

TABLE OF CONTENTS

Chapter 1: Introduction to the BISO Role and Evolution	01-22
1.1 Definition and Origin of the BISO Role	
1.2 BISO vs CISO vs CIO	
1.3 Bridge Between Business & Security	
1.4 Evolution of Security Leadership	
1.5 BISO Operating Models	
1.6 Strategic Importance	
1.7 Case Examples	
Chapter 2: Enterprise Risk Management	23-42
2.1 ERM Fundamentals	
2.2 Cyber Risk Identification	
2.3 Risk Quantification	
2.4 Risk Appetite Framework	
2.5 Integration with Business Strategy	
2.6 Third-Party Risk	
2.7 Risk Reporting Metrics	
Chapter 3: Regulatory Compliance	43-63
3.1 Overview of Key Regulations (GLBA, HIPAA, SOX, PCI-DSS)	
3.2 Compliance vs Security	
3.3 Audit Readiness	
3.4 Regulatory Engagement	
3.5 Data Governance	
3.6 Regulatory Technology (RegTech)	
3.7 Cross-border Compliance	
Chapter 4: AI Governance	64-87
4.1 AI Governance Foundations	
4.2 AI Risk Categories	
4.3 Responsible AI Principles	
4.4 AI Lifecycle Governance	
4.5 BISO Role in AI Oversight	
4.6 Regulatory Expectations	
4.7 AI Ethics	

Chapter 5: Security Architecture	88-111
5.1 Business Alignment	
5.2 Security-by-Design	
5.3 Zero Trust Architecture	
5.4 Cloud Security	
5.5 Digital Transformation	
5.6 DevSecOps Integration	
5.7 Architecture Review	
Chapter 6: Third-Party Risk Management	112-136
6.1 TPRM Frameworks	
6.2 Vendor Assessment	
6.3 Supply Chain Risk	
6.4 Contractual Security Requirements	
6.5 Continuous Monitoring	
6.6 Outsourcing Risks	
6.7 Governance Models	
Chapter 7: Security Operations	137-161
7.1 Security Operations Center (SOC) Functions	
7.2 Incident Response	
7.3 Threat Intelligence	
7.4 Business Continuity Planning	
7.5 Crisis Management	
7.6 Cyber Resilience	
7.7 Post-Incident Analysis	
Chapter 8: Leadership & Future of BISO	162-185
8.1 Executive Communication	
8.2 Building a Security Culture	
8.3 Leadership Skills for BISOs	
8.4 Metrics & Dashboards	
8.5 Future of the BISO Role	
8.6 Emerging Trends	
8.7 Career Development	