

Contents

PREFACE	xii
ABOUT THE AUTHOR	xvi
CHAPTER 1 INTRODUCTION	1
Why Are Current Implementations of Cybersecurity Frameworks Effective in Identifying, Monitoring and Responding to Cybersecurity Threats?	2
What Factors Are Used by an Organisation When Investing in Cybersecurity Controls?	2
What Decision-Making Mechanisms Are Organisations Using When Evaluating Different Security Measures Prior to Implementation?	2
Measuring the Effectiveness of Implemented Frameworks	4
Risk Level	4
Importance of Decision-Makers	5
Why Should Organisations Implement Secure Measures to Meet Privacy Laws and Government Regulations?	5
Countering Identity Takeover Incidents	9
Data Protection	16
CHAPTER 2 PRIVACY LAWS	19
Canada	19
Principle 1: Accountability	20
Principle 2: Identifying Purposes	20
Principle 3: Consent	20
Principle 4: Limiting Collection	20
Principle 5: Limiting Use, Disclosure and Retention	21

Principle 6: Accuracy	21
Principle 7: Safeguards	21
Principle 8: Openness	21
Principle 9: Individual Access	21
Principle 10: Challenging Compliance	21
The United States	22
Children's Online Privacy Protection Act ("COPPA")	23
Australia	23
Health Service Providers	24
Health and Medical Research	25
Privacy Breach Reports	26
Personal Information at Issue	27
Privacy by Design	28
Data Governance	31
Privacy as Code	31
Minimisation of PII	32
Shared Management of PII	33
Appendix A: The Personal Information Protection and Electronic Documents Act (PIPEDA) Self-Assessment Tool	34
Appendix B: Personal Health Information Protection Act (PHIPA) Checklist	47
Appendix C: The Health Insurance Portability and Accountability Act (HIPAA)	
JOURNAL – HIPAA Compliance Checklist	52
Note	53
CHAPTER 3 DATA PROTECTION	54
E-Commerce	54
Types of Reported Breaches	55
Data Protection	57
Scope, Penalties and Key Definitions	61
Legal Terms	61
Data Protection Principles	61
Accountability	62
Data Security	63
Data Protection by Design and by Default	63
Processing Data	63
Consent	63
Data Protection Officers	64
An Individual's Privacy Rights	64
CHAPTER 4 THIRD-PARTY RISK MANAGEMENT	72
Government Regulations: Third-Party Risk Management Requirements	72
Governance	73
Accountability	73
Third-Party Risk Management Framework (TPRMF)	74
Management of Third-Party Risk	75

Risk-Based Approach	76
Risk Identification and Assessment	77
Risk Management and Mitigation	80
Monitoring and Reporting	84
Special Arrangements	86
Standardised Contracts	86
No Written Contract	86
Digital Operational Resilience Act (DORA)	86
ICT Risk Management	87
ICT Third-Party Risk Management	87
Digital Operational Resilience Testing	87
Information Sharing	87

CHAPTER 5 TECHNOLOGY AND CYBER RISK 88

Technology and Cyber Risk in Third-Party Arrangements	88
Clear Roles and Responsibilities Are Established for	
Technology and Cyber Controls	88
Third Parties Comply with the Organisation's	
Technology and Cyber Standards	88
Cloud-Specific Requirements Are Established	89
Cloud Portability Is Considered	89
Governance and Risk Management	89
Accountability and Organisational Structure	89
Technology and Cyber Strategy	90
RMF Is Well-Aligned and Continuously Improved	91
Technology Operations and Resilience	92
Technology Architecture	92
Technology Project Management	94
System Development Life Cycle	94
Change and Release Management	95
Patch Management	96
Incident and Problem Management	96
Technology Service Measurement and Monitoring	97
Disaster Recovery	98
Cyber Security	99
Confidentiality, Integrity and Availability of Technology	
Assets Is Maintained	100
Identify	100
Defend	102
Detect	105
Continuous, Centralised Security Logging to Support	
Investigations	105
Respond, Recover and Learn	106

CHAPTER 6 GOVERNANCE 108

Guiding Principles of Corporate Governance	108
Enterprise Risk Management Framework	110
Internal Environment	110

Common Language around Risk	110
Risk Management Steering Committee	111
Objective Setting	112
ERM Methodology	112
Risk Appetite	112
Risk Tolerance	112
Event Identification	112
Risk Assessment	113
Quantitative Risk Assessment	113
Risk Calculation	113
Qualitative Risk Assessment	113
Risk Response	114
Control Activities	114
Risk Identification	114
Risk Prioritisation	115
Risk Mitigation Plans	115
Information and Communication	115
Monitoring	115
Risk Monitoring and Reporting	116
Scenario Planning and Stress Testing	116
Step 1: Brainstorm Future Scenarios	116
Step 2: Identify Trends and Driving Forces	116
Step 3: Create a Scenario Planning Template	117
Step 4: Develop a Scenario	117
Step 5: Evaluate a Scenario	117
Scenario Analysis	117
Step 6: Update Strategies and Policies Accordingly	119
Operational Risk Management	119
Information Security Aspects of Operational Risk	120
Cybersecurity Risk Assessment Process	120
Risk Identification	120
Identification of Assets	121
Identification of Threats	121
Identification of Existing Controls	121
Identification of Vulnerabilities	122
Identification of Consequences	122
Expressing and Measuring Risk	122
Risk Analysis	123
Risk Evaluation and Quantification	123
Risk Mitigation Planning and Verification	124
Risk Treatment	124
Risk Modification	124
Risk Transfer	124
Risk Avoidance	124
Risk Acceptance	125
Risk Remediation	125

Risk Communication	125
Risk Monitoring and Review	125
Loss Event Management	125
Security Metrics	125
Key Performance Indicators	126
Key Risk Indicators	127
Risk Culture and Risk Behaviours	127
CHAPTER 7 CYBERSECURITY RISK MANAGEMENT	
FRAMEWORK	129
Cyber Risk Investment Model	129
Technology Landscape	130
Data Classification	130
Risk Management Practices	130
Cost-Benefit Analysis for Cybersecurity Measures	130
Business Objectives	131
Cybersecurity Risk Management Framework	131
Risk Assessment Process	133
Threat Modelling	134
Risk Prioritisation: Assess the Inherent Risk	138
Assess the Internal Controls	139
Determine the Organisational Risk Appetite	144
Risk Mitigation Strategy	145
CHAPTER 8 CASE STUDY #1: CHIME LIVE	148
Questions	150
Solution: Chime Live	150
Executive Summary	150
Business Impact and Risk	151
Objective and Scope	152
Results	152
Recommendations	153
Risk Assessment	153
Privacy Laws	153
Standard Operating Procedures	154
PII Elements	154
Privacy Compliance Analysis	156
Business Driven Risk Assessment – Qualitative	
Inherent Risk	158
Business Driven Risk Assessment – Quantitative	
Inherent Risk	159
Residual Risk Rating Scale	160
Internal Control Assessment: Highly Effective	160
Technical Overview	160
SOC for Service Organisations: Trust Services	
Criteria – AWS	161
Organisation's Risk Appetite	162