

TABLE OF CONTENTS

Chapter 1: Foundations of Agentic AI in Enterprise Systems	01-26
1.1 Introduction to Agentic AI and Autonomous Systems	
1.2 Evolution from Traditional AI to Agentic AI	
1.3 Core Components of Agentic AI Architectures	
1.4 Role of AI Agents in Modern Enterprises	
1.5 Use Cases in Regulated Industries (Finance, Healthcare, Defense)	
Chapter 2: Secure Enterprise Architecture for AI Systems	27-59
2.1 Principles of Secure-by-Design AI Systems	
2.2 Enterprise Architecture Models for AI Deployment	
2.3 Data Flow Design in Agentic Pipelines	
2.4 Integration with Legacy Enterprise Systems	
2.5 Scalability and Resilience in AI Infrastructure	
Chapter 3: Trustworthy AI Design Principles	60-86
3.1 Explainability and Transparency in AI Agents	
3.2 Bias Detection and Mitigation Techniques	
3.3 Model Validation and Verification Strategies	
3.4 Human-in-the-Loop Decision Frameworks	
3.5 Ethical AI Governance Models	
Chapter 4: AI Security and Threat Management	87-114
4.1 Threat Landscape in Agentic AI Systems	
4.2 Adversarial Attacks and Model Poisoning Risks	
4.3 Secure Model Training and Deployment Pipelines	
4.4 Runtime Monitoring and Anomaly Detection	
4.5 Incident Response for AI-Driven Systems	
Chapter 5: Compliance and Regulatory Frameworks	115-138
5.1 Overview of Global AI Regulations (US, EU, India)	
5.2 Data Privacy Laws (GDPR, CCPA, HIPAA) in AI Context	
5.3 AI Auditability and Compliance Reporting	
5.4 Governance Standards (NIST AI RMF, ISO/IEC 42001)	
5.5 Legal Accountability of Autonomous Agents	

Chapter 6: Self-Governing AI Pipelines	139-162
6.1 Concept of Autonomous AI Pipelines	
6.2 Continuous Learning and Self-Optimization Mechanisms	
6.3 Policy-Driven AI Execution Frameworks	
6.4 Feedback Loops and Reinforcement Systems	
6.5 Guardrails and Fail-Safe Mechanisms	
Chapter 7: DevSecOps for Agentic AI Systems	163-179
7.1 AI-Enabled DevSecOps Lifecycle	
7.2 CI/CD for Machine Learning Models (MLOps Integration)	
7.3 Automated Security Testing in AI Pipelines	
7.4 Continuous Monitoring and Model Drift Detection	
7.5 Infrastructure as Code for AI Systems	
Chapter 8: Future of Agentic AI in Industry	180-200
8.1 Autonomous Enterprises and Digital Workforce	
8.2 AI-Driven Decision Intelligence Systems	
8.3 Multi-Agent Collaboration Frameworks	
8.4 Industry Transformation (Banking, Manufacturing, Defense)	
8.5 Emerging Risks and Strategic Opportunities	