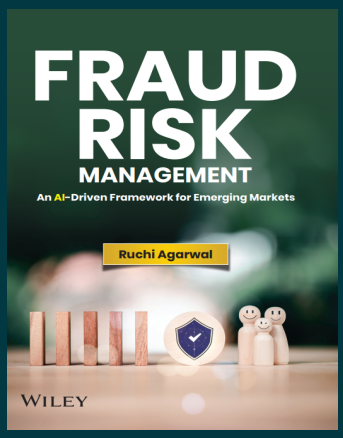
WILEY



Fraud Risk Management: An AI-Driven Framework for Emerging Markets

By Ruchi Agarwal

Paperback 9788166060045 ₹899.00

Pages: 268

Description

Fraud Risk Management: An AI-Driven Framework for Emerging Markets presents a structured approach to fraud in an increasingly digital economy. As financial services, insurance, healthcare, government systems, digital payments, and procurement platforms run on interconnected data and decision systems, fraud has become more sophisticated, less visible, and harder to catch through conventional audits or transaction rules.

At the heart of the book is the Structured Digital Fraud Framework (SDFF), which distinguishes between Monocarpic, Bonsai, Banyan, and Baobab fraud. Each form reflects a different fraud architecture and calls for a different mix of analytical, technological, investigative, and governance responses. The book integrates traditional fraud theories with anomaly detection, behavioral analytics, time-series models, Graph Neural Networks, community detection, NLP, deep learning, and entity resolution, emphasizing that AI works best when matched to the structure of the fraud rather than applied as a universal solution.

Responsible implementation is a central theme. Dedicated chapters examine ethical blind spots in AI, Responsible AI, privacy, fairness, transparency, accountability, and regulation, including GDPR and the EU AI Act. Further chapters cover fraud-management tools such as the Fraud-o-Meter, fraud-control strategies, Loss Mitigation Units, field investigation, and health-insurance case studies. The final chapter introduces Fraud Architecture Theory, explaining how fraud evolves from isolated acts into coordinated, institutionally embedded structures.

The book is intended for undergraduate and postgraduate students of management, finance, accounting, auditing, insurance, risk management, business analytics, and corporate governance, as well as researchers. It is equally suited to fraud investigators, internal auditors, risk and compliance professionals, banking and insurance professionals, regulators, and executives responsible for fraud prevention.

About the Author

Ruchi Agarwal

Ruchi Agarwal is Assistant Professor of Strategy and Risk Management at the Management Development Institute (MDI), Gurugram. Her teaching and research interests include enterprise risk management, fraud risk management, risk governance, organizational fraud, sustainable strategy, and competitive strategy. She holds a PhD in the implementation of Enterprise Risk Management from the University of Edinburgh Business School, UK, and an MBA in Finance from the Institute of Management Technology, Ghaziabad. She is a Fellow of the Insurance Institute of India and holds an Advanced Diploma in Insurance from the Chartered Insurance Institute, UK.

Before joining MDI, she was a Senior Researcher at the Indian School of Business, Hyderabad, a Visiting Scholar at the University of Southampton, UK, and Visiting Faculty at EDC Paris. She brings around twelve years of industry and consulting experience in insurance, finance, technology, and risk management, and has contributed to research and consulting engagements involving the World Bank, Reserve Bank of India, IRDAI, Ayushman Bharat, European Central Bank, Allianz, Bajaj Allianz, GIC Re, Reliance General, and Ernst & Young.

Her research has appeared in the California Management Review, Accounting Horizons, Journal of Accounting & Organizational Change, Journal of Risk Finance, Review of Accounting and Finance, Business Ethics, the Environment and Responsibility, and Strategic Change. She conducts executive programs on fraud analytics, risk governance, and strategic management, and speaks regularly at academic institutions, regulatory bodies, and professional forums.

Table of Contents

Chapter 1 One Size Does not Fit All 1

1.1 Introduction 1

1.2 State-of-the-Art of a Framework for Fraud Control 2

1.3 Can Only Humans Commit Fraud? 4

1.4 Need for a New Structured Framework 5

1.5 Structured Digital Fraud Classification Framework 7

1.6 Conclusion 13

References 14

Key Terms 15

Self-Assessment Questions 16

Discussion Questions 16

Chapter 2 Monocarpic Approach 17

2.1 Introduction 17

2.2 Solo vs Collusive Fraud 18

2.3 Fraudsters' Personality and Solo Fraud 19

2.4 Traditional Tools to Control Solo Frauds 24

2.5 Unsupervised Learning 29

2.6 Conclusion 31

References 32

Key Terms 33

Self-Assessment Questions 33

Discussion Questions 33

Chapter 3 Bonsai Approach 35

3.1 Introduction 35

3.2 Bonsai Fraud and Personality of Fraudsters 36

3.3 Traditional Tools to Catch Bonsai Fraudsters 42

3.4 AI-Powered Techniques for Procurement Fraud Detection 47

3.5 Behavioral Profile Engine 55

Case Study: Double-Billing Fraud Uncovered Post-Acquisition in a Steel Manufacturing Firm 56

References 56

Key Terms 57

Self-Assessment Questions 58

Discussion Questions 58

Chapter 4 Banyan Approach 59

4.1 Introduction 59

4.2 Nexus Collusion 60

4.3 Uncovering Fraud Using a Banyan Approach 68

4.4 Analytics Techniques for Detecting Complex Fraud Networks 74

4.5 AI-Based Strategies 75

4.6 Conclusion 79

References 80

Key Terms 81

Self-Assessment Questions 82

Discussion Questions 82

Chapter 5 The Baobab Approach 83

5.1 Introduction 83

5.2 Definition of Organized Crime 84

5.3 Rational Choice Theory and Organized Crime: A Practical Perspective 88

5.4 AI Approaches to Deal with Nexus 97

5.5 Conclusion 100

References 101

Key Terms 102

Self-Assessment Questions 103

Discussion Questions 103

Chapter 6 Ethical Blind Spots of AI-driven Governance Framework 105

6.1 Introduction 105

6.2 Six Domains Defining Ethical AI Practice 106

6.3 Transparency and Explainability 109

6.4 Agentic AI and Emerging Governance Challenges 116

6.5 Conclusion 118

References 119

Key Terms 120

Self-Assessment Questions 121

Discussion Questions 121

Chapter 7 Responsible AI Framework 123

7.1 Introduction 123

7.2 General Data Protection Regulation (GDPR) 124

7.3 European AI Act and Pyramid of Criticality 126

7.4 Unacceptable-Risk AI Systems (Outright Ban) 127
7.5 High-Risk AI Systems (Strict Regulation) 129
7.6 Limited-Risk Systems (Transparency Obligations) 130
7.7 Minimal-Risk Systems 131
7.8 Key Risks 131
7.9 Conclusion 133
References 134
Key Terms 134
Self-Assessment Questions 135
Discussion Questions 136

Chapter 8 Tools, Techniques, and Processes to Manage Frauds 137
8.1 Introduction 137
8.2 Critiques of Fraud Identification Tools in Emerging Markets 140
8.3 Fraud-o-Meter 141
8.4 Development Process of Fraudometer (2017–2020) 143
8.5 Phases of Development of Fraud-o-Meter 146
8.6 Pre-Assessing Insurance Fraud with Fraud-o-Meter 151
8.7 Conclusion 151
8.8 Key Takeaways from the Case 152
References 153
Key Terms 154
Self-Assessment Questions 154
Discussion Questions 155

Chapter 9 Strategies to Control Fraud 157
9.1 Introduction 157
9.2 The Five Key Strategies for Fraud Control 158
9.3 Conclusion 168
References 169
Key Terms 170
Self-Assessment Questions 170
Discussion Questions 171

Chapter 10 Fraud Prevention and Loss Mitigation Frameworks 173
10.1 Introduction 173
10.2 Establishing a Loss Mitigation Unit 174
10.3 Core Objectives and Functions of a Loss Mitigation Unit (LMU) 174
10.4 Stages of Committing Fraud and Control 179
10.5 Containing and Dismantling Collusion (Stage II Controls) 186

10.6 Discussion 186
References 188
Key Terms 188
Self-Assessment Questions 189
Discussion Questions 189

Chapter 11 Field Investigation 191
11.1 Introduction 191
11.2 Traditional Approaches 192
11.3 Advanced Approaches 197
11.4 Advanced Tools and Techniques in Fraud Investigation 200
11.5 Conclusion 208
References 209
Key Terms 210
Self-Assessment Questions 211
Discussion Questions 212

Chapter 12 Structured Classification – Multiple Case Studies from Health Insurance 213
12.1 Introduction 213
12.2 Field Study Summary: An Investigator’s View of Collusion 218
12.3 Mapping Five Healthcare Case Studies to the Structured Framework 219
12.4 Governance Implications: Aligning Controls with Fraud Structure 224
12.5 Conclusion 224
References 225
Key Terms 226
Self-Assessment Questions 227
Discussion Questions 227

Chapter 13 Future Trends in AI-Driven Fraud Risk Management in Emerging Markets 229
13.1 Introduction 229
13.2 Fraud Architecture Theory vs Fraud Triangle, Diamond and Pentagon 230
13.3 Key Elements of Fraud Architecture Theory 232
13.4 Behaviorally Invisible Fraud in Emerging Markets 236
13.5 AI Strategies for Fraud Detection Across Fraud Types 242
13.6 Conclusion 243
References 245
Key Terms 245
Self-Assessment Questions 246
Discussion Questions 246

To purchase this product, please visit:
https://www.wileyindia.com/fraud-risk-management-an-ai-driven-framework-for-emerging-markets.html

Scan to buy