	198



- ◆ In-house Software development
- ◆ Cloud Computing
- ◆ Big Data
- ◆ Know Your Progress
- ◆ Key Words

C MODULE

**IT SECURITY THREATS**

14

**IT SECURITY THREATS**

- ◆ Introduction 217
- ◆ Threats! 217
- ◆ Cyber Espionage 226
- ◆ Cyber Terrorism 227
- ◆ Know Your Progress 231
- ◆ Key Words 232

15

**SOFTWARE ATTACKS - VIRUS AND MALWARES**

- ◆ Objectives 236
- ◆ Introduction 236
- ◆ Malware 238
- ◆ Controls 244
- ◆ Know Your Progress 248
- ◆ Key Words 248

16

**INCIDENT MANAGEMENT**

- ◆ Objectives 252
- ◆ Introduction 252
- ◆ Objectives of Incident Response 254
- ◆ Action Methodology 256



	PAGE
◆ Processes running	258
◆ Awareness	262
◆ Know Your Progress	262
◆ Key Words	263

## 17

### **FAULT TOLERANT SYSTEMS**

◆ Objectives	266
◆ Introduction	266
◆ High Availability (HA)	269
◆ Know Your Progress	275
◆ Key Words	276

## 18

### **BUSINESS CONTINUITY AND DISASTER RECOVERY MANAGEMENT**

◆ Objectives	279
◆ Introduction	279
◆ Downtime	281
◆ Phase I	283
◆ Backups	285
◆ Who should call 'disaster'?	288
◆ Phase II	289
◆ Phase III	290
◆ Know Your Progress	290
◆ Key Words	291

## D MODULE

### **IS AUDIT & REGULATORY COMPLIANCE**

## 19

### **INFORMATION SYSTEMS AUDIT**

◆ Objectives	297
--------------	-----

	<i>PAGE</i>
◆ Introduction	297
◆ History of EDP Audit in banks	299
◆ IS Auditor	300
◆ External vs Internal IS Auditor	301
◆ Audit Methodologies	302
◆ Types of Audits	303
◆ Planning Phase	305
◆ Report Presentation	307
◆ Audit Policy	308
◆ COBIT and Framework	309
◆ Audit Reports	309
◆ Know Your Progress	311
◆ Key Words	311

## 20

### **REGULATORY MECHANISM IN INDIAN BANKS**

◆ Objectives	314
◆ Introduction	314
◆ RBI as the regulator	315
◆ RBI's regulatory initiatives taken so far	317
◆ Gopalakrishna Working Group	318
◆ Compliance in banks	320
◆ Penal powers of RBI	322
◆ RBI's regulatory mechanism already in place	323
◆ SEBI	326
◆ TRAI	327
◆ IRDAI	329
◆ Legal Enactments	330
◆ Know Your Progress	332
◆ Key Words	332