

The Cybersecurity Guide to Governance, Risk, and Compliance

Jason Edwards
Griffin Weaver

WILEY

An abstract visualization of a network or data flow, featuring a dense web of blue and white lines and nodes, with some yellow highlights, set against a dark blue background.

The Cybersecurity Guide to Governance, Risk, and Compliance

The Cybersecurity Guide to Governance, Risk, and Compliance

Dr. Jason Edwards

New Braunfels
TX, USA

Griffin Weaver

San Antonio
TX, USA

WILEY

This edition first published 2024
© 2024 John Wiley & Sons Ltd.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by law. Advice on how to obtain permission to reuse material from this title is available at <http://www.wiley.com/go/permissions>.

The right of Jason Edwards and Griffin Weaver to be identified as the authors of the editorial material in this work has been asserted in accordance with law.

Registered Offices

John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA

John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

Limit of Liability/Disclaimer of Warranty

While the publisher and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives, written sales materials or promotional statements for this work. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for your situation. You should consult with a specialist where appropriate. The fact that an organization, website, or product is referred to in this work as a citation and/or potential source of further information does not mean that the publisher and authors endorse the information or services the organization, website, or product may provide or recommendations it may make. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Library of Congress Cataloging-in-Publication Data applied for

Hardback ISBN: 9781394250196

Cover Design: Wiley

Cover Image: © Andriy Onufriyenko/Getty Images

Set in 10.5/13pt Muli by Straive, Chennai, India

Dedication by Griffin Weaver

As I present this book on cybersecurity and governance, coauthored with immense dedication and passion, my thoughts turn not only to the profound complexities of our digital world but also to the incredible journey that has led me here. As a legal expert deeply entrenched in the nuances of cybersecurity, I've embarked on this endeavor with a singular purpose: to bridge the gap between theoretical knowledge and practical application in a field that is as challenging as it is essential.

To my wife, Whitney, and our three children, Harper, Gideon, and Flynn, my journey in this field is a testament to the balance between pursuing professional passions and cherishing the invaluable support of family. It is with this balanced perspective that I've approached the writing of this book, aiming to infuse it not just with legal and technical insights but also with the underlying values of dedication, curiosity, and perseverance.

Cybersecurity and the law are not just areas of professional interest to me; they are vital pillars upon which our digital society rests. In writing this book, my hope is to illuminate these complex subjects for a diverse audience, from students who are just beginning their academic pursuits to seasoned practitioners looking to deepen their understanding and enhance their skills.

The landscape of cybersecurity is ever-evolving, and with it, the legal frameworks that govern our digital interactions. It is my earnest desire that this book serves as a beacon, guiding readers through the intricacies of cybersecurity and governance with clarity, depth, and relevance. May it inspire you to explore further, question deeper, and contribute to the shaping of a secure, ethical digital future.

Dedication by Jason Edwards

This book is dedicated to my family, whose unwavering support and love have been the cornerstone of my endeavors; to my wife, Selda, whose wisdom and strength have been my guiding light; and to my children, Michelle, Chris, Ceylin, and Mayra, who inspire me daily to be the best version of myself. The book is a testament to my professional journey and a reflection of the values and resilience you have instilled in me.

I acknowledge my fellow veterans and colleagues in the cybersecurity community, who have been comrades and mentors on this challenging yet rewarding path. Your camaraderie and insights have been invaluable in shaping the perspectives shared on these pages. A special acknowledgment goes out to those who serve in silence, dedicating their lives to the safety and security of our digital world.

This book is also dedicated to educators, students, and professionals in cybersecurity and related fields. May this work serve as a beacon, guiding you through the complexities of governance, risk, and compliance in our ever-evolving digital landscape. Your commitment to learning and adapting will drive us forward in these unprecedented times.

And, with a wry smile, I dedicate this book to the indomitable spirits of the “A7” project team. For two years, we waded through a quagmire of confusion and challenges that often teetered on the edge of chaos. Yet, against all odds, we emerged victorious. This dedication is a salute to our collective perseverance, ingenuity, and slightly warped sense of humor that saw us through the hellish yet unforgettable adventure of “A7.”

Contents

	Purpose of the Book	xvii
	Target Audience	xix
	Structure of the Book	xxi
	Foreword by Wil Bennett	xxiii
	Foreword by Gary McAlum	xxv
	Acknowledgments	xxvii
CHAPTER 1	Governance, Risk Management, and Compliance	1
	Understanding GRC	1
	The Business Case for GRC	3
	Governance: Laying the Foundation	4
	Risk Management: Managing Uncertainties	5
	Compliance: Adhering to Regulations and Standards	7
	The Intersection of Governance, Risk, and Compliance	8
	GRC Frameworks and Standards	9
	GRC Tools and Technologies	12
	Building a GRC Culture	14
	The Role of GRC in Strategic Planning	15
	Chapter Conclusion	16
	Case Study: GRC Implementation at SpectraCorp	17
CHAPTER 2	The Landscape of Cybersecurity	19
	Comprehensive Overview of Cybersecurity Maturity	19
	Cybersecurity in the Financial Industry	21
	Cybersecurity in the Healthcare Industry	23
	Cybersecurity in the Government Sector	25
	Cybersecurity in Small to Large Enterprises	28
	Chapter Conclusion	30
	Case Study: TechGiant Inc.'s Holistic Approach to Information Security	31
CHAPTER 3	Cybersecurity Leadership: Insights and Best Practices	33
	The Essential Traits of a Cybersecurity Leader	33
	Building and Leading Effective Cybersecurity Teams	35
	Adapting to Emerging Trends in Cybersecurity Leadership	36
	Strategic Decision-Making in Cybersecurity Leadership	37
	Developing the Next Generation of Cybersecurity Leaders	39
	Personal Development for Cybersecurity Leaders	40

	Incident Management and Crisis Leadership	42
	Leading Cybersecurity Culture and Awareness	43
	The Ethical Dimension of Cybersecurity Leadership	44
	Balancing Business Objectives and Cybersecurity	46
	Learning from Military Leadership	48
	Future Trends and Preparing for What's Next	49
	Chapter Conclusion	51
	Case Study: The Transformation of Cybersecurity Leadership at CyberFusion Inc.	51
CHAPTER 4	Cybersecurity Program and Project Management	53
	Program and Project Management in Cybersecurity	53
	Types of Cybersecurity Projects	55
	Project Management Fundamentals Applied to Cybersecurity	56
	Agile Project Management for Cybersecurity	58
	Managing Cybersecurity Programs	59
	Communication and Collaboration in Cybersecurity Projects	61
	A Guide for Project Managers in Cybersecurity	63
	Chapter Conclusion	65
	Case Study: Proactive Program Management at Acme Tech	66
CHAPTER 5	Cybersecurity for Business Executives	69
	Why Business Executives Need to Be Involved in Cybersecurity	69
	Roles and Responsibilities of Business Executives in Cybersecurity	71
	Effective Collaboration Between Business Executives and Cybersecurity Teams	73
	Key Cybersecurity Concepts for Business Executives	74
	Incorporating Cybersecurity into Business Decision-Making	76
	Developing a Cybersecurity Risk Appetite	78
	Training and Awareness for Business Executives	80
	Legal and Regulatory Considerations for Business Executives	81
	The Future of Business Executive Engagement in Cybersecurity	83
	Chapter Conclusion	84
	Case Study: Engaging Cybersecurity at Spectrum Enterprises	85
CHAPTER 6	Cybersecurity and the Board of Directors	87
	The Critical Role of the Board in Cybersecurity	87
	Perspectives from the Board of Directors	89
	Perspectives from Cybersecurity Executives	91
	The Board's Responsibilities in Cybersecurity	92
	Effective Communication Between the Board and Cybersecurity Executives	94
	Specific Recommendations for Reporting to the Board	96

	Insights from the FFIEC and Other Standards on Board Involvement	97
	Cybersecurity Governance: Embedding Cybersecurity in Corporate Culture	98
	Legal and Regulatory Considerations for the Board	100
	The Future of Board Involvement in Cybersecurity	101
	Chapter Conclusion	103
	Case Study: Cybersecurity Board Governance at TechPioneer Inc.	104
CHAPTER 7	Risk Management	109
	Risk Management in the Business	109
	Understanding the Risk Management Life Cycle	111
	FFIEC Handbooks and Risk Management Guidance	112
	Governance and Risk Management Framework	115
	Risk Approvals and the Role of Committees	117
	Risk Identification and Analysis	118
	Third-Party Risk Management	120
	Regulatory Expectations for Third-Party Risk Management	122
	Compliance and Legal Risk Management	124
	Monitoring and Reporting	126
	Chapter Conclusion	127
	Case Study: Navigating Risk Management at Phoenix Innovations	128
CHAPTER 8	The NIST Risk Management Framework	131
	The NIST Risk Management Framework	131
	Understanding RMF's Authorization Process	133
	NIST RMF in Practice: Step-by-Step Analysis	134
	Applicability to Regulatory Expectations	136
	Integrating NIST RMF into an Organization	137
	Using NIST RMF for Risk Assessment and Management	139
	NIST RMF and Technology Implementation	141
	Challenges and Solutions in Implementing NIST RMF	142
	NIST RMF and Third-Party Risk Management	144
	Chapter Conclusion	145
	Case Study: OmniTech Corporation and NIST RMF Implementation	146
	Sample RMF Authorization Document Package	147
CHAPTER 9	Cybersecurity Metrics	151
	Understanding Cybersecurity Metrics	151
	The Importance of Metrics in Cybersecurity	154
	The Role of Metrics in Decision-Making and Resource Allocation	155
	Differentiating Between KPIs and KRIs	157
	The Role of Metrics in Compliance	159
	Challenges and Considerations	161
	Key Performance Indicators (KPIs)	162

	Key Risk Indicators (KRIs)	164
	Integrating KPIs and KRIs into Cybersecurity Strategy	166
	Chapter Conclusion	168
	Case Study: Transforming TechNova's Defense Landscape	169
CHAPTER 10	Risk Assessments	171
	The Importance of Risk Assessments	171
	The FFIEC's Perspective on Risk Assessments	173
	NIST's Approach to Risk Assessments	175
	Risk Assessment Frameworks	177
	Conducting a Cybersecurity Risk Assessment	179
	Managing Third-Party Risks	180
	Challenges and Best Practices in Risk Assessments	182
	Chapter Conclusion	185
	Case Study: Utilizing Risk Assessments in Cybersecurity: The Journey of Innovative Tech Solutions	186
	Risk Assessment Template Example	188
CHAPTER 11	NIST Cybersecurity Framework	191
	Background on the NIST CSF	191
	Core Functions and Categories	193
	Implementation Tiers	196
	Profiles	199
	Implementation	202
	Chapter Conclusion	205
	Case Study: Cybersecurity Journey of TechPulse Inc.	206
CHAPTER 12	Cybersecurity Frameworks	209
	ISO/IEC 27001: Information Security Management	209
	COBIT (Control Objectives for Information and Related Technologies)	210
	CMMC (Cybersecurity Maturity Model Certification)	212
	CIS (Center for Internet Security) Controls	213
	PCI DSS (Payment Card Industry Data Security Standard)	214
	ICFR (Internal Control Over Financial Reporting)	216
	Cloud Security Alliance Controls	218
	ISO 27017: Code of Practice for Information Security Controls	219
	ISO 27701: Privacy Information Management	220
	Comparing and Integrating Different Cybersecurity Frameworks	221
	Future Trends in Cybersecurity Frameworks	223
	Chapter Conclusion	225
	Case Study: Securing Globex Corporation Top Strengths of Each Framework	226
		227
CHAPTER 13	NIST SP 800-53: Security and Privacy Controls Framework	231
	Overview of NIST SP 800-53	231

Structure and Organization of NIST SP 800-53	232
Understanding Controls and Control Families	234
Chapter Conclusion	235
Case Study: SecureTech Solutions	236
NIST 800-53 Control Families and Descriptions	237
CHAPTER 14 The FFIEC: An Introduction	245
FFIEC History and Background	245
Role and Responsibilities	247
Understanding the FFIEC Examination Handbooks	249
The FFIEC Cybersecurity Assessment Tool (CAT)	250
The FFIEC Audit Handbook	252
The FFIEC Business Continuity Handbook	254
The FFIEC Development and Acquisition Handbook	255
The FFIEC Information Security Handbook	257
The FFIEC Management Handbook	258
The Architecture, Infrastructure, and Operations Handbook	259
The Outsourcing Technology Services Handbook	261
The Retail Payment Systems Handbook	262
The Supervision of Technology Service Providers Handbook	263
The Wholesale Payment Systems Handbook	264
Chapter Conclusion	265
CHAPTER 15 U.S. Federal Cybersecurity Regulations	267
Gramm–Leach–Bliley Act (GLBA)	267
The Health Insurance Portability and Accountability Act (HIPAA)	268
Interagency Guidelines Establishing Information Security Standards (12 CFR 30 Part B)	270
Payment Card Industry Data Security Standard (PCI DSS)	271
Sarbanes–Oxley Act (SOX)	273
The Cloud Act	274
Internal Revenue Service Publication 1075	275
Criminal Justice Information Services (CJIS) Security Policy	277
Defense Federal Acquisition Regulation Supplement (DFARS)	278
Department of Defense Cloud Computing Security Requirements Guide	279
Family Educational Rights and Privacy Act (FERPA)	280
Sec Rules 17A-4 and 18A-6	280
Section 508	281
Federal Information Security Management Act (FISMA)	282
Federal Information Processing Standard (FIPS) 140-2	283
Chapter Conclusion	284
Case Study: CyberSecure’s Compliance Journey	285
CHAPTER 16 State-level Cybersecurity Regulations	287
State-Level Cybersecurity Regulations	287
Harmonizing State and Federal Compliance	289
Future Developments	290

Notable State Regulations	292
Chapter Conclusion	295
Case Study: Cyberguard's Path to Compliance	296
CHAPTER 17 International Cybersecurity Laws and Regulations	299
International Cybersecurity Laws	299
General Data Protection Regulation (GDPR) – European Union	301
Personal Information Protection and Electronic PIPEDA – Canada	303
The Data Protection Act – United Kingdom	305
The Cybersecurity Law – China	307
The Personal Data Protection Act – Singapore	309
Other Notable International Cybersecurity Laws	310
Coordinating Global Cybersecurity Compliance Efforts	311
Chapter Conclusion	313
Case Study: CyberShield Corporation	313
CHAPTER 18 Privacy Laws and Their Intersection with Cybersecurity	315
The Intersection of Privacy and Cybersecurity	315
Privacy and Data Protection	317
Key Privacy Principles	318
Privacy Laws in the United States	320
International Privacy Laws and Regulations	321
Privacy by Design and by Default	323
Challenges in Maintaining Privacy and Security Compliance	325
Tools and Frameworks for Privacy Management	326
Chapter Conclusion	328
Case Study: Privacy and Cybersecurity at DataSage Inc.	329
Example Privacy Impact Assessment	330
CHAPTER 19 Auditing Cybersecurity: Guides for Auditors and the Audited	333
The Evolving Role of Auditors in Cybersecurity	333
Understanding Cybersecurity: Essential Concepts for Auditors	335
The Audit Charter and Audit Engagement	336
Risk-Based Auditing Approach in Cybersecurity	338
Evaluating Internal Controls for Cybersecurity	339
Testing and Sampling Techniques in Cybersecurity Auditing	340
Compliance With Legal and Regulatory Requirements	342
Reporting and Communication of Audit Findings	344
Consideration of Third-Party Relationships	346
Quality Assurance and Improvement Program	347
Professional Ethics, Skills, and Continuing Education	348

	Best Practices for Cybersecurity Executives and Teams	
	When Interfacing With Auditors	351
	Chapter Conclusion	353
	Case Study: Cybersecurity Audit at Techsphere Inc.	354
CHAPTER 20	The Challenging Role of the Regulator	355
	The Paramount Role of the Regulator in Cybersecurity	355
	Identifying Key Focus Areas in Cybersecurity for Regulators	357
	Utilizing FFIEC Work Papers Effectively	359
	Developing Effective Communication Strategies	360
	Continuous Improvement and Adaptation for Regulators	362
	Staying Informed and Continuously Learning as Regulators	364
	Providing Support and Guidance to the Business	365
	Challenges Faced by Regulators and How to	
	Overcome them	367
	Regulatory Excellence and Forward-Looking Leadership	369
	Becoming a Regulator: Selection, Education, and	
	Career Paths	370
	Balancing Objectivity and Advocacy	372
	Chapter Conclusion	374
	Case Study: Zephyr Tech	375
CHAPTER 21	Understanding US Regulatory Bodies	377
	Federal Financial Institutions Examination Council (FFIEC)	377
	Office of the Comptroller of the Currency (OCC)	379
	Board of Governors of the Federal Reserve System	380
	Federal Deposit Insurance Corporation (FDIC)	382
	Consumer Financial Protection Bureau (CFPB)	384
	Securities and Exchange Commission (SEC)	385
	Financial Industry Regulatory Authority (FINRA)	387
	National Credit Union Administration (NCUA)	388
	The Federal Trade Commission	390
	Chapter Conclusion	391
	Online Regulatory Resources	392
CHAPTER 22	Managing Regulatory Visits and Requests	
	for Information	395
	Regulatory Visits and Requests for Information	395
	Preparing for Regulatory Visits	397
	Responding to Requests for Information	398
	Best Practices During Regulatory Visits	400
	Developing Internal Processes for Managing	
	Regulatory Requests	402
	Building and Maintaining Relationships With Regulators	404
	Chapter Conclusion	405
	Case Study: Orchid Technologies	406

CHAPTER 23	Understanding Regulatory Penalties	409
	Overview of Regulatory Penalties	409
	Regulatory Penalties and Enforcement Actions	410
	Understanding the Authority Behind Enforcement Actions	412
	The Importance of Understanding Penalties as Part of Compliance Efforts	414
	Matters Requiring Attention (MRAS)	416
	Consent Orders	417
	Civil Money Penalties (CMPS)	419
	Cease and Desist Orders	420
	Other Enforcement Actions	422
	Other Enforcement Actions	423
	Chapter Conclusion	425
	Case Study: Phoenix Corporation and Robust Compliance	426
CHAPTER 24	Addressing and Remediating Regulatory Findings	429
	Receiving and Reviewing Regulatory Feedback and Findings	429
	Creating a Remediation Plan	431
	Allocating Resources and Responsibilities for Remediation	433
	Monitoring Progress and Compliance	435
	Reporting Back to the Regulator	436
	Chapter Conclusion	438
	Case Study: XYZ Corporation's Remediation Plan	439
	Example Regulatory Finding Remediation Plan	440
CHAPTER 25	Cybersecurity Architecture	445
	Cybersecurity Architecture	445
	Fundamental Concepts	447
	Architectural Components and Layers	449
	Security Reference Models and Frameworks	454
	Building and Evolving Cybersecurity Architecture	456
	Adapting Architecture to Emerging Threats	457
	Chapter Conclusion	459
	Case Study: Orchid Enterprises and Robust Cybersecurity	461
CHAPTER 26	Risk Mitigation	463
	Risk Mitigation Basics	463
	Policies, Standards, and Procedures	465
	Inventory and Classification of Assets	466
	Mitigating Interconnectivity Risk	467
	User Security Controls	469
	Physical Security	471
	Network Controls	472
	Change Management Within the IT Environment	474
	End-of-Life Management	477
	Chapter Conclusion	478
	Case Study: Risk Mitigation at SkyTech Solutions	479

CHAPTER 27	Cloud Security	481
	Cloud Computing	481
	Major Cloud Service Providers	483
	Types of Cloud Services	485
	Cloud Security Challenges	487
	Security Tools and Techniques for Cloud Environments	489
	Cloud Security Standards and Best Practices	491
	Future Trends in Cloud Security	493
	Chapter Conclusion	494
	Case Study: Moving to the Cloud with Aurora Innovations	495
CHAPTER 28	Artificial Intelligence in Cybersecurity	497
	Unraveling the AI-Cybersecurity Conundrum	497
	A Historical Tapestry: Tracing the Origins and Evolution of AI	499
	The AI Revolution: Transforming Cyber Defense	502
	AI-Powered Cybersecurity Solutions	503
	Chapter Conclusion	507
	Case Study: Embracing AI in Cybersecurity at FuturaTech	508
	The CISO's AI Preparation Checklist	509
CHAPTER 29	Quantum Computing: A New Frontier	511
	Quantum Computing – an Emerging Paradigm in Cybersecurity	511
	The Quantum-Cryptography Nexus: a Shift in the Cybersecurity Paradigm	513
	The Quantum Race: Strategic and Security Implications	515
	Chapter Conclusion	517
	Case Study: Preparing for Quantum	518
	The CISO's Quantum Preparation Checklist	519
CHAPTER 30	Incident Response and Recovery	521
	Planning and Preparedness	521
	Detecting and Analyzing Incidents	524
	Containment, Eradication, and Recovery	526
	Communication and Reporting Requirements	528
	Working With Legal Firms	529
	Chapter Conclusion	531
	Case Study: NexTech Corporation's Journey	532
	Example Cybersecurity Incident Response Plan – for NexTech Corporation	533
CHAPTER 31	Navigating the Cyber Insurance Maze	541
	Cyber Insurance: a Primer for Businesses	541
	Exploring the Uses and Misuses of Cyber Insurance	543
	The Complex Dance of Claim Settlement: Unraveling the Truth	545

Chapter Conclusion	546
Case Study: Navigating the Cyber Insurance Maze with TechGuard Inc.	547
Glossary	549
Cybersecurity Resources	555
Ready to Use KPI Examples	567
Ready to Use KRI Examples	599
The End	631
Index	633

Purpose of the Book

The first step in any journey of understanding is to clarify the why. This book was born out of a need for comprehensive yet practical insights into cybersecurity governance, risk management, and compliance. Navigating these complex domains can be a daunting task without a reliable roadmap. This book aims to guide, elucidating the pathways through the labyrinth of cyber threats and security measures, organizational policies, and regulatory requirements.

This book aims to bridge the knowledge gaps in the dynamic cybersecurity field. While many resources tackle the subject, they often focus on a narrow aspect, leaving you to stitch together various pieces of information. This guide takes a different approach to provide a holistic understanding of cybersecurity from a governance, risk, and compliance perspective.

A critical aspect of cybersecurity is compliance. Compliance is not just about checking off boxes on a list. Instead, it is about integrating practices safeguarding an organization's data and digital assets. This book strives to provide insights that can elevate an organization's compliance activities from mere tasks to strategic initiatives, thus enhancing the resilience of the enterprise against cyber threats.

Professional development is a continual process. The pace of technological change necessitates that professionals in the field of cybersecurity continually upgrade their skills and understanding. This book is designed to be a valuable tool in that process, providing in-depth insights and practical approaches that can be applied in various professional settings.

The regulatory landscape related to cybersecurity is multifaceted and ever-evolving. Without a clear understanding of these complexities, an organization can easily find itself noncompliant and vulnerable. This book aims to aid you in navigating this challenging environment, providing you with the knowledge needed to build a cybersecurity program that aligns with regulatory requirements.

While this book strongly focuses on financial compliance, the insights and guidance can be applied to all industries. Cyber threats and the need for effective cybersecurity measures are universal issues impacting businesses of all sizes and sectors. Therefore, this guide can be beneficial for a diverse range of professionals.

Finally, this book is not just about learning but also about sharing experiences. You contribute to the book's purpose by exploring the content and applying the insights in your professional environment. By adding your expertise to the collective wisdom, you can help others navigate their cybersecurity journey.

Target Audience

The subject of cybersecurity touches a wide range of professionals. One of the key strengths of this book is its cross-industry applicability, which means it can benefit a diverse audience. This guide targets cybersecurity professionals, from those beginning their careers to seasoned experts. It provides foundational knowledge and in-depth insights into cybersecurity governance, risk, and compliance.

Compliance officers are another primary audience for this book. These professionals ensure that their organizations adhere to the necessary regulations and standards. Compliance officers can more effectively align their practices with the organization's cyber risk management efforts with a clear understanding of cybersecurity principles.

IT professionals can gain substantial value from this guide, whether directly involved in cybersecurity or not. Cybersecurity is not a stand-alone function; it is deeply interwoven with other IT practices. Therefore, understanding cybersecurity principles can aid IT professionals in designing, implementing, and maintaining systems and networks that are resilient against cyber threats.

For business executives, understanding cybersecurity is about much more than technology; it is about ensuring business continuity and preserving stakeholder trust. This book aims to give executives the knowledge they need to make informed decisions related to cybersecurity and drive cyber risk governance in their organizations.

The book is equally valuable for boards of directors. Boards are responsible for overseeing risk, including cyber risk. With the knowledge in this guide, board members can play a more active role in directing their organization's cybersecurity strategy and ensuring compliance with relevant regulations.

Legal professionals can also find value in this book. As laws and regulations related to cybersecurity continue to evolve, legal professionals must stay informed. This guide can help them understand cybersecurity's technological and compliance aspects, enabling them to provide more practical advice and support to their clients or organizations.

Regulators are the final primary audience for this book. Effective regulation requires a deep understanding of the subject being regulated. This guide can support regulators in developing and implementing effective cybersecurity regulations by providing comprehensive insights into cybersecurity from a governance, risk, and compliance perspective.

Structure of the Book

As authors, we have crafted this book to offer a well-rounded and engaging journey through cybersecurity governance, risk, and compliance. The book is thoughtfully divided into specific sections, each concentrating on a unique aspect of the subject. These sections are filled with in-depth discussions, practical tips, and real-world examples that help bring the subject to life.

Our book is not just for sequential reading from cover to cover. We have designed it so you can read specific sections depending on your immediate needs or interests. Each chapter is independent, providing a focused exploration of a distinct cybersecurity dimension. This means you can always revisit or explore new sections at your own pace and according to your requirements.

Throughout the book, we have highlighted key themes such as the crucial role of cybersecurity in an organization's strategy, the use of risk management in cyber defense, and the importance of compliance in safeguarding against cyber threats. We believe that understanding these themes is fundamental to grasping the complex world of modern cybersecurity.

We've also included over 70 Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs) and references to relevant regulations, standards, and online resources. These additions are intended to aid you in measuring your cybersecurity efforts and to provide extra material for your learning.

We want you to understand and act on what you learn. So, after each section, we offer a few actionable recommendations. With over 1300 suggestions in the book, we are equipping you with the tools to translate the knowledge into practical steps.

One of our favorite features of the book is the real-life case studies and examples. They illustrate the concepts we are discussing and help you envision how they can be applied in real-world situations.

Finally, we have mapped the Federal Financial Institutions Examination Council (FFIEC) Information Security Handbook to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). This will serve as a guide, helping you navigate these critical regulatory and guidance documents. It will enable you to understand their connections and overlaps for an efficient approach to compliance, thus bolstering your cybersecurity stance.

Foreword by Wil Bennett

Over the past 30 years in cybersecurity, I've witnessed its transformation from a simple defense mechanism to an intricate architecture interwoven with governance, risk, compliance, leadership, technology, and business strategies. This evolution was unimaginable three decades ago.

Having worked extensively in crafting and steering cybersecurity strategies, I've been fortunate to observe the expertise and dedication of Jason and Griffin closely. Their combined strengths in cybersecurity strategy, regulatory remediation, and legal aspects have proved crucial in meeting contemporary cybersecurity challenges.

The Cybersecurity Guide to Governance, Risk, and Compliance represents the wealth of knowledge and practical insights that Jason and Griffin possess. Having collaborated with Jason at USAA, I can attest to his unwavering commitment and strategic expertise in cybersecurity, especially in regulatory remediation. Similarly, Griffin's expertise in legal aspects has significantly shaped our understanding of cybersecurity laws and regulations.

This book delves deeply into the multifaceted realm of cybersecurity in today's age. Designed for professionals across the board, from seasoned cybersecurity veterans to business leaders, auditors, and regulators, this guide integrates the latest technological insights with governance, risk, and compliance (GRC). Every chapter brims with actionable recommendations from the authors' vast experience and forward-thinking vision.

Readers will find a comprehensive range of topics, from key performance indicators and cutting-edge technological advancements to risk management strategies and regulatory insights. This book stands not just as a testament to the knowledge of Dr. Jason Edwards and Griffin Weaver but also as a beacon guiding those eager to navigate current and future cybersecurity challenges.

In sum, this book is more than a text – it's an enlightening compass for traversing the dynamic terrain of cybersecurity governance, risk management, and compliance. I wholeheartedly endorse this guide as a pivotal resource for anyone striving for cybersecurity excellence and resilience.

—Wil Bennett
Vice President,
Chief Information Security Officer
CISSP

Foreword by Gary McAlum

In an era of constant digital evolution and deepening ties between governance, risk, compliance, and cybersecurity, *The Cybersecurity Guide to Governance, Risk, and Compliance* emerges as a pivotal resource. This guide combines practical insights with actionable strategies, providing a detailed road map through the complexities of modern cybersecurity.

During my tenure as Chief Security Officer at USAA, I had the privilege of working with Griffin Weaver and Dr. Jason Edwards. Griffin's expertise as a cyber attorney enhanced our cybersecurity strategies, ensuring their robustness and alignment with regulatory requirements. Dr. Jason Edwards' strategic approach and practical experiences significantly contributed to our efforts, and their insights are evident in this book.

Jason and Griffin have crafted a versatile guide suitable for beginners, educators, cybersecurity professionals, and executive leaders. With over 1300 actionable recommendations, KPIs, and KRIs, it offers a comprehensive route to a more secure cyber environment. From my role as Chief Information Security Officer, I appreciate the guide's exploration of cutting-edge topics like AI, cloud, and quantum computing, providing insights into their potential impacts on security and compliance.

This guide's coverage of governance, leadership, legal frameworks, and regulatory nuances ensures organizations can establish resilient cybersecurity postures. Each chapter delivers actionable knowledge, making the guide thorough and practical.

In summary, this book is a testament to the authors' expertise and commitment to advancing cybersecurity knowledge. It's a valuable resource for anyone in the field of cybersecurity, governance, risk, and compliance.

—Gary McAlum
Senior Vice President,
Chief Information Security Officer
CISSP

Acknowledgments

This journey of writing “Mastering Cybersecurity” has been one of profound learning, discovery, and collaboration. It would not have been possible without the unwavering support of my family and the invaluable insights from a remarkable community of cybersecurity professionals.

First and foremost, I extend my deepest gratitude to my family—my wife, Selda, and our four children, Michelle, Chris, Ceylin, and Mayra. Your love, patience, and encouragement have been my anchor and inspiration through the countless hours dedicated to this project.

I also wish to express my sincere thanks to the incredible individuals I have had the privilege of meeting and working within cybersecurity. Each of you has contributed to this book in ways words can hardly capture:

Wil Bennet
Gary McAlum
Rob Fisher
Wendell Ladd
Brady Justice
Kurt Lubelan
Kim Kemp
Don Wuebben
Brennan Holland, Esq.
Derek Burkes
Amy Reed
Kanishk Mehta
Chris Gile
Jodi Marlette
Dr. Patrick Woods
Dr. Paul Cooper
Joe Arthur
Mike Stewart
Eric Fisch
Sandra Cerda
Jason Witty
Jeff Spaeth
Clark Cummings
Selda Edwards
Derek Burkes (acknowledged twice for their exceptional contribution)
Meltem Burkes

Clarke Cummings
Kristyn Lette
Chinho Ko
Subash Poudyal, PhD
Kul Subedi, PhD
Jim Huseman
Gordon Bjorman
Dr. Angela Dogan
Jerry Smith
Leead Negri
Kesha Lindbergdashwork
Michael Castillo
Kelley Dadah

Your expertise, enthusiasm, and willingness to share knowledge have enriched this book and contributed to our cybersecurity community's growth and resilience.

To those embarking on or considering a career in cybersecurity, let this book serve not just as a guide but as a testament to the power of collaboration, curiosity, and continuous learning. The path to mastering cybersecurity is challenging but immensely rewarding. It offers the opportunity to impact safeguarding our digital world significantly. May you find inspiration in these pages and from the people mentioned above to pursue your passions, overcome obstacles, and contribute to a safer, more secure future for all.

Thank you, one and all, for being part of this journey.
Warmest regards,
Dr. Jason Edwards