

Implementing an Information Security Management System

**Security Management Based on
ISO 27001 Guidelines**

**Abhishek Chopra
Mukund Chaudhary**

Apress®

Table of Contents

About the Authors	xi
About the Technical Reviewer	xiii
Acknowledgments	xv
Introduction	xvii
Chapter 1: The Need for Information Security	1
What Is Information Security?.....	1
Data	2
Information	2
How ISO 27001 Applies to You	4
ISO 27001: Information Security Management System.....	4
Why Is It Important to Safeguard Information?	9
Yahoo	9
Marriott International.....	9
eBay.....	10
Heartland Payment Systems	10
Uber	10
NHS Cyberattack.....	11
Safeguarding Summary.....	11
Scenario 1: Banking.....	12
Scenario 2: Trade Secrets.....	14
Scenario 3: Healthcare	15
Scenario 4: Manufacturing	18
Scenario 5: Information Technology	19
Summary.....	20

TABLE OF CONTENTS

- Chapter 2: Assessing Needs and Scope..... 21**
 - Assessing Business Needs 21
 - Scope and High-level Timeframe for Implementation..... 24
 - What's Covered in the Scope Document?..... 27
 - What Is the Statement of Applicability (SOA)? 28
 - High-Level Timeframe 46
 - Senior Management Support 47
 - Summary..... 48
 - Reference..... 48

- Chapter 3: Project Kick-Off..... 49**
 - Presenting a High-Level Plan..... 50
 - Setting Up the Project Taskforce..... 52
 - Administration Department 52
 - Chief Information Security Officer (CISO) 52
 - System Admin or IT Manager 53
 - Information Security Management (ISM) Team 54
 - Human Resources Management 54
 - Getting Commitment..... 55
 - Summary..... 58

- Chapter 4: Initial Risk Assessment..... 59**
 - Meeting the Team 59
 - Annex 5: Information Security Policies 60
 - Annex 6: Organization of Information Security 61
 - Annex 7: Human Resources Security..... 61
 - Annex 8: Asset Management 62
 - Annex 9: Access Control 63
 - Annex 10: Cryptographic Control 63
 - Annex 11: Physical and Environmental Security 64
 - Annex 12: Operations Security 66
 - Annex 13: Communications Security 67

Annex 14: Security Requirements of Information Systems	68
Annex 15: Supplier Relationships	71
Annex 16: Information Security Incident Management	71
Annex 17: Information Security Aspects of Business Continuity Management	72
Annex 18: Compliance	72
Preparing the Analysis Report.....	73
Presenting the Report to Management/Teams.....	75
Summary.....	76
Chapter 5: Risk Management Approach	77
Defining and Finalizing the Risk Assessment Framework	77
Risk Components.....	78
What Are Threats?	79
What Are Vulnerabilities?.....	79
What Is a Security Risk?.....	80
What Is a Risk Ranking?.....	82
Risk Prioritization	82
Risk Owner Identification	83
Risk Treatment.....	83
What Is Acceptable Risk?.....	86
Risk Monitoring and Review	87
Identifying Assets.....	87
Asset Value	88
Asset Classification	89
Asset Labeling	90
Asset Register	92
Asset Disposal	94
Asset Register Examples	95
Managing Risks	98
Identifying Security Controls.....	100
Revisiting the Statement of Applicability (SoA).....	101
Summary.....	101

TABLE OF CONTENTS

- Chapter 6: Execution 103**
 - Information Security Awareness 103
 - An Emphasis on Training Content 104
 - Awareness Quiz 104
 - Policies and Procedures 105
 - Who Defines the Policies? 105
 - Who Reviews and Approves the Policies? 106
 - Which Policies and Procedures Are Covered? 106
 - Understanding and Implementing Controls 121
 - A.5 Information Security Policies 121
 - A.6 Organization of Information Security 123
 - A.7 Human Resources Security 130
 - A.8 Asset Management 137
 - A.9 Access Control 144
 - A.10 Cryptography 155
 - A.11 Physical and Environmental Security 158
 - A.12 Operations Security 166
 - A.13 Communication Security 181
 - A.14 System Acquisition, Development, and Maintenance 188
 - A.15 Supplier Relationships 197
 - A.16 Information Security Incident Management 204
 - A.17 Information Security Aspects of Business Continuity Management 210
 - A.18 Compliance 213
 - Summary 219
 - References 219
- Chapter 7: Internal Audit 221**
 - Preparing an Internal Audit Team 221
 - Conducting Audits 224
 - Audit Plan 224
 - Pre-Audit Meeting/Briefing 226
 - Opening Meeting 227

Audit's Finding Report	230
Closing the Findings and Gaps.....	232
Planning Improvement.....	232
Eliminating Gaps.....	233
Can You Eliminate All Gaps?	234
Communicating.....	234
Summary.....	235
Chapter 8: Management Review.....	237
Conducting the Review	237
What Is Expected from Department Heads/Stakeholders?.....	238
Scheduling the Management Review Meeting.....	238
Items To Be Covered in the Presentation.....	240
Conducting the Review Meeting.....	241
Plan Improvement.....	244
What Do You Improve?.....	244
How Do You Know if You Have Improved?	244
Communicate	245
Summary.....	245
Chapter 9: External Audit	247
Audit Preparation	247
Stage 1 Audit	248
Stage 2 Audit	248
Stage 3 Audit	249
Best Practices	251
Audit Closure.....	253
Audit Report	254
Executive Summary.....	254
SWOT Analysis.....	256
Scope Description Control by Control.....	256
Finding Summary	257

TABLE OF CONTENTS

Evidence Summary..... 257

Lead Auditor Recommendation 257

Front Page 257

Summary..... 258

Chapter 10: Continual Improvement..... 259

Areas of Improvement..... 260

 Monthly KPIs/Reports 260

 Employee Observations 260

 Periodic Internal Audits 261

 Management Review Meetings 261

 Customers/Clients 261

 New Tools/Technology 261

 Regulatory/Governmental Laws 262

Execution Plan 262

 Pilot the Improvement First 263

 Measure Success 263

Performing Regular Audits/Reviews 264

Summary..... 265

Index..... 267