

Measuring And Managing Information Risk A Fair Approach

How to Measure Anything in Cybersecurity Risk
Health and Safety: Risk Management
IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data
Measuring and Managing Information Risk
Measuring and Managing Credit Risk
The Project Risk Maturity Model
Measuring and Managing Liquidity Risk
The Failure of Risk Management
Liquidity Risk Measurement and Management
Managing and Measuring of Risk
Cyber Risk Management
Developing Cybersecurity Programs and Policies
Financial Risk Management
Intangibles
Measuring and Managing Operational Risk
How to Measure Anything
Workbook
Managing Risk and Information Security
Carbon Dioxide Capture and Storage
Fundamentals of Risk Management
Measuring and Managing Operational Risks in Financial Institutions
Security Metrics
The Rise And Fall of British Naval Mastery
Digital Asset Valuation and Cyber Risk Measurement
Information Security Risk Assessment Toolkit
Story-Based Inquiry: A Manual for Investigative Journalists
Credit Risk Management
Information Security Management Metrics
Managing Information Quality
The Future of Risk Management
The Gray Rhino
Modeling, Measuring and Managing Risk
Measuring and Managing Information Risk
How to Manage Cybersecurity Risk
Risk Management: 10 Principles
Liquidity Risk Management
The Cyber Risk Handbook
Asset Liability Management Optimisation
Managing Cyber Risk
Measuring Political Risk
Security Risk Management

How to Measure Anything in Cybersecurity Risk

This book introduces to basic and advanced methods for credit risk management. It covers classical debt instruments and modern financial markets products. The author describes not only standard rating and scoring methods like Classification Trees or Logistic Regression, but also less known models that are subject of ongoing research, like e.g. Support Vector Machines, Neural Networks, or Fuzzy Inference Systems. The book also illustrates financial and commodity markets and analyzes the principles of advanced credit risk modeling techniques and credit derivatives pricing methods. Particular attention is given to the challenges of counterparty risk management, Credit Valuation Adjustment (CVA) and the related regulatory Basel III requirements. As a conclusion, the book provides the reader with all the essential aspects of classical and modern credit risk management and modeling.

Health and Safety: Risk Management

Health and Safety: Risk Management is the clearest and most comprehensive book on risk management available today. This newly revised fifth edition takes into account new developments in legislation, standards and good practice. ISO 45001, the international health and safety management system standard, is given comprehensive treatment, and the latest

ISO 9004 and ISO 19011 have also been addressed. The book is divided into four main parts. Part 1.1 begins with a basic introduction to the techniques of health and safety risk management and continues with a description of ISO 45001. Part 1.2 covers basic human factors including how the sense organs work and the psychology of the individual. Part 2.1 deals with more advanced techniques of risk management including advanced incident investigation, audit and risk assessment, and Part 2.2 covers a range of advanced human factors topics including human error and decision making. This authoritative treatment of health and safety risk management is essential reading for both students working towards degrees, diplomas and postgraduate or vocational qualifications, and experienced health and safety professionals, who will find it invaluable as a reference.

IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data

A global banking risk management guide geared toward the practitioner Financial Risk Management presents an in-depth look at banking risk on a global scale, including comprehensive examination of the U.S. Comprehensive Capital Analysis and Review, and the European Banking Authority stress tests. Written by the leaders of global banking risk products and management at SAS, this book provides the most up-to-date information and expert insight into real risk management. The discussion begins with an overview of methods for computing and managing a variety of risk, then moves into a review of the economic foundation of modern risk management and the growing importance of model risk management. Market risk, portfolio credit risk, counterparty credit risk, liquidity risk, profitability analysis, stress testing, and others are dissected and examined, arming you with the strategies you need to construct a robust risk management system. The book takes readers through a journey from basic market risk analysis to major recent advances in all financial risk disciplines seen in the banking industry. The quantitative methodologies are developed with ample business case discussions and examples illustrating how they are used in practice. Chapters devoted to firmwide risk and stress testing cross reference the different methodologies developed for the specific risk areas and explain how they work together at firmwide level. Since risk regulations have driven a lot of the recent practices, the book also relates to the current global regulations in the financial risk areas. Risk management is one of the fastest growing segments of the banking industry, fueled by banks' fundamental intermediary role in the global economy and the industry's profit-driven increase in risk-seeking behavior. This book is the product of the authors' experience in developing and implementing risk analytics in banks around the globe, giving you a comprehensive, quantitative-oriented risk management guide specifically for the practitioner. Compute and manage market, credit, asset, and liability risk Perform macroeconomic stress testing and act on the results Get up to date on regulatory practices and model risk management Examine the structure and construction of financial risk systems Delve into funds transfer pricing, profitability analysis, and more Quantitative capability is increasing with lightning speed, both methodologically and technologically. Risk professionals must keep pace with the changes, and exploit every tool at their disposal. Financial Risk Management is the practitioner's guide to anticipating, mitigating, and preventing risk in the

modern banking industry.

Measuring and Managing Information Risk

This book is the first comprehensive, scientifically based study of the nature and impact of intangibles. Weaving case studies and real-world examples with contemporary business theory, Baruch Lev - establishes an economic framework to analyze managerial and investment issues concerning intangibles; - surveys the impact of intangibles on corporate performance and market values, including management difficulties, risk, questions of property rights, marketability, and cost structure; - analyzes information deficiencies associated with intangibles, including the major economic principles governing intangible investments, limits of management information systems, and recommendations for improved accounting disclosure; - sets forth a comprehensive information system—aimed at satisfying the needs of both internal and external decision makers—to reflect the impact and value of intangibles within the context of enterprise performance.

Measuring and Managing Credit Risk

Publisher Description

The Project Risk Maturity Model

This volume presents the most recent achievements in risk measurement and management, as well as regulation of the financial industry, with contributions from prominent scholars and practitioners, and provides a comprehensive overview of recent emerging standards in risk management from an interdisciplinary perspective.

Measuring and Managing Liquidity Risk

Managing Risk and Information Security: Protect to Enable, an ApressOpen title, describes the changing risk environment and why a fresh approach to information security is needed. Because almost every aspect of an enterprise is now dependent on technology, the focus of IT security must shift from locking down assets to enabling the business while managing and surviving risk. This compact book discusses business risk from a broader perspective, including privacy and regulatory considerations. It describes the increasing number of threats and vulnerabilities, but also offers strategies for developing solutions. These include discussions of how enterprises can take advantage of new and emerging technologies—such as social media and the huge proliferation of Internet-enabled devices—while minimizing risk. With ApressOpen, content is freely available through multiple online distribution channels and electronic formats with the goal of

disseminating professionally edited and technically reviewed content to the worldwide community. Here are some of the responses from reviewers of this exceptional work: “Managing Risk and Information Security is a perceptive, balanced, and often thought-provoking exploration of evolving information risk and security challenges within a business context. Harkins clearly connects the needed, but often-overlooked linkage and dialog between the business and technical worlds and offers actionable strategies. The book contains eye-opening security insights that are easily understood, even by the curious layman.” Fred Wettling, Bechtel Fellow, IS&T Ethics & Compliance Officer, Bechtel “As disruptive technology innovations and escalating cyber threats continue to create enormous information security challenges, Managing Risk and Information Security: Protect to Enable provides a much-needed perspective. This book compels information security professionals to think differently about concepts of risk management in order to be more effective. The specific and practical guidance offers a fast-track formula for developing information security strategies which are lock-step with business priorities.” Laura Robinson, Principal, Robinson Insight Chair, Security for Business Innovation Council (SBIC) Program Director, Executive Security Action Forum (ESAF) “The mandate of the information security function is being completely rewritten. Unfortunately most heads of security haven’t picked up on the change, impeding their companies’ agility and ability to innovate. This book makes the case for why security needs to change, and shows how to get started. It will be regarded as marking the turning point in information security for years to come.” Dr. Jeremy Bergsman, Practice Manager, CEB “The world we are responsible to protect is changing dramatically and at an accelerating pace. Technology is pervasive in virtually every aspect of our lives. Clouds, virtualization and mobile are redefining computing – and they are just the beginning of what is to come. Your security perimeter is defined by wherever your information and people happen to be. We are attacked by professional adversaries who are better funded than we will ever be. We in the information security profession must change as dramatically as the environment we protect. We need new skills and new strategies to do our jobs effectively. We literally need to change the way we think. Written by one of the best in the business, Managing Risk and Information Security challenges traditional security theory with clear examples of the need for change. It also provides expert advice on how to dramatically increase the success of your security strategy and methods – from dealing with the misperception of risk to how to become a Z-shaped CISO. Managing Risk and Information Security is the ultimate treatise on how to deliver effective security to the world we live in for the next 10 years. It is absolute must reading for anyone in our profession – and should be on the desk of every CISO in the world.” Dave Cullinane, CISSP CEO Security Starfish, LLC “In this overview, Malcolm Harkins delivers an insightful survey of the trends, threats, and tactics shaping information risk and security. From regulatory compliance to psychology to the changing threat context, this work provides a compelling introduction to an important topic and trains helpful attention on the effects of changing technology and management practices.” Dr. Mariano-Florentino Cuéllar Professor, Stanford Law School Co-Director, Stanford Center for International Security and Cooperation (CISAC), Stanford University “Malcolm Harkins gets it. In his new book Malcolm outlines the major forces changing the information security risk landscape from a big picture perspective, and then goes on to offer effective methods of managing that risk from a practitioner's viewpoint. The combination makes this book unique and a must read for anyone interested in IT risk.” Dennis Devlin AVP, Information Security and Compliance, The George Washington

University “Managing Risk and Information Security is the first-to-read, must-read book on information security for C-Suite executives. It is accessible, understandable and actionable. No sky-is-falling scare tactics, no techno-babble – just straight talk about a critically important subject. There is no better primer on the economics, ergonomics and psycho-behaviourals of security than this.” Thornton May, Futurist, Executive Director & Dean, IT Leadership Academy “Managing Risk and Information Security is a wake-up call for information security executives and a ray of light for business leaders. It equips organizations with the knowledge required to transform their security programs from a “culture of no” to one focused on agility, value and competitiveness. Unlike other publications, Malcolm provides clear and immediately applicable solutions to optimally balance the frequently opposing needs of risk reduction and business growth. This book should be required reading for anyone currently serving in, or seeking to achieve, the role of Chief Information Security Officer.” Jamil Farshchi, Senior Business Leader of Strategic Planning and Initiatives, VISA “For too many years, business and security – either real or imagined – were at odds. In Managing Risk and Information Security: Protect to Enable, you get what you expect – real life practical ways to break logjams, have security actually enable business, and marries security architecture and business architecture. Why this book? It's written by a practitioner, and not just any practitioner, one of the leading minds in Security today.” John Stewart, Chief Security Officer, Cisco “This book is an invaluable guide to help security professionals address risk in new ways in this alarmingly fast changing environment. Packed with examples which makes it a pleasure to read, the book captures practical ways a forward thinking CISO can turn information security into a competitive advantage for their business. This book provides a new framework for managing risk in an entertaining and thought provoking way. This will change the way security professionals work with their business leaders, and help get products to market faster. The 6 irrefutable laws of information security should be on a stone plaque on the desk of every security professional.” Steven Proctor, VP, Audit & Risk Management, Flextronics

The Failure of Risk Management

What makes information useful? This seemingly simple and yet intriguing and complicated question is discussed in this book. It examines ways in which the quality of information can be improved in knowledge-intensive processes (such as on-line communication, strategy, product development, or consulting). Based on existing information quality literature, the book proposes a conceptual framework to manage information quality for knowledge-based content. It presents four proven principles to apply the framework to a variety of information products. Five in-depth company case studies show how information quality can be managed systematically. The book uses frequent diagrams and tables, as well as diagnostic questions and summary boxes to make its content actionable.

Liquidity Risk Measurement and Management

This book "takes a close look at misused and misapplied basic analysis methods and shows how some of the most popular "risk management" methods are no better than astrology! Using examples from the 2008 credit crisis, natural disasters, outsourcing to China, engineering disasters, and more, Hubbard reveals critical flaws in risk management methods—and shows how all of these problems can be fixed. The solutions involve combinations of scientifically proven and frequently used methods from nuclear power, exploratory oil, and other areas of business and government. Finally, Hubbard explains how new forms of collaboration across all industries and government can improve risk management in every field." - product description.

Managing and Measuring of Risk

In the same way as the 4Ps of marketing are a fundamental principle of business theory, this book puts forward the 10Ps of Risk Management as a consistent and comprehensive approach to the subject. The 10Ps of Risk Management offers a holistic approach, bringing together all elements of risk management for managers, safety and environmental consultants, business advisers and students on occupational health and safety and environmental studies courses.

Cyber Risk Management

Offering a fresh, transparent approach encompassing new material, this invigorating volume measures political risk - for instance the risk that foreign investment might face in any country. It also demonstrates how progress or regress made in good governance initiatives as conditionalities to aid can be assessed. Governments can monitor their own policy environment(s), and take remedial action if necessary. The methodology allows for measurement of previously unquantified 'soft' factors that add to the risks foreign investors might face, demonstrating why these factors are of importance to both risk assertive and risk averse investors. Features include: - 103 contextualized, measurable risk factors and their 411 risk factor indicators. - Guidelines to using these factors in order to perform generic macro analyses, or micro, client/project/industry-specific analyses. - Explanation of the methodology with which to comprehensively measure the probability of risk occurring in any macro or micro investment climate.

Developing Cybersecurity Programs and Policies

Cyber risk is the second highest perceived business risk according to U.S. risk managers and corporate insurance experts. Digital assets now represent over 85% of an organization's value. In a survey of Fortune 1000 organizations, 83% surveyed described cyber risk as an organizationally complex topic, with most using only qualitative metrics that provide little, if any insight into an effective cyber strategy. Written by one of the foremost cyber risk experts in the world and with

contributions from other senior professionals in the field, *Managing Cyber Risk* provides corporate cyber stakeholders – managers, executives, and directors – with context and tools to accomplish several strategic objectives. These include enabling managers to understand and have proper governance oversight of this crucial area and ensuring improved cyber resilience. *Managing Cyber Risk* helps businesses to understand cyber risk quantification in business terms that lead risk owners to determine how much cyber insurance they should buy based on the size and the scope of policy, the cyber budget required, and how to prioritize risk remediation based on reputational, operational, legal, and financial impacts. Directors are held to standards of fiduciary duty, loyalty, and care. These insights provide the ability to demonstrate that directors have appropriately discharged their duties, which often dictates the ability to successfully rebut claims made against such individuals. Cyber is a strategic business issue that requires quantitative metrics to ensure cyber resiliency. This handbook acts as a roadmap for executives to understand how to increase cyber resiliency and is unique since it quantifies exposures at the digital asset level.

Financial Risk Management

IPCC Report on sources, capture, transport, and storage of CO₂, for researchers, policy-makers and engineers.

Intangibles

"A "gray rhino" is a highly probable, imminent threat; we can see the dust cloud on the horizon long before the charging animal comes into view. Gray rhinos are not random, but occur after a series of warnings and visible events. The Lehman Brothers crash of 2008, the devastating aftermath of Hurricane Sandy and other natural disasters, the file-sharing that presaged the collapse of the traditional music business model, the rising chaos in the Middle East were evident well in advance of the consequences. Gray rhinos are much easier to spot and guard against than "black swans"-- the rare, truly unforeseen catastrophes. Why then, when faced with solvable problems, do we continually fail to address them before they spiral out of control? Drawing on her extensive background in policy formation and crisis management, as well as in-depth interviews with leaders from around the world, Michele Wucker explains in *The Gray Rhino* how significant crises can be recognized and countered strategically. Filled with persuasive stories, real-world examples, and practical advice, *The Gray Rhino* is essential reading for managers, investors, planners, policy makers, and anyone who wants to understand how change really occurs"--

Measuring and Managing Operational Risk

The invaluable companion to the new edition of the bestselling *How to Measure Anything* This companion workbook to the

new edition of the insightful and eloquent *How to Measure Anything* walks readers through sample problems and exercises in which they can master and apply the methods discussed in the book. The book explains practical methods for measuring a variety of intangibles, including approaches to measuring customer satisfaction, organizational flexibility, technology risk, technology ROI, and other problems in business, government, and not-for-profits. Companion to the revision of the bestselling *How to Measure Anything* Provides chapter-by-chapter exercises Written by industry leader Douglas Hubbard Written by recognized expert Douglas Hubbard—creator of Applied Information Economics—*How to Measure Anything* Workbook illustrates how the author has used his approach across various industries and how any problem, no matter how difficult, ill defined, or uncertain can lend itself to measurement using proven methods.

How to Measure Anything Workbook

An advanced method for financial institutions to optimize Asset Liability Management for maximized return and minimized risk Financial institutions today are facing daunting regulatory and economic challenges. As they manage bank regulation and competition, institutions are also optimizing their Asset Liability Management (ALM) operations. The function of the ALM unit today goes beyond risk management related to the banking book into managing regulatory capital and positioning the balance sheet to maximize profit. *Asset Liability Management Optimization: A Practitioner's Guide to Balance Sheet Management and Remodelling* offers a step-by-step process for modeling and reshaping a bank's balance sheet. Based on the author's extensive research, it describes how to apply a quantifiable optimization method to help maximize asset return and minimize funding cost in the banking book. ALM ranks as a key component of any financial institution's overall operating strategy. Now, financial professionals can use an advanced solution for optimizing ALM. This book takes a closer look at the evolving role of the ALM function and the target position of the banking book. It provides strategies for active management, structuring, and hedging of a bank balance sheet, while also exploring additional topics related to ALM. A description of the Funds Transfer Pricing (FTP) process related to a bank's target position Detailed examinations of interest rate risk in the banking book (IRRBB) Discussion of Basel III regulatory requirements and maturity gap analysis Overview of customer behavior, along with its impact on interest rate and liquidity risk Practical spreadsheet models (NII sensitivity and EVE volatility IRRBB model, simplified optimization model for minimization of average funding cost for a bank and an example of behavioral model for Non-Maturing Deposits) Explorations of model risk, sensitivity analysis, and case studies The optimization techniques found in *Asset Liability Management Optimization* can prove vital to financial professionals who are tasked with maximizing asset return and reducing funding costs as a critical part of business objectives.

Managing Risk and Information Security

A fully up-to-date, cutting-edge guide to the measurement and management of liquidity risk Written for front and middle

office risk management and quantitative practitioners, this book provides the ground-level knowledge, tools, and techniques for effective liquidity risk management. Highly practical, though thoroughly grounded in theory, the book begins with the basics of liquidity risks and, using examples pulled from the recent financial crisis, how they manifest themselves in financial institutions. The book then goes on to look at tools which can be used to measure liquidity risk, discussing risk monitoring and the different models used, notably financial variables models, credit variables models, and behavioural variables models, and then at managing these risks. As well as looking at the tools necessary for effective measurement and management, the book also looks at and discusses current regulation and the implication of new Basel regulations on management procedures and tools.

Carbon Dioxide Capture and Storage

Digital Asset Valuation and Cyber Risk Measurement: Principles of Cybernomics is a book about the future of risk and the future of value. It examines the indispensable role of economic modeling in the future of digitization, thus providing industry professionals with the tools they need to optimize the management of financial risks associated with this megatrend. The book addresses three problem areas: the valuation of digital assets, measurement of risk exposures of digital valuables, and economic modeling for the management of such risks. Employing a pair of novel cyber risk measurement units, bitmort and hekla, the book covers areas of value, risk, control, and return, each of which are viewed from the perspective of entity (e.g., individual, organization, business), portfolio (e.g., industry sector, nation-state), and global ramifications. Establishing adequate, holistic, and statistically robust data points on the entity, portfolio, and global levels for the development of a cybernomics databank is essential for the resilience of our shared digital future. This book also argues existing economic value theories no longer apply to the digital era due to the unique characteristics of digital assets. It introduces six laws of digital theory of value, with the aim to adapt economic value theories to the digital and machine era. Comprehensive literature review on existing digital asset valuation models, cyber risk management methods, security control frameworks, and economics of information security Discusses the implication of classical economic theories under the context of digitization, as well as the impact of rapid digitization on the future of value Analyzes the fundamental attributes and measurable characteristics of digital assets as economic goods Discusses the scope and measurement of digital economy Highlights cutting-edge risk measurement practices regarding cybersecurity risk management Introduces novel concepts, models, and theories, including opportunity value, Digital Valuation Model, six laws of digital theory of value, Cyber Risk Quadrant, and most importantly, cyber risk measures hekla and bitmort Introduces cybernomics, that is, the integration of cyber risk management and economics to study the requirements of a databank in order to improve risk analytics solutions for (1) the valuation of digital assets, (2) the measurement of risk exposure of digital assets, and (3) the capital optimization for managing residual cyber risk Provides a case study on cyber insurance

Fundamentals of Risk Management

Villains for the Great Meltdown of 2007-2008 seem plentiful. But the very concept of finding and punishing villains misses the target. Ideally, we learn from past failures. We perfect our craft. Lessons to be learned from the Great Meltdown are not just plentiful - they are also insightful. In LIQUIDITY RISK MEASUREMENT AND MANAGENT -- BASEL III AND BEYOND, Mr. Matz provides detailed, practical analysis and recommendations covering every aspect of liquidity risk measurement and management. * Examples of what went wrong are used extensively. * Best practices procedures are explained. * New regulatory guidance - both qualitative and quantitative, including Basel III - is discussed in detail.* Source material and examples from many countries are included.This is the "how to guide" for liquidity risk managers in financial institutions around the globe.

Measuring and Managing Operational Risks in Financial Institutions

Spectacular security failures continue to dominate the headlines despite huge increases in security budgets and ever-more draconian regulations. The 20/20 hindsight of audits is no longer an effective solution to security weaknesses, and the necessity for real-time strategic metrics has never been more critical. Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement offers a radical new approach for developing and implementing security metrics essential for supporting business activities and managing information risk. This work provides anyone with security and risk management responsibilities insight into these critical security questions: How secure is my organization? How much security is enough? What are the most cost-effective security solutions? How secure is my organization? You can't manage what you can't measure This volume shows readers how to develop metrics that can be used across an organization to assure its information systems are functioning, secure, and supportive of the organization's business objectives. It provides a comprehensive overview of security metrics, discusses the current state of metrics in use today, and looks at promising new developments. Later chapters explore ways to develop effective strategic and management metrics for information security governance, risk management, program implementation and management, and incident management and response. The book ensures that every facet of security required by an organization is linked to business objectives, and provides metrics to measure it. Case studies effectively demonstrate specific ways that metrics can be implemented across an enterprise to maximize business benefit. With three decades of enterprise information security experience, author Krag Brotby presents a workable approach to developing and managing cost-effective enterprise information security.

Security Metrics

The Definitive Guide to Quantifying, Classifying, and Measuring Enterprise IT Security Operations Security Metrics is the first comprehensive best-practice guide to defining, creating, and utilizing security metrics in the enterprise. Using sample charts, graphics, case studies, and war stories, Yankee Group Security Expert Andrew Jaquith demonstrates exactly how to establish effective metrics based on your organization's unique requirements. You'll discover how to quantify hard-to-measure security activities, compile and analyze all relevant data, identify strengths and weaknesses, set cost-effective priorities for improvement, and craft compelling messages for senior management. Security Metrics successfully bridges management's quantitative viewpoint with the nuts-and-bolts approach typically taken by security professionals. It brings together expert solutions drawn from Jaquith's extensive consulting work in the software, aerospace, and financial services industries, including new metrics presented nowhere else. You'll learn how to:

- Replace nonstop crisis response with a systematic approach to security improvement
- Understand the differences between "good" and "bad" metrics
- Measure coverage and control, vulnerability management, password quality, patch latency, benchmark scoring, and business-adjusted risk
- Quantify the effectiveness of security acquisition, implementation, and other program activities
- Organize, aggregate, and analyze your data to bring out key insights
- Use visualization to understand and communicate security issues more clearly
- Capture valuable data from firewalls and antivirus logs, third-party auditor reports, and other resources
- Implement balanced scorecards that present compact, holistic views of organizational security effectiveness

The Rise And Fall of British Naval Mastery

Security Risk Management is the definitive guide for building or running an information security risk management program. This book teaches practical techniques that will be used on a daily basis, while also explaining the fundamentals so students understand the rationale behind these practices. It explains how to perform risk assessments for new IT projects, how to efficiently manage daily risk activities, and how to qualify the current risk level for presentation to executive level management. While other books focus entirely on risk analysis methods, this is the first comprehensive text for managing security risks. This book will help you to break free from the so-called best practices argument by articulating risk exposures in business terms. It includes case studies to provide hands-on experience using risk assessment tools to calculate the costs and benefits of any security investment. It explores each phase of the risk management lifecycle, focusing on policies and assessment processes that should be used to properly assess and mitigate risk. It also presents a roadmap for designing and implementing a security risk management program. This book will be a valuable resource for CISOs, security managers, IT managers, security consultants, IT auditors, security analysts, and students enrolled in information security/assurance college programs. Named a 2011 Best Governance and ISMS Book by InfoSec Reviews Includes case studies to provide hands-on experience using risk assessment tools to calculate the costs and benefits of any security investment Explores each phase of the risk management lifecycle, focusing on policies and assessment processes that should be used to properly assess and mitigate risk Presents a roadmap for designing and implementing a security risk

management program

Digital Asset Valuation and Cyber Risk Measurement

Using the factor analysis of information risk (FAIR) methodology developed over ten years and adopted by corporations worldwide, Measuring and Managing Information Risk provides a proven and credible framework for understanding, measuring, and analyzing information risk of any size or complexity. Intended for organizations that need to either build a risk management program from the ground up or strengthen an existing one, this book provides a unique and fresh perspective on how to do a basic quantitative risk analysis. Covering such key areas as risk theory, risk calculation, scenario modeling, and communicating risk within the organization, Measuring and Managing Information Risk helps managers make better business decisions by understanding their organizational risk. Uses factor analysis of information risk (FAIR) as a methodology for measuring and managing risk in any organization. Carefully balances theory with practical applicability and relevant stories of successful implementation. Includes examples from a wide variety of businesses and situations presented in an accessible writing style.

Information Security Risk Assessment Toolkit

Implement an Effective Security Metrics Project or Program IT Security Metrics provides a comprehensive approach to measuring risks, threats, operational activities, and the effectiveness of data protection in your organization. The book explains how to choose and design effective measurement strategies and addresses the data requirements of those strategies. The Security Process Management Framework is introduced and analytical strategies for security metrics data are discussed. You'll learn how to take a security metrics program and adapt it to a variety of organizational contexts to achieve continuous security improvement over time. Real-world examples of security measurement projects are included in this definitive guide. Define security metrics as a manageable amount of usable data Design effective security metrics Understand quantitative and qualitative data, data sources, and collection and normalization methods Implement a programmable approach to security using the Security Process Management Framework Analyze security metrics data using quantitative and qualitative methods Design a security measurement project for operational analysis of security metrics Measure security operations, compliance, cost and value, and people, organizations, and culture Manage groups of security measurement projects using the Security Improvement Program Apply organizational learning methods to security metrics

Story-Based Inquiry: A Manual for Investigative Journalists

Credit Risk Management

This book is the first in the market to treat single- and multi-period risk measures (risk functionals) in a thorough, comprehensive manner. It combines the treatment of properties of the risk measures with the related aspects of decision making under risk. The book introduces the theory of risk measures in a mathematically sound way. It contains properties, characterizations and representations of risk functionals for single-period and multi-period activities, and also shows the embedding of such functionals in decision models and the properties of these models.

Information Security Management Metrics

In order to protect company's information assets such as sensitive customer records, health care records, etc., the security practitioner first needs to find out: what needs protected, what risks those assets are exposed to, what controls are in place to offset those risks, and where to focus attention for risk treatment. This is the true value and purpose of information security risk assessments. Effective risk assessments are meant to provide a defensible analysis of residual risk associated with your key assets so that risk treatment options can be explored. Information Security Risk Assessments gives you the tools and skills to get a quick, reliable, and thorough risk assessment for key stakeholders. Based on authors' experiences of real-world assessments, reports, and presentations Focuses on implementing a process, rather than theory, that allows you to derive a quick and valuable assessment Includes a companion web site with spreadsheets you can utilize to create and maintain the risk assessment

Managing Information Quality

All the Knowledge You Need to Build Cybersecurity Programs and Policies That Work Clearly presents best practices, governance frameworks, and key standards Includes focused coverage of healthcare, finance, and PCI DSS compliance An essential and invaluable guide for leaders, managers, and technical professionals Today, cyberattacks can place entire organizations at risk. Cybersecurity can no longer be delegated to specialists: success requires everyone to work together, from leaders on down. Developing Cybersecurity Programs and Policies offers start-to-finish guidance for establishing effective cybersecurity in any organization. Drawing on more than 20 years of real-world experience, Omar Santos presents realistic best practices for defining policy and governance, ensuring compliance, and collaborating to harden the entire organization. First, Santos shows how to develop workable cybersecurity policies and an effective framework for governing them. Next, he addresses risk management, asset management, and data loss prevention, showing how to align functions from HR to physical security. You'll discover best practices for securing communications, operations, and access; acquiring, developing, and maintaining technology; and responding to incidents. Santos concludes with detailed coverage of

compliance in finance and healthcare, the crucial Payment Card Industry Data Security Standard (PCI DSS) standard, and the NIST Cybersecurity Framework. Whatever your current responsibilities, this guide will help you plan, manage, and lead cybersecurity—and safeguard all the assets that matter. Learn How To · Establish cybersecurity policies and governance that serve your organization's needs · Integrate cybersecurity program components into a coherent framework for action · Assess, prioritize, and manage security risk throughout the organization · Manage assets and prevent data loss · Work with HR to address human factors in cybersecurity · Harden your facilities and physical environment · Design effective policies for securing communications, operations, and access · Strengthen security throughout the information systems lifecycle · Plan for quick, effective incident response and ensure business continuity · Comply with rigorous regulations in finance and healthcare · Plan for PCI compliance to safely process payments · Explore and apply the guidance provided by the NIST Cybersecurity Framework

The Future of Risk Management

A comprehensive and innovative look at how to protect financial institutions from operational risks Operational risk is the risk associated with human error, systems failures, and inadequate controls and procedures in information systems or internal controls that will result in an unexpected loss. According to a recent survey, about seventy percent of banks consider operational risk as important as market or credit risks. Nearly a quarter of the same banks admit to operation-related losses of more than \$1.6 million-many cases are so embarrassing that banks will not actually admit any error on their part. Firms are just beginning to develop their own operational risk management systems and they need guidance on how to do it. This book will help them identify, measure, and manage their operational risks. Christopher Marshall (Singapore) is Associate Director of the Center for Financial Engineering at the National University of Singapore. He has written numerous articles in Risk magazine and Harvard Business School cases.

The Gray Rhino

The most up-to-date, comprehensive guide on liquidity risk management—from the professionals Written by a team of industry leaders from the Price Waterhouse Coopers Financial Services Regulatory Practice, Liquidity Risk Management is the first book of its kind to pull back the curtain on a global approach to liquidity risk management in the post-financial crisis. Now, as a number of regulatory initiatives emerge, this timely and informative book explores the real-world implications of risk management practices in today's market. Taking a clear and focused approach to the operational and financial obligations of liquidity risk management, the book builds upon a foundational knowledge of banking and capital markets and explores in-depth the key aspects of the subject, including governance, regulatory developments, analytical frameworks, reporting, strategic implications, and more. The book also addresses management practices that are

particularly insightful to liquidity risk management practitioners and managers in numerous areas of banking organizations. Each chapter is authored by a Price Waterhouse Coopers partner or director who has significant, hands-on expertise. Content addresses key areas of the subject, such as liquidity stress testing and information reporting. Several chapters are devoted to Basel III and its implications for bank liquidity risk management and business strategy. Includes a dedicated, current, and all-inclusive look at liquidity risk management. Complemented with hands-on insight from the field's leading authorities on the subject, *Liquidity Risk Management* is essential reading for practitioners and managers within banking organizations looking for the most current information on liquidity risk management.

Modeling, Measuring and Managing Risk

This book covers Operational Risk Management (ORM), in the current context, and its new role in the risk management field. The concept of operational risk is subject to a wide discussion also in the field of ORM's literature, which has increased throughout the years. By analyzing different methodologies that try to integrate qualitative and quantitative data or different measurement approaches, the authors explore the methodological framework, the assumptions, statistical tool, and the main results of an operational risk model projected by intermediaries. A guide for academics and students, the book also discusses the avenue of mitigation acts, suggested by the main results of the methodologies applied. The book will appeal to students, academics, and financial supervisory and regulatory authorities.

Measuring and Managing Information Risk

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.

How to Manage Cybersecurity Risk

Fundamentals of Risk Management, now in its fourth edition, is a comprehensive introduction to commercial and business risk for students and a broad range of risk professionals. Providing extensive coverage of the core frameworks of business continuity planning, enterprise risk management and project risk management, this is the definitive guide to dealing with the different types of risk an organization faces. With relevant international case examples from both the private and public sectors, this revised edition of Fundamentals of Risk Management is completely aligned to ISO 31000 and provides a full analysis of changes in contemporary risk areas including supply chain, cyber risk, risk culture and improvements in risk management documentation and statutory risk reporting. This new edition of Fundamentals of Risk Management has been fully updated to reflect the development of risk management standards and practice, in particular business continuity standards, regulatory developments, risks to reputation and the business model, changes in enterprise risk management (ERM), loss control and the value of insurance as a risk management method. Also including a thorough overview of the international risk management standards and frameworks, strategy and policy, this book is the definitive professional text for risk managers.

Risk Management: 10 Principles

Top businesses recognise risk management as a core feature of their project management process and approach to the governance of projects. However, a mature risk management process is required in order to realise its benefits; one that takes into account the design and implementation of the process and the skills, experience and culture of the people who use it. To be mature in the way you manage risk you need an accepted framework to assess your risk management maturity, allowing you to benchmark against a recognised standard. A structured pathway for improvement is also needed, not just telling you where you are now, but describing the steps required to reach the next level. The Project Risk Maturity Model detailed here provides such an assessment framework and development pathway. It can be used to benchmark your project risk processes and support the introduction of effective in-house project risk management. Using this model,

implementation and improvement of project risk management can be managed effectively to ensure that the expected benefits are achieved in a way that is appropriate to the needs of each organisation. Martin Hopkinson has developed The Project Risk Maturity Model into a robust framework, and this book allows you to access and apply his insights and experience. A key feature is a CD containing a working copy of the QinetiQ Project Risk Maturity Model (RMM). This will enable you to undertake maturity assessments for as many projects as you choose. The RMM has been proven over a period of 10 years, with at least 250 maturity assessments on projects and programmes with a total value exceeding £60 billion. A case study in the book demonstrates how it has been used to deliver significant and measurable benefits to the performance of major projects.

Liquidity Risk Management

Paul Kennedy's classic naval history, now updated with a new introduction by the author This acclaimed book traces Britain's rise and fall as a sea power from the Tudors to the present day. Challenging the traditional view that the British are natural 'sons of the waves', he suggests instead that the country's fortunes as a significant maritime force have always been bound up with its economic growth. In doing so, he contributes significantly to the centuries-long debate between 'continental' and 'maritime' schools of strategy over Britain's policy in times of war. Setting British naval history within a framework of national, international, economic, political and strategic considerations, he offers a fresh approach to one of the central questions in British history. A new introduction extends his analysis into the twenty-first century and reflects on current American and Chinese ambitions for naval mastery. 'Excellent and stimulating' Correlli Barnett 'The first scholar to have set the sweep of British Naval history against the background of economic history' Michael Howard, Sunday Times 'By far the best study that has ever been done on the subject a sparkling and apt quotation on practically every page' Daniel A. Baugh, International History Review 'The best single-volume study of Britain and her naval past now available to us' Jon Sumida, Journal of Modern History

The Cyber Risk Handbook

Using the factor analysis of information risk (FAIR) methodology developed over ten years and adopted by corporations worldwide, Measuring and Managing Information Risk provides a proven and credible framework for understanding, measuring, and analyzing information risk of any size or complexity. Intended for organizations that need to either build a risk management program from the ground up or strengthen an existing one, this book provides a unique and fresh perspective on how to do a basic quantitative risk analysis. Covering such key areas as risk theory, risk calculation, scenario modeling, and communicating risk within the organization, Measuring and Managing Information Risk helps managers make better business decisions by understanding their organizational risk. Uses factor analysis of information risk (FAIR) as a

methodology for measuring and managing risk in any organization. Carefully balances theory with practical applicability and relevant stories of successful implementation. Includes examples from a wide variety of businesses and situations presented in an accessible writing style.

Asset Liability Management Optimisation

Learn how to prioritize threats, implement a cyber security programme and effectively communicate risks

Managing Cyber Risk

A ground shaking exposé on the failure of popular cyber risk management methods How to Measure Anything in Cybersecurity Risk exposes the shortcomings of current "risk management" practices, and offers a series of improvement techniques that help you fill the holes and ramp up security. In his bestselling book How to Measure Anything, author Douglas W. Hubbard opened the business world's eyes to the critical need for better measurement. This book expands upon that premise and draws from The Failure of Risk Management to sound the alarm in the cybersecurity realm. Some of the field's premier risk management approaches actually create more risk than they mitigate, and questionable methods have been duplicated across industries and embedded in the products accepted as gospel. This book sheds light on these blatant risks, and provides alternate techniques that can help improve your current situation. You'll also learn which approaches are too risky to save, and are actually more damaging than a total lack of any security. Dangerous risk management methods abound; there is no industry more critically in need of solutions than cybersecurity. This book provides solutions where they exist, and advises when to change tracks entirely. Discover the shortcomings of cybersecurity's "best practices" Learn which risk management approaches actually create risk Improve your current practices with practical alterations Learn which methods are beyond saving, and worse than doing nothing Insightful and enlightening, this book will inspire a closer examination of your company's own risk management practices in the context of cybersecurity. The end goal is airtight data protection, so finding cracks in the vault is a positive thing—as long as you get there before the bad guys do. How to Measure Anything in Cybersecurity Risk is your guide to more robust protection through better quantitative processes, approaches, and techniques.

Measuring Political Risk

Protecting information systems to reduce the risk of security incidents is critical for organizations today. This writing provides instruction for security leaders on the processes and techniques for managing a security program. It contains practical information on the breadth of information security topics, referring to many other writings that provide details on

technical security topics. This provides foundation for a security program responsive to technology developments and an evolving threat environment. The security leader may be engaged by an organization that is in crisis, where the priority action is to recover from a serious incident. This work offers foundation knowledge for the security leader to immediately apply to the organization's security program while improving it to the next level, organized by development stage:

- Reactive – focused on incident detection and response
- Planned – control requirements, compliance and reporting
- Managed – integrated security business processes

The security leader must also communicate with the organization executive, whose focus is on results such as increasing revenues or reducing costs. The security leader may initially be welcomed as the wizard who applies mysterious skills to resolve an embarrassing incident. But the organization executive will lose patience with a perpetual crisis and demand concrete results. This writing explains how to communicate in terms executives understand.

Security Risk Management

Whether man-made or naturally occurring, large-scale disasters can cause fatalities and injuries, devastate property and communities, savage the environment, impose significant financial burdens on individuals and firms, and test political leadership. Moreover, global challenges such as climate change and terrorism reveal the interdependent and interconnected nature of our current moment: what occurs in one nation or geographical region is likely to have effects across the globe. Our information age creates new and more integrated forms of communication that incur risks that are difficult to evaluate, let alone anticipate. All of this makes clear that innovative approaches to assessing and managing risk are urgently required. When catastrophic risk management was in its inception thirty years ago, scientists and engineers would provide estimates of the probability of specific types of accidents and their potential consequences. Economists would then propose risk management policies based on those experts' estimates with little thought as to how this data would be used by interested parties. Today, however, the disciplines of finance, geography, history, insurance, marketing, political science, sociology, and the decision sciences combine scientific knowledge on risk assessment with a better appreciation for the importance of improving individual and collective decision-making processes. The essays in this volume highlight past research, recent discoveries, and open questions written by leading thinkers in risk management and behavioral sciences. The Future of Risk Management provides scholars, businesses, civil servants, and the concerned public tools for making more informed decisions and developing long-term strategies for reducing future losses from potentially catastrophic events. Contributors: Mona Ahmadiani, Joshua D. Baker, W. J. Wouter Botzen, Cary Coglianese, Gregory Colson, Jeffrey Czajkowski, Nate Dieckmann, Robin Dillon, Baruch Fischhoff, Jeffrey A. Friedman, Robin Gregory, Robert W. Klein, Carolyn Kousky, Howard Kunreuther, Craig E. Landry, Barbara Mellers, Robert J. Meyer, Erwann Michel-Kerjan, Robert Muir-Wood, Mark Pauly, Lisa Robinson, Adam Rose, Paul J. H. Schoemaker, Paul Slovic, Phil Tetlock, Daniel Västfjäll, W. Kip Viscusi, Elke U. Weber, Richard Zeckhauser.

[ROMANCE](#) [ACTION & ADVENTURE](#) [MYSTERY & THRILLER](#) [BIOGRAPHIES & HISTORY](#) [CHILDREN'S](#) [YOUNG ADULT](#) [FANTASY](#)
[HISTORICAL FICTION](#) [HORROR](#) [LITERARY FICTION](#) [NON-FICTION](#) [SCIENCE FICTION](#)