

Cyber Security Management A Governance Risk And Compliance Framework

This book will address the cybersecurity and cooperate governance challenges associated with enterprises, providing a bigger picture of the concepts, intelligent techniques, practices, and open research directions in this area.

Cyber Security Management places security management in a holistic context and outlines how the strategic marketing approach can be used to underpin cyber security in partnership arrangements. The book is unique because it integrates material that is of a highly specialized nature but which can be interpreted by those with a non-specialist background in the area. Indeed, those with a limited knowledge of cyber security will be able to develop a comprehensive understanding of the subject and will be guided into devising and implementing relevant policy, systems and procedures that make the organization better able to withstand the increasingly sophisticated forms of cyber attack.

Past events have shed light on the vulnerability of mission-critical computer systems at highly sensitive levels. It has been demonstrated that common hackers can use tools and techniques downloaded from the Internet to attack government and commercial information systems. Although threats may come from mischief makers and pranksters, they are more

This new volume, Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with Information Security Standard, looks at information security management system standards, risk management associated with information security, and information security awareness within an organization. The authors aim to improve the overall ability of organizations to participate, forecast, and actively assess their information security circumstances. It is important to note that securing and keeping information from parties who do not have authorization to access such information is an extremely important issue. To address this issue, it is essential for an organization to implement an ISMS standard such as ISO 27001 to address the issue comprehensively. The authors of this new volume have constructed a novel security framework (ISF) and subsequently used this framework to develop software called Integrated Solution Modeling (ISM), a semi-automated system that will greatly help organizations comply with ISO 27001 faster and cheaper than other existing methods. In addition, ISM does not only help organizations to assess their information security compliance with ISO 27001, but it can also be used as a monitoring tool, helping organizations monitor the security statuses of their information resources as well as monitor potential threats. ISM is developed to provide solutions to solve obstacles, difficulties, and expected challenges associated with literacy and governance of ISO 27001. It also functions to assess the RISC level of organizations towards compliance with ISO 27001. The information provide here will act as blueprints for managing information security within business organizations. It will allow users to compare and benchmark their own processes and practices against these results shown and come up with new, critical insights to aid them in information

security standard (ISO 27001) adoption.

A Controls-Based Approach

FISMA and the Risk Management Framework

A Practical Development and Implementation Approach

Understanding Cybersecurity Management in FinTech

Information Governance and Security

The Security Leaders' Guide to Business Alignment

For many companies, their intellectual property can often be more valuable than their physical assets. Having an effective IT governance strategy in place can protect this intellectual property, reducing the risk of theft and infringement. Data protection, privacy and breach regulations, computer misuse around investigatory powers are part of a complex and often competing range of requirements to which directors must respond. There is increasingly the need for an overarching information security framework that can provide context and coherence to compliance activity worldwide. IT Governance is a key resource for forward-thinking managers and executives at all levels, enabling them to understand how decisions about information technology in the organization should be made and monitored, and, in particular, how information security risks are best dealt with. The development of IT governance – which recognises the convergence between business practice and IT management – makes it essential for managers at all levels, and in organizations of all sizes, to understand how best to deal with information security risk. The new edition has been full updated to take account of the latest regulatory and technological developments, including the creation of the International Board for IT Governance Qualifications. IT Governance also includes new material on key international markets – including the UK and the US, Australia and South Africa.

Cyber Security Management A Governance, Risk and Compliance Framework Routledge

This book concentrates on a wide range of advances related to IT cybersecurity management. The topics covered in this book include, among others, management techniques in security, IT risk management, the impact of technologies and techniques on security management, regulatory techniques and issues, surveillance technologies, security

policies, security for protocol management, location management, GOS management, resource management, channel management, and mobility management. The authors also discuss digital contents copyright protection, system security management, network security management, security management in network equipment, storage area networks (SAN) management, information security management, government security policy, web penetration testing, security operations, and vulnerabilities management. The authors introduce the concepts, techniques, methods, approaches and trends needed by cybersecurity management specialists and educators for keeping current their cybersecurity management knowledge. Further, they provide a glimpse of future directions where cybersecurity management techniques, policies, applications, and theories are headed. The book is a rich collection of carefully selected and reviewed manuscripts written by diverse cybersecurity management experts in the listed fields and edited by prominent cybersecurity management researchers and specialists.

"This textbook places cyber security management within an organizational and strategic framework, enabling students to develop their knowledge and skills for a future career. The reader will learn to: evaluate different types of cyber risk, carry out a threat analysis and place cyber threats in order of severity, formulate appropriate cyber security management policy, establish an organization-specific intelligence framework and security culture, devise and implement a cyber security awareness programme, and integrate cyber security within an organization's operating system. Learning objectives, chapter summaries and further reading in each chapter provide structure and routes to further in-depth research. Firm theoretical grounding is coupled with short problem-based case studies reflecting a range of organizations and perspectives, illustrating how the theory translates to practice, with each case study followed by a set of questions to encourage understanding and analysis. Non-technical and comprehensive, this textbook shows final year undergraduate students and postgraduate students of Cyber Security Management, as well as reflective practitioners, how to adopt a pro-active approach to the management of cyber security. Online resources include PowerPoint slides, an instructor's manual, and a test bank of questions"--

Creating and Measuring Effective Cybersecurity Capabilities

The New Practice of Federal Cyber Security

Strategic Cyber Security Management

IT Governance and Information Security

Information Security Management Systems

Business Analytics and Cyber Security Management in Organizations

In the last decade, the proliferation of billions of new Internet-enabled devices and users has significantly expanded concerns about cybersecurity. But should we believe the prophets of cyber war or worry about online government surveillance? Are such security concerns real, exaggerated or just poorly understood? In this comprehensive text, Damien Van Puyvelde and Aaron F. Brantly provide a cutting-edge introduction to the key concepts, controversies and policy debates in cybersecurity. Exploring the interactions of individuals, groups and states in cyberspace, and the integrated security risks to which these give rise, they examine cyberspace as a complex socio-technical-economic domain that fosters both great potential and peril. Structured around ten chapters, the book explores the complexities and challenges of cybersecurity using case studies – from the Morris Worm and Titan Rain to BlackEnergy and the Cyber Caliphate – to highlight the evolution of attacks that can exploit and damage individual systems and critical infrastructures. With questions for group discussion and suggestions for further reading throughout, Cybersecurity will be essential reading for anyone interested in understanding the challenges and opportunities presented by the continued expansion of cyberspace. Security practitioners must be able to build cost-effective security programs while also complying with government regulations. Information Security Governance Simplified: From the Boardroom to the Keyboard lays out these regulations in simple terms and explains how to use control frameworks to build an air-tight information security (IS) program and governance structure. Defining the leadership skills required by IS officers, the book examines the pros and cons of different reporting structures and highlights the various control frameworks available. It details the functions of the security department and considers the control areas, including physical, network, application, business continuity/disaster recover, and identity management. Todd Fitzgerald explains how to establish a solid foundation for building your security program and shares time-tested insights about what works and what doesn't when building an IS program. Highlighting security considerations for managerial, technical, and operational controls, it provides helpful tips for selling your program to management. It also includes tools to help you create a workable IS charter and your own IS policies. Based on proven experience rather than theory, the book gives you the tools and real-world insight needed to secure your information while ensuring compliance with government regulations.

The Practical, Comprehensive Guide to Applying Cybersecurity Best Practices and Standards in Real Environments In Effective Cybersecurity, William Stallings introduces the technology, operational procedures, and management practices needed for successful cybersecurity. Stallings makes extensive use of standards and best practices documents that are often used to guide or mandate cybersecurity implementation. Going beyond these, he offers in-depth tutorials on the “how” of implementation, integrated into a unified framework and realistic plan of action. Each chapter contains a clear technical overview, as well as a detailed discussion of action items and appropriate policies. Stallings offers many pedagogical features designed to help readers master the material: clear learning objectives, keyword lists, review questions, and QR codes linking to relevant standards documents and web resources. Effective Cybersecurity aligns with the comprehensive Information Security Forum document “The Standard of Good Practice for Information Security,” extending ISF’s work with extensive insights from ISO, NIST, COBIT, other official standards and guidelines, and modern professional, academic, and industry literature. • Understand the cybersecurity discipline and the role of standards and best practices • Define security governance, assess risks, and manage strategy and tactics • Safeguard information and privacy, and ensure GDPR compliance • Harden systems across the system development life cycle (SDLC) • Protect servers, virtualized systems, and storage • Secure networks and electronic communications, from email to VoIP • Apply the most appropriate methods for user authentication • Mitigate security risks in supply chains and cloud environments This knowledge is indispensable to every cybersecurity professional. Stallings presents it systematically and coherently, making it practical and actionable.

Cyber Security Management: A Governance, Risk and Compliance Framework by Peter Trim and Yang-Im Lee has been written for a wide audience. Derived from research, it places security management in a holistic context and outlines how the strategic marketing approach can be used to underpin cyber security in partnership arrangements. The book is unique because it integrates material that is of a highly specialized nature but which can be interpreted by those with a non-specialist background in the area. Indeed, those with a limited knowledge of cyber security will be able to develop a comprehensive understanding of the subject and will be guided into devising and implementing relevant policy, systems and procedures that make the organization better able to withstand the increasingly sophisticated forms of cyber attack. The book includes a sequence-of-events model; an organizational governance framework; a business continuity management planning framework; a multi-cultural communication model; a cyber security management model and strategic management framework; an integrated governance mechanism; an integrated resilience management model; an integrated management model and system; a communication risk management strategy; and recommendations for counteracting a range of cyber threats. Cyber Security Management: A Governance, Risk and Compliance Framework

simplifies complex material and provides a multi-disciplinary perspective and an explanation and interpretation of how managers can manage cyber threats in a pro-active manner and work towards counteracting cyber threats both now and in the future.

Effective Cybersecurity

An International Guide to Data Security and ISO27001/ISO27002

A Guide to Using Best Practices and Standards

From the Boardroom to the Keyboard

Auditing Information and Cyber Security Governance

Guidance for Boards of Directors and Executive Management, 2nd Edition

Examines the governance challenges of cybersecurity through twelve, real-world case studies Through twelve detailed case studies, this superb collection provides an overview of the ways in which government officials and corporate leaders across the globe are responding to the challenges of cybersecurity. Drawing perspectives from industry, government, and academia, the book incisively analyzes the actual issues, and provides a guide to the continually evolving cybersecurity ecosystem. It charts the role that corporations, policymakers, and technologists are playing in defining the contours of our digital world. Rewired: Cybersecurity Governance places great emphasis on the interconnection of law, policy, and technology in cyberspace. It examines some of the competing organizational efforts and institutions that are attempting to secure cyberspace and considers the broader implications of the in-place and unfolding efforts—tracing how different notions of cybersecurity are deployed and built into stable routines and practices. Ultimately, the book explores the core tensions that sit at the center of cybersecurity efforts, highlighting the ways in which debates about cybersecurity are often inevitably about much more. Introduces the legal and policy dimensions of cybersecurity Collects contributions from an international collection of scholars and practitioners Provides a detailed "map" of the emerging cybersecurity ecosystem, covering the role that corporations, policymakers, and technologists play Uses accessible case studies to provide a non-technical description of key terms and technologies Rewired: Cybersecurity Governance is an excellent guide for all policymakers, corporate leaders, academics, students, and IT professionals responding to and engaging with ongoing cybersecurity challenges. Traditional marketing techniques have become outdated by the emergence of the internet, and for companies to survive in the new technological marketplace, they must adopt digital marketing and business analytics practices. Unfortunately, with the benefits of improved storage and flow of information comes the risk of cyber-attack. Business Analytics and Cyber Security Management in Organizations compiles innovative research from international professionals discussing the opportunities

and challenges of the new era of online business. Outlining updated discourse for business analytics techniques, strategies for data storage, and encryption in emerging markets, this book is ideal for business professionals, practicing managers, and students of business.

Introduction -- Enterprise Risk Management Framework -- Alignment with the Enterprise Risk Management Framework -- Risk Management Practice - Vulnerability Management -- Risk Management Practice - System Development Lifecycle -- Risk Management Practice - Business Continuity Management -- Cybersecurity Risk Management Framework -- Case Studies.

Cybersecurity threats are on the rise. As a leader, you need to be prepared to keep your organization safe. Companies are investing an unprecedented amount of money to keep their data and assets safe, yet cyberattacks are on the rise--and the problem is worsening. No amount of technology, resources, or policies will reverse this trend. Only sound governance, originating with the board, can turn the tide. Protection against cyberattacks can't be treated as a problem solely belonging to an IT or cybersecurity department. It needs to cast a wide and impenetrable net that covers everything an organization does--from its business operations, models, and strategies to its products and intellectual property. And boards are in the best position to oversee the needed changes to strategy and hold their companies accountable. Not surprisingly, many boards aren't prepared to assume this responsibility. In *A Leader's Guide to Cybersecurity*, Thomas Parenty and Jack Domet, who have spent over three decades in the field, present a timely, clear-eyed, and actionable framework that will empower senior executives and board members to become stewards of their companies' cybersecurity activities. This includes: Understanding cyber risks and how best to control them Planning and preparing for a crisis--and leading in its aftermath Making cybersecurity a companywide initiative and responsibility Drawing attention to the nontechnical dynamics that influence the effectiveness of cybersecurity measures Aligning the board, executive leadership, and cybersecurity teams on priorities Filled with tools, best practices, and strategies, *A Leader's Guide to Cybersecurity* will help boards navigate this seemingly daunting but extremely necessary transition.

The Cyber Risk Handbook

Securing an IT Organization through Governance, Risk Management, and Audit

Guidance for Information Security Managers

Challenges, Strategies, and Trends

General Strong Security Governance Through Integration and Automation

Resolving conflicts between security compliance and human behaviour

The Complete Guide to Cybersecurity Risks and Controls presents the fundamental concepts of information and communication technology (ICT) governance and control. In this book, you will learn how to create a working, practical control structure that will ensure the ongoing, day-to-day trustworthiness of ICT systems and data. The book explains how

to establish systematic control functions and timely reporting procedures within a standard organizational framework and how to build auditable trust into the routine assurance of ICT operations. The book is based on the belief that ICT operation is a strategic governance issue rather than a technical concern. With the exponential growth of security breaches and the increasing dependency on external business partners to achieve organizational success, the effective use of ICT governance and enterprise-wide frameworks to guide the implementation of integrated security controls are critical in order to mitigate data theft. Surprisingly, many organizations do not have formal processes or policies to protect their assets from internal or external threats. The ICT governance and control process establishes a complete and correct set of managerial and technical control behaviors that ensures reliable monitoring and control of ICT operations. The body of knowledge for doing that is explained in this text. This body of knowledge process applies to all operational aspects of ICT responsibilities ranging from upper management policy making and planning, all the way down to basic technology operation. Information Governance and Security shows managers in any size organization how to create and implement the policies, procedures and training necessary to keep their organization's most important asset—its proprietary information—safe from cyber and physical compromise. Many intrusions can be prevented if appropriate precautions are taken, and this book establishes the enterprise-level systems and disciplines necessary for managing all the information generated by an organization. In addition, the book encompasses the human element by considering proprietary information lost, damaged, or destroyed through negligence. By implementing the policies and procedures outlined in Information Governance and Security, organizations can proactively protect their reputation against the threats that most managers have never even thought of. Provides a step-by-step outline for developing an information governance policy that is appropriate for your organization Includes real-world examples and cases to help illustrate key concepts and issues Highlights standard information governance issues while addressing the circumstances unique to small, medium, and large companies IT governance seems to be one of the best strategies to optimize IT assets in an economic context dominated by information, innovation, and the race for performance. The multiplication of internal and external data and increased digital management, collaboration, and sharing platforms exposes organizations to ever-growing risks. Understanding the threats, assessing the risks, adapting the organization, selecting and implementing the appropriate controls, and implementing a management system are the activities required to establish proactive security governance that will provide management and customers the assurance of an effective mechanism to manage risks. IT Governance and Information Security: Guides, Standards, and Frameworks is a fundamental resource to discover IT governance and information security. This book focuses on the guides, standards, and maturity frameworks for adopting an efficient IT governance and information security strategy in the organization. It describes numerous case studies from an international perspective and brings together industry standards and research from scientific databases. In this way, this book clearly illustrates the issues, problems, and trends related to the topic while promoting the international perspectives of readers. This book offers comprehensive coverage of the essential topics, including: IT governance guides and practices; IT service management as a key pillar for IT governance; Cloud computing as a key pillar for Agile IT governance; Information security governance and maturity frameworks. In this new book, the authors share their experience to help you navigate today's dangerous information

security terrain and take proactive steps to measure your company's IT governance and information security maturity and prepare your organization to survive, thrive, and keep your data safe. It aspires to provide a relevant reference for executive managers, CISOs, cybersecurity professionals, engineers, and researchers interested in exploring and implementing efficient IT governance and information security strategies.

Information security cannot be effectively managed unless secure methods and standards are integrated into all phases of the information security life cycle. And, although the international community has been aggressively engaged in developing security standards for network and information security worldwide, there are few textbooks available that

Information Security Governance Simplified

Concepts and Practice

Politics, Governance and Conflict in Cyberspace

Guides, Standards and Frameworks

Counteracting Cyber Threats through Organizational Learning and Training

Actionable guidance and expert perspective for real-world cybersecurity The Cyber Risk Handbook is the practitioner's guide to implementing, measuring and improving the counter-cyber capabilities of the modern enterprise. The first resource of its kind, this book provides authoritative guidance for real-world situations, and cross-functional solutions for enterprise-wide improvement. Beginning with an overview of counter-cyber evolution, the discussion quickly turns practical with design and implementation guidance for the range of capabilities expected of a robust cyber risk management system that is integrated with the enterprise risk management (ERM) system. Expert contributors from around the globe weigh in on specialized topics with tools and techniques to help any type or size of organization create a robust system tailored to its needs. Chapter summaries of required capabilities are aggregated to provide a new cyber risk maturity model used to benchmark capabilities and to road-map gap-improvement. Cyber risk is a fast-growing enterprise risk, not just an IT risk. Yet seldom is guidance provided as to what this means. This book is the first to tackle in detail those enterprise-wide capabilities expected by Board, CEO and Internal Audit, of the diverse executive management functions that need to team up with the Information Security function in order to provide integrated solutions. Learn how cyber risk management can be integrated to better protect your enterprise Design and benchmark new and improved practical counter-cyber capabilities Examine planning and implementation approaches, models, methods, and more Adopt a new cyber risk maturity model tailored to your enterprise needs The need to manage cyber risk across the enterprise—inclusive of the IT operations—is a growing concern as massive data breaches make the news on an alarmingly frequent basis. With a cyber risk management system now a business-necessary requirement, practitioners need to assess the effectiveness of their current system, and measure its gap-

improvement over time in response to a dynamic and fast-moving threat landscape. The Cyber Risk Handbook brings the world's best thinking to bear on aligning that system to the enterprise and vice-a-versa. Every functional head of any organization must have a copy at-hand to understand their role in achieving that alignment.

The Growing Imperative Need for Effective Information Security Governance With monotonous regularity, headlines announce ever more spectacular failures of information security and mounting losses. The succession of corporate debacles and dramatic control failures in recent years underscores the necessity for information security to be tightly integrated into the fabric of every organization. The protection of an organization's most valuable asset information can no longer be relegated to low-level technical personnel, but must be considered an essential element of corporate governance that is critical to organizational success and survival. Written by an industry expert, Information Security Governance is the first book-length treatment of this important topic, providing readers with a step-by-step approach to developing and managing an effective information security program. Beginning with a general overview of governance, the book covers: The business case for information security Defining roles and responsibilities Developing strategic metrics Determining information security outcomes Setting security governance objectives Establishing risk management objectives Developing a cost-effective security strategy A sample strategy development The steps for implementing an effective strategy Developing meaningful security program development metrics Designing relevant information security management metrics Defining incident management and response metrics Complemented with action plans and sample policies that demonstrate to readers how to put these ideas into practice, Information Security Governance is indispensable reading for any professional who is involved in information security and assurance. The Psychology of Information Security - Resolving conflicts between security compliance and human behaviour considers information security from the seemingly opposing viewpoints of security professionals and end users to find the balance between security and productivity. It provides recommendations on aligning a security programme with wider organisational objectives, successfully managing change and improving security culture. "A much-needed service for society today. I hope this book reaches information managers in the organization now vulnerable to hacks that are stealing corporate information and even holding it hostage for ransom." - Ronald W. Hull, author, poet, and former professor and university administrator A comprehensive entity security program deploys information asset protection through stratified technological and non-technological controls. Controls are necessary for counteracting threats, opportunities, and vulnerabilities risks in a manner that reduces potential adverse effects to defined, acceptable levels. This book presents a methodological approach in the context of normative decision theory constructs and concepts with appropriate reference to standards and the

respective guidelines. Normative decision theory attempts to establish a rational framework for choosing between alternative courses of action when the outcomes resulting from the selection are uncertain. Through the methodological application, decision theory techniques can provide objectives determination, interaction assessments, performance estimates, and organizational analysis. A normative model prescribes what should exist according to an assumption or rule.

Optimal Spending on Cybersecurity Measures

The Cyber Security Handbook - Prepare for, respond to and recover from cyber attacks

Information Security Management

Rational Cybersecurity for Business

IT Governance

Why Boards Need to Lead--and How to Do It

FISMA and the Risk Management Framework: The New Practice of Federal Cyber Security deals with the Federal Information Security Management Act (FISMA), a law that provides the framework for securing information systems and managing risk associated with information resources in federal government agencies. Comprised of 17 chapters, the book explains the FISMA legislation and its provisions, strengths and limitations, as well as the expectations and obligations of federal agencies subject to FISMA. It also discusses the processes and activities necessary to implement effective information security management following the passage of FISMA, and it describes the National Institute of Standards and Technology's Risk Management Framework. The book looks at how information assurance, risk management, and information systems security is practiced in federal government agencies; the three primary documents that make up the security authorization package: system security plan, security assessment report, and plan of action and milestones; and federal information security-management requirements and initiatives not explicitly covered by FISMA. This book will be helpful to security officers, risk managers, system owners, IT managers, contractors, consultants, service providers, and others involved in securing, managing, or overseeing federal information systems, as well as the mission functions and business processes supported by those systems. Learn how to build a robust, near real-time risk management system and comply with FISMA Discover the changes to FISMA compliance and beyond Gain your systems the authorization they need Understand critical cybersecurity and risk perspectives, insights, and tools for the leaders of complex

financial systems and markets. This book offers guidance for decision makers and helps establish a framework for communication between cyber leaders and front-line professionals. Information is provided to help in the analysis of cyber challenges and choosing between risk treatment options. Financial cybersecurity is a complex, systemic risk challenge that includes technological and operational elements. The interconnectedness of financial systems and markets creates dynamic, high-risk environments where organizational security is greatly impacted by the level of security effectiveness of partners, counterparties, and other external organizations. The result is a high-risk environment with a growing need for cooperation between enterprises that are otherwise direct competitors. There is a new normal of continuous attack pressures that produce unprecedented enterprise threats that must be met with an array of countermeasures. Financial Cybersecurity Risk Management explores a range of cybersecurity topics impacting financial enterprises. This includes the threat and vulnerability landscape confronting the financial sector, risk assessment practices and methodologies, and cybersecurity data analytics. Governance perspectives, including executive and board considerations, are analyzed as are the appropriate control measures and executive risk reporting. What You'll Learn Analyze the threat and vulnerability landscape confronting the financial sector Implement effective technology risk assessment practices and methodologies Craft strategies to treat observed risks in financial systems Improve the effectiveness of enterprise cybersecurity capabilities Evaluate critical aspects of cybersecurity governance, including executive and board oversight Identify significant cybersecurity operational challenges Consider the impact of the cybersecurity mission across the enterprise Leverage cybersecurity regulatory and industry standards to help manage financial services risks Use cybersecurity scenarios to measure systemic risks in financial systems environments Apply key experiences from actual cybersecurity events to develop more robust cybersecurity architectures Who This Book Is For Decision makers, cyber leaders, and front-line professionals, including: chief risk officers, operational risk officers, chief information security officers, chief security officers, chief information officers, enterprise risk managers, cybersecurity operations directors, technology and cybersecurity risk analysts, cybersecurity architects and engineers, and compliance officers This book uncovers the idea of understanding cybersecurity management in FinTech. It commences with introducing fundamentals of FinTech and cybersecurity to readers. It emphasizes on the importance of cybersecurity for financial institutions by illustrating recent cyber breaches, attacks, and financial

losses. The book delves into understanding cyber threats and adversaries who can exploit those threats. It advances with cybersecurity threat, vulnerability, and risk management in FinTech. The book helps readers understand cyber threat landscape comprising different threat categories that can exploit different types of vulnerabilities identified in FinTech. It puts forward prominent threat modelling strategies by focusing on attackers, assets, and software and addresses the challenges in managing cyber risks in FinTech. The authors discuss detailed cybersecurity policies and strategies that can be used to secure financial institutions and provide recommendations to secure financial institutions from cyber-attacks.

The cost and frequency of cybersecurity incidents are on the rise, is your enterprise keeping pace? The numbers of threats, risk scenarios and vulnerabilities have grown exponentially. Cybersecurity has evolved as a new field of interest, gaining political and societal attention. Given this magnitude, the future tasks and responsibilities associated with cybersecurity will be essential to organizational survival and profitability. This publication applies the COBIT 5 framework and its component publications to transforming cybersecurity in a systemic way. First, the impacts of cybercrime and cyberwarfare on business and society are illustrated and put in context. This section shows the rise in cost and frequency of security incidents, including APT attacks and other threats with a critical impact and high intensity. Second, the transformation addresses security governance, security management and security assurance. In accordance with the lens concept within COBIT 5, these sections cover all elements of the systemic transformation and cybersecurity improvements.

Advances in Cybersecurity Management

Cyber Security Management

Strategies for e-Service, e-Governance, and Cybersecurity

Cybersecurity Governance

A Governance, Risk and Compliance Framework

Cybersecurity

Organizations, worldwide, have adopted practical and applied approaches for mitigating risks and managing information security program. Considering complexities of a large-scale, distributed IT environments, security should be proactively planned for and prepared ahead, rather than as used as reactions to changes in the landscape. Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions presents high-quality research papers and practice articles on management

and governance issues in the field of information security. The main focus of the book is to provide an organization with insights into practical and applied solutions, frameworks, technologies and practices on technological and organizational factors. The book aims to be a collection of knowledge for professionals, scholars, researchers and academicians working in this field that is fast evolving and growing as an area of information assurance.

Security practitioners must be able to build a cost-effective security program while at the same time meet the requirements of government regulations. This book lays out these regulations in simple terms and explains how to use the control frameworks to build an effective information security program and governance structure. It discusses how organizations can best ensure that the information is protected and examines all positions from the board of directors to the end user, delineating the role each plays in protecting the security of the organization.

This book is a comprehensive cyber security implementation manual which gives practical guidance on the individual activities identified in the IT Governance Cyber Resilience Framework (CRF) that can help organisations become cyber resilient and combat the cyber threat landscape. Start your cyber security journey and buy this book today!

IT Security governance is becoming an increasingly important issue for all levels of a company. IT systems are continuously exposed to a wide range of threats, which can result in huge risks that threaten to compromise the confidentiality, integrity, and availability of information. This book will be of use to those studying information security, as well as those in industry.

Rewired

Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions

The Complete Guide to Cybersecurity Risks and Controls

CISSP For Dummies

Transforming Cybersecurity: Using COBIT 5

A Novel Framework and Software as a Tool for Compliance with Information Security Standard

Focusing on countermeasures against orchestrated cyber-attacks, Cyber Security Culture is research-based and reinforced with insights from experts who do not normally release information into the public arena. It will enable managers of organizations across different industrial sectors and government agencies to better understand how organizational learning and training can be utilized to develop a culture that ultimately protects an organization from attacks. Peter Trim and David Upton believe that the speed and complexity of cyber-attacks demand a different approach to security management, including scenario-based planning and training, to supplement security policies and technical protection systems. The authors provide in-depth understanding of how organizational learning can produce cultural change addressing the behaviour of individuals, as well as machines. They provide information to help managers form policy to prevent cyber intrusions, to put robust security systems and procedures in place and to arrange appropriate training interventions such as table top exercises. Guidance embracing current and future threats and addressing issues such as social engineering is included. Although the work is embedded in a theoretical framework, non-technical staff will find the book of practical use because it renders highly technical subjects accessible and links firmly with areas beyond ICT, such as human resource

management - in relation to bridging the education/training divide and allowing organizational learning to be embraced. This book will interest Government officials, policy advisors, law enforcement officers and senior managers within companies, as well as academics and students in a range of disciplines including management and computer science.

In the world of digitization today, many services of government and industry are carried out in electronic mode in order to avoid the misuse of natural resources. The implementation of e-services also provides transparency and efficiency. However, these e-services are vulnerable to cyber threats and need special measures in place to provide safety and security as they are being used in the cyber space. This new volume provides an introduction to and overview of cybersecurity in e-services and e-governance systems. The volume presents and discusses the most recent innovations, trends, and concerns, as well as the practical challenges encountered and solutions adopted in the fields of security and e-services. The editors bring together leading academics, scientists, researchers, and research scholars to share their experiences and research results on many aspects of e-services, e-governance, and cybersecurity. The chapters cover diverse topics, such as using digital education to curb gender violence, cybersecurity threats and technology in the banking industry, e-governance in the healthcare sector, cybersecurity in the natural gas and oil industry, developing information communication systems, and more. The chapters also include the uses and selection of encryption technology and software.

This book provides step by step directions for organizations to adopt a security and compliance related architecture according to mandatory legal provisions and standards prescribed for their industry, as well as the methodology to maintain the compliances. It sets a unique mechanism for monitoring controls and a dashboard to maintain the level of compliances. It aims at integration and automation to reduce the fatigue of frequent compliance audits and build a standard baseline of controls to comply with the applicable standards and regulations to which the organization is subject. It is a perfect reference book for professionals in the field of IT governance, risk management, and compliance. The book also illustrates the concepts with charts, checklists, and flow diagrams to enable management to map controls with compliances.

Use the guidance in this comprehensive field guide to gain the support of your top executives for aligning a rational cybersecurity plan with your business. You will learn how to improve working relationships with stakeholders in complex digital businesses, IT, and development environments. You will know how to prioritize your security program, and motivate and retain your team.

Misalignment between security and your business can start at the top at the C-suite or happen at the line of business, IT, development, or user level. It has a corrosive effect on any security project it touches. But it does not have to be like this. Author Dan Blum presents valuable lessons learned from interviews with over 70 security and business leaders. You will discover how to successfully solve issues related to: risk management, operational security, privacy protection, hybrid cloud management, security culture and user awareness, and communication challenges. This book presents six priority areas to focus on to maximize the effectiveness of your cybersecurity program: risk management, control baseline, security culture, IT rationalization, access control, and cyber-resilience.

Common challenges and good practices are provided for businesses of different types and sizes. And more than 50 specific keys to alignment are included. What You Will Learn Improve your security culture: clarify security-related roles, communicate effectively to businesspeople, and hire, motivate, or retain outstanding security staff by creating a sense of efficacy Develop a consistent accountability model, information risk taxonomy, and risk management framework Adopt a security and risk governance model consistent with your business structure or culture, manage policy, and optimize security budgeting within the larger business unit and CIO organization IT spend Tailor a control baseline to your organization's maturity level, regulatory requirements, scale, circumstances, and critical assets Help CIOs, Chief Digital Officers, and other executives to develop an IT strategy for curating cloud solutions and reducing shadow IT, building up DevSecOps and Disciplined Agile, and more Balance access control and accountability approaches, leverage modern digital identity standards to improve digital relationships, and provide data governance and privacy-enhancing capabilities Plan for cyber-resilience: work with the SOC, IT, business groups, and external sources to coordinate incident response and to recover from outages and come back stronger Integrate your learnings from this book into a quick-hitting rational cybersecurity success plan Who This Book Is For Chief Information Security Officers (CISOs) and other heads of security, security directors and managers, security architects and project leads, and other team members providing security leadership to your business

Information Security Governance

Next-Generation Enterprise Security and Governance

A Practical Guide to Building an Integrated GRC Framework for Your Organization

Protecting and Managing Your Company's Proprietary Information

The Psychology of Information Security

Technologies and Applied Solutions