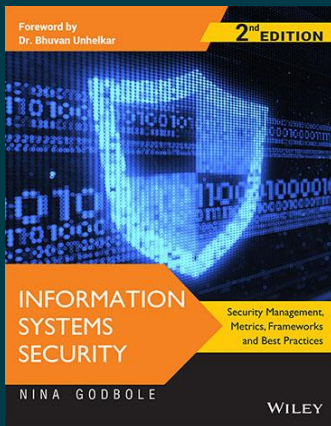


**WILEY**

# Information Systems Security, 2ed: Security Management, Metrics, Frameworks and Best Practices

By Nina Godbole

**Paperback**

ISBN: 9788126564057

Publication: [ NOT PROVIDED ] *publication\_date*

Page Count: 972 pages

**₹1,179.00**

## • Description

Keeping the essence of the first edition, this new edition of Information Systems Security: Security Management, Metrics, Frameworks and Best Practices is restructured to meet the ever-growing demand for books that give a comprehensive treatment of the Information Security topic. Designed with ample figures to illustrate key points and Review Questions and Reference Material Pointers at the end of each chapter, it is truly a treatise on the subject. This book should prove a valuable reference on the topic to students as well as professionals. It is useful for candidates appearing for the CISA certification exam and maps well with the CBOK for CSTE and CSQA Certifications.

## • About the Author

**Nina Godbole***[ NOT PROVIDED ] author\_details*

## • Table of Contents

Foreword

About the Author

Preface to the Second Edition

Preface to the First Edition

Acknowledgments

List of Figures

List of Tables

List of Boxes

Part I Introduction

1 Information Systems in Global Context

1.1 History of Information Systems

1.2 Importance of Information Systems

1.3 Basics of Information Systems

1.4 The Changing Nature of Information Systems

1.5 Globalization of Businesses and the Need for Distributed Information Systems

1.6 Global Information Systems: Role of Internet and Web Services

1.7 Information Systems Security and Threats: A Glimpse

2 Threats to Information Systems

## 2.1 Introduction

### 2.2 New Technologies Open Door to the Threats

### 2.3 Information-Level Threats versus Network-Level Threats

### 2.4 Information Systems Security: Threats and Attacks

### 2.5 Computer Viruses: The bête noire of Computing Era

### 2.6 Classifications of Threats and Assessing Damages

### 2.7 Protecting Information Systems Security

## 3 Information Security Management in Organizations

### 3.1 The Context for Information Security Management (ISM)

### 3.2 Security Policy, Standards, Guidelines and Procedures

### 3.3 Information Security Scenario in the Financial Sector

### 3.4 Information Security Management System (ISMS)

### 3.5 Organizational Responsibility for Information Security Management

### 3.6 Information Security Awareness Scenario in Indian Organizations

## 4 Building Blocks of Information Security

### 4.1 Introduction

### 4.2 Basic Principles of Information Systems Security

### 4.3 Security-Related Basic Terms and Definitions

### 4.4 The Three Pillars of Information Security

### 4.5 Other Important Terms in Information Security

### 4.6 Information Classification

### 4.7 Terms for Information Classification

### 4.8 Criteria for Classification of Data and Information

### 4.9 Information Classification: Various Roles

### 4.10 Data Obfuscation

### 4.11 Business Systems' Classification

### 4.12 Event Classification

## 5 Information Security Risk Analysis

### 5.1 Introduction

### 5.2 Terms and Definitions for Risk Analysis of Information Security

### 5.3 Risk Management and Risk Analysis: What it is and the Need for it

### 5.4 Approaches and Considerations in Information Security Risk Analysis

### 5.5 Auditing Perspective on Information Security Risk Analysis

## Part II Cloud, Mobile Applications, Smartphone, IoT, Smart Cities and Wireless Networks in Security Perspective

## 6 Security Considerations in Mobile and Wireless Computing

### 6.1 Introduction

### 6.2 Proliferation of Mobile and Wireless Devices

### 6.3 Trends in Mobility

### 6.4 Credit Card Frauds in Mobile and Wireless Computing Era

### 6.5 Security Challenges Posed by Mobile Devices

### 6.6 Registry Settings for Mobile Devices

### 6.7 Authentication Service Security

### 6.8 Mobile Devices: Security Implications for Organizations

6.9 Organizational Measures for Handling Mobile Devices Related Security Issues

6.10 Organizational Security Policies and Measures in Mobile Computing Era

6.11 Laptops

6.12 Use of RFID in Mobile Commerce and Information Asset Protection

6.13 Wearable Devices and Security Threats

7 Security in Cloud Computing

7.1 Introduction

7.2 Cloud Computing: Why?

7.3 How Does Computing with the 'Cloud' Work

7.4 Conceptual View of Cloud Computing – Characteristics and Deployment Models

7.5 Big Data and Cloud Computing

7.6 Security and Privacy Risks in Cloud Computing

7.7 Protecting Information Security and Data Privacy in Cloud Computing

8 Smartphone Security

8.1 Introduction: The Emergence of Smartphones

8.2 Smartphones: Security Risks, Issues and Challenges

8.3 Protected Health Information and Smartphones

8.4 Smartphones and Electronically Stored Medical Information: The Challenges

8.5 Smartphones: The Downside

8.6 Guidelines for using Smartphone Securely

9 Security of Wireless Networks

9.1 Introduction

9.2 An Overview of Wireless Technology

9.3 Wireless Network Usage Scenario Today and Implications

9.4 Wired World versus Wireless World: Putting Wireless Networks in Information Security Context

9.5 Attacks on Wireless Networks

10 The Internet of Things (IoT) and Smart Cities: Security and Privacy Challenges

10.1 Introduction

10.2 The 'Internet of Things' (IoT): The New Kid on the Block

10.3 Understanding Security and Privacy Issues in IoT

10.4 Intelligent Buildings: Security Threats

10.5 Smart Cities: Privacy and Security

10.6 Personal and Business Impact of IoT

Part III Network Security and Other Controls

11 Biometrics for Security

11.1 Introduction

11.2 Access Control, User Identification and User Authentication

11.3 What is Biometrics?

11.4 Biometric Identification/Authentication Techniques

11.5 Biometric Techniques

11.6 Matching and Enrolment Process in Biometrics

11.7 Classification of Biometric Applications

11.8 Criteria for Selection of Biometric Application

- 11.9 Biometric Systems: Architectural Design Issues
- 11.10 Biometric Measurement Issues
- 11.11 Key Success Factors for Biometric Systems
- 11.12 Benefits of Biometrics over Traditional Authentication Methods
- 11.13 Standards for Biometrics
- 11.14 Economic and Social Aspects of Biometrics
- 11.15 Legal Challenges in Biometrics
- 11.16 The Future of Biometrics
  
- 12 Network Security in Perspective
- 12.1 Need for Security in the Networked World
- 12.2 Net-Centric Information Systems
- 12.3 Basic Concepts of Network Security
- 12.4 Network Security Dimensions
- 12.5 Establishing Security Perimeter for Network Protection
  
- 13 Networking and Digital Communication Fundamentals
- 13.1 Introduction
- 13.2 Network Types
- 13.3 Network Architecture
- 13.4 Network Topologies
- 13.5 The OSI Seven-Layer Model
- 13.6 Network Components
- 13.7 Network Protocols
- 13.8 Working of Networks and the Internet
- 13.9 Telecommunication Links and Other Important Related Topics
  
- 14 Cryptography and Encryption
- 14.1 Introduction
- 14.2 What is Cryptography?
- 14.3 Genesis and Application of Cryptography
- 14.4 Role of Cryptography in Information Security
- 14.5 Digital Signature – A Method for Information Security
- 14.6 Cryptographic Algorithms
  
- 15 Intrusion Detection for Securing the Networks
- 15.1 Introduction
- 15.2 Network Attacks – The Stages
- 15.3 Need for Intrusion Monitoring and Detection
- 15.4 Intrusion Detection for Information Systems Security
  
- 16 Firewalls for Network Protection
- 16.1 Introduction
- 16.2 What are Firewalls?
- 16.3 Demilitarized Zone (DMZ)
- 16.4 Why Firewalls are Needed – Protection Provided by Firewalls
- 16.5 Proxy Servers
- 16.6 Topologies for Different Types of Firewalls
- 16.7 Examining Firewalls in the Context of Intrusion Detection Systems

- 16.8 Firewalls vis-à-vis Routers
- 16.9 Design and Implementation Issues in Firewalls
- 16.10 Policies for Firewalls – The Importance
- 16.11 Using Firewalls Effectively
- 16.12 Vendors of Firewall Products

## 17 Virtual Private Networks for Security

- 17.1 Introduction
- 17.2 What is a Virtual Private Network?
- 17.3 The Need for Virtual Private Networks
- 17.4 Role of a Virtual Private Network for an Enterprise
- 17.5 Use of Tunneling with Virtual Private Networks
- 17.6 Working of Virtual Private Networks
- 17.7 Authentication Mechanisms in Virtual Private Networks
- 17.8 Types of VPNs and Their Usage
- 17.9 Tunneling Security
- 17.10 VPN Technologies
- 17.11 VPN Architecture
- 17.12 Configurations/Topologies for Virtual Private Networks
- 17.13 Security Concerns in VPN
- 17.14 VPN Best Practices

## Part IV Security of Applications and Operating Systems

### 18 Security of Electronic Mail Systems

- 18.1 Introduction
- 18.2 Today's Electronic Mail Usage Scenario
- 18.3 Electronic Mail System Mechanism
- 18.4 The Growing Power of Electronic Mail Systems
- 18.5 Security Threats Posed By Electronic Mails
- 18.6 Countermeasures to Protect from Threats Posed Through E-Mails
- 18.7 Governance for Electronic Mail Systems

### 19 Security of Electronic Commerce

- 19.1 Introduction
- 19.2 'Electronic Commerce' Paradigm
- 19.3 Strategic Issues in EDI Security
- 19.4 The IT Environment and Infrastructure for Electronic Commerce
- 19.5 Security Issues and Concerns in the Electronic Commerce

### 20 Security of Databases

- 20.1 Introduction
- 20.2 Database Security Challenge in the Modern World
- 20.3 Databases in the Context of Business Intelligence
- 20.4 Nature of Database Security Issues: Why it is Important?
- 20.5 Federated Databases: The Need and the Security Issues
- 20.6 Securing the Contents of Mobile Databases
- 20.7 Securing Connectivity with Enterprise Databases

20.8 Data Integrity as a Parameter for Database Security

20.9 Database Security Policy

21 Security of Operating Systems

21.1 Introduction

21.2 Role of Operating Systems in Information Systems Application

21.3 Operating System Types

21.4 Operating Systems, Functions and Tasks

21.5 Network Operating Systems (NOSs)

21.6 Operating System Security

21.7 Host Security and OS Hardening

21.8 Patched Operating System

21.9 Current 'Insecurity' Scenario

Part V Models, Frameworks and Metrics for Maturing Security Practices

22 Security Models, Frameworks, Standards and Methodologies

22.1 Introduction

22.2 Terminology

22.3 Methodologies for Information Systems Security

23 ISO 17799/ISO 27001

23.1 Introduction

23.2 Evolution of the Standard

23.3 ISO 27001 in Organizational Context: Relation to ISO 17799

23.4 Inside the ISO 17799

23.5 ISMS Implementation in Organizations Using Security Controls of ISO 27001

23.6 Security Certification Using the ISO 17799/ISO 27001

23.7 Benefits of ISO 27001 Certification

24 COBIT, COSO-ERM and SOC

24.1 Introduction

24.2 Control Objectives for Information and Related Technologies – the COBIT

24.3 COSO Enterprise Risk Management Model (COSO-ERM)

24.4 ERM: Definition and History

24.5 Service Organization Control (SOC)

Part VI Metrics, Legal Aspects and Privacy Consideration for Information Security

25 Security Metrics

25.1 Introduction

25.2 What are Measurements and Metrics?

25.3 Security Metrics Basics

25.4 Security Metrics Classification

25.5 Why Security Metrics are Important

25.6 Benefits of Using Security Metrics

25.7 InfoSec Metrics Management in Organizations

- 25.8 Quantitative versus Qualitative Approach to Security Risk Metrics
- 25.9 Security Metrics for Considerations
- 25.10 Implementing Security Metrics Program
- 25.11 Components of Security Metrics Program
- 25.12 Metrics Development Process
- 25.13 Metrics Implementation Process
- 25.14 Implementation Approach
- 25.15 Communication of Security Metrics in the Organization
- 25.16 Key Success Factors in Implementing InfoSec Metrics
- 25.17 Pitfalls and Challenges in Organizational Security Metrics Program

## 26 Laws and Legal Framework for Information Security

- 26.1 Introduction
- 26.2 Information Security and the Law: The Rising Need
- 26.3 Understanding the Laws for Information Security: A Conceptual Framework
- 26.4 The Indian IT Act
- 26.5 Laws for Intellectual Property Rights (IPR)
- 26.6 Patent Law
- 26.7 Copyright Law
- 26.8 Indian Copyright Act
- 26.9 Privacy Issues and Laws in Hong Kong, Japan and Australia
- 26.10 European Outlook on Laws for Information Security
- 26.11 Data Protection Act in Europe
- 26.12 Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- 26.13 Gramm-Leach-Bliley Act of 1999 (GLBA)
- 26.14 Overview of Sarbanes-Oxley (SOX)
- 26.15 Legal Issues in Data Mining Security
- 26.16 Building Security into Software/System Development Life Cycle
- 26.17 Federal Information Security Management Act (FISMA)
- 26.18 The Need for Global Action

## 27 Privacy - Fundamental Concepts and Principles

- 27.1 Introduction
- 27.2 Why Privacy is a Business Issue?
- 27.3 Privacy and Security: Confusion and Conflict
- 27.4 Privacy and Related Key Terms and Concepts
- 27.5 Transactional Context and Historical Perspective for Privacy
- 27.6 The Growing Importance of Privacy
- 27.7 The Need for Privacy Awareness
- 27.8 Fair Information Practices (FIPs)
- 27.9 Information Privacy Principles (IPPs)

## 28 Privacy - Business Challenges and Technological Impacts

- 28.1 Introduction
- 28.2 Privacy and Direct Marketing
- 28.3 Data Mining and Privacy Invasion
- 28.4 Privacy and Business Outsourcing
- 28.5 Privacy Challenges in a Test Environment
- 28.6 Masking the Test Data to Address Data Privacy during Testing

28.7 Best Practices – Data Privacy in Test Data Management

28.8 Privacy – Technological Impacts

29 Privacy Aspects of Web Services

29.1 Introduction

29.2 Privacy on the Internet – A Legal Perspective and Organizational Implications

29.3 Privacy Considerations in Web Services

29.4 Privacy in the Semantic Web

29.5 Privacy Considerations in the Use of Context-Sensitive Technologies

29.6 Security and Privacy Aspects of Service-Oriented Architectures

Part VII Security Best Practices

30 Staffing the Security Function

30.1 Introduction

30.2 Security Reporting Structure in Organizations

30.3 Choices for Placement of Security Function in Organizations

30.4 Managing Security Staffing – Possible Approaches

30.5 Security Certifications

31 Business Continuity and Disaster Recovery Planning

31.1 Introduction

31.2 The Genesis of DRP

31.3 Importance of BCP

31.4 Business Impact Analysis

31.5 Approaches to DRP

31.6 Defining Business Goals to Prepare for BCP and DRP

31.7 Types of Alternate Sites from BCP Perspective

31.8 DRP Test Types

31.9 Identification of Key Personnel

31.10 Business Interruption Preparedness Checklist

31.11 Business Resilience

32 Auditing for Security

32.1 Introduction

32.2 Basic Terms Related to Audits

32.3 Security Audits – What are They?

32.4 The Need for Security Audits in Organizations

32.5 Organizational Roles and Responsibilities for Security Audit

32.6 Auditor's Responsibility in Security Audits

32.7 Types of Security Audits

32.8 Approaches to Audits

32.9 Technology-Based Audits – Vulnerability Scanning and Penetration Testing

32.10 Resistance to Security Audits

32.11 Phases in Security Audit

32.12 Security Audit Engagement Costs and Other Aspects

32.13 Budgeting for Security Audits

32.14 Selecting External Security Consultants

32.15 Key Success Factors for Security Audits

33 Privacy Best Practices in Organizations

- 33.1 Introduction
- 33.2 Privacy – Organizational Implications
- 33.3 Privacy Audits – Driving Factors
- 33.4 Privacy Practices: Caveats for Management – Planning and Oversight
- 33.5 Privacy Auditing Standards and Privacy Audit Phases
- 33.6 Privacy Officer: The Job and Responsibilities and Skills
- 33.7 Privacy Impact Assessments of Information Systems Application
- 33.8 Organizational Reactions to Privacy Audits

## 34 IT Asset Management

- 34.1 Introduction
- 34.2 Understanding the Organizational Context for Asset Management
- 34.3 Security Aspects in IT Asset Management
- 34.4 Asset Management in Organizations: Issues and Challenges
- 34.5 Asset Management Life Cycle
- 34.6 Tools for IT Asset Management
- 34.7 Benefits of Asset Management
- 34.8 Roles and Responsibilities in Asset Management
- 34.9 Identifying Asset Containers
- 34.10 Organizational Best Practices in IT Asset Management
- 34.11 Treatment of IT Assets in the Company’s Book of Accounts
- 34.12 SOX Compliance Requirements for IT Assets
- 34.13 SAS 70 and the Asset Manager
- 34.14 Managing Software Assets
- 34.15 IT Assessment Management – Key Success Factors

## Part VIII Other Important Concepts in Information Systems Security

### 35 Physical Security: An Overview

- 35.1 Introduction
- 35.2 Need for Physical Security
- 35.3 What is Physical Security?
- 35.4 Natural Disasters and Controls
- 35.5 Basic Tenets of Physical Security of Information Systems Resources
- 35.6 Physical Entry Controls: Protecting Organization’s Physical Entry Points

### 36 Perimeter Security for Physical Protection

- 36.1 Introduction
- 36.2 Scope of Perimeter Security
- 36.3 Typical Terms in Perimeter Security
- 36.4 Elements of Perimeter Security

### 37 Business Applications Security: An EAI Perspective

- 37.1 Introduction
- 37.2 Meaning and Evolution of EAI
- 37.3 Application Security: Basic Issues
- 37.4 Understanding Web Services in the Context of EAI
- 37.5 Business Drivers for Enterprise Application Integration
- 37.6 Application Communication Through EAI
- 37.7 Role of Web Services in Enterprise Application Integration
- 37.8 Security Complexities and Complications Due to Enterprise Application Integration

37.9 Security Threats and Risks for the Extended Enterprise  
37.10 Mitigating Security Issues in Enterprise Application Development

## 38 Systems Security Engineering Capability Maturity Model – The SSE-CMM

38.1 Introduction  
38.2 What is Security Engineering?  
38.3 SSE-CMM – Nature and Scope  
38.4 Importance of the SSE-CMM Model  
38.5 Target Audience for the SSE-CMM  
38.6 SSE-CMM Usage Paradigm  
38.7 SSE-CMM – Structure and Architecture  
38.8 Process Areas of the SSE-CMM  
38.9 Common Misconceptions About Capability Maturity Models

## 39 Information Security: Other Models and Methodologies

39.1 Introduction  
39.2 Other Frameworks for Information Security  
39.3 Other Methodologies and Standards for Information Security

## 40 Ethical Issues and Intellectual Property Concerns in Information Security

40.1 Introduction  
40.2 Information Systems – Threats from Within  
40.3 Characteristics of Insider Attacks on Organizational Information Systems  
40.4 The Nature of Ethical Issues in the Networked Enterprise  
40.5 Implications for the Healthcare Industry: Ethical and Legal Concerns  
40.6 Data Auctioning, Data Hijacking and Data Laundering: Ethical Issues in Paramedical Process Outsourcing  
40.7 Ethical Issues Owing to Information Warfare  
40.8 Cryptography, Cryptographic Tools and Ethical Issues  
40.9 Understanding Ethical Hacking  
40.10 Social Engineering Issues  
40.11 Concerns from Information Brokers' Activities  
40.12 The Need for Ethical Guidance for Security Professionals  
40.13 Understanding Intellectual Property and its Various Forms  
40.14 Trademark, Trade Name, Company Name, Business Name and Domain Name – The Relationship  
40.15 Ethical Domain for Information Security: Some Concluding Thoughts

Index

---

**To purchase this product, please visit:**

<https://wiley.indiafin.com/information-systems-security-2ed-security-management-metrics-frameworks-and-best-practices.html>



Scan to buy