Measuring And Managing Information Risk A Fair Approach

Now updated with new research and even more intuitive explanations, a demystifying explanation of how managers can inform themselves to make less risky, more profitable business decisions This insightful and eloquent book will show you how to measure those things in your own business that, until now, you may have considered "immeasurable," including customer satisfaction, organizational flexibility, technology risk, and technology ROI. Adds even more intuitive explanations of powerful measurement methods and shows how they can be applied to areas such as risk management and customer satisfaction Continues to boldly assert that any perception of "immeasurability" is based on certain popular misconceptions about measurement and measurement methods Shows the common reasoning for calling something immeasurable, and sets out to correct those ideas Offers practical methods for measuring a variety of "intangibles" Adds recent research, especially in regards to methods that seem like measurement, but are in fact a kind of "placebo effect" for management - and explains how to tell effective methods from management mythology Written by recognized expert Douglas Hubbard-creator of Applied Information Economics-How to Measure Anything, Second Edition 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.

Written for people who manage information security risks for their organizations, this book details a security risk evaluation approach called "OCTAVE." The book provides a framework for systematically evaluating and managing security risks, illustrates the implementation of self-directed evaluations, and shows how to tailor evaluation methods to the needs of specific organizations. A running example illustrates key concepts and techniques. Evaluation worksheets and a catalog of best practices are included. The authors are on the technical staff of the Software Engineering Institute. Annotation copyrighted by Book News, Inc., Portland, OR

In the ever-changing world of business, we've arrived at a point where process has trumped culture, where the race toward efficiency has left us unable to reach our potential. Stuck in the land of status quo, we've forgotten how to think. The very structures put in place to help businesses grow are now holding us back;; it's time to Kill the Company. This book is a call to arms: to start a revolution in how we think and work. But instead of more one-size-fits-all change initiatives forced upon employees, we need to embrace small changes that create ripple effects throughout the organization. Lisa Bodell urges companies to move from "Zombies, Inc." to "Think, Inc." Thinking can no longer be exclusive to the creative team or lead strategists. A culture of curiosity must be fostered among the ranks to shake up our standard practices, from unproductive meetings to go-nowhere strategic planning. This revolution can and will awaken our ability to think, and ultimately, to innovate and grow.

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.

A Complete Guide for Performing Security Risk Assessments, Second Edition

Measuring the Effectiveness and Efficiency of a Security Program

New Contexts, Themes and Challenges

Kill the Company

Liquidity Risk Management

Infonomics

Tools, Techniques, and other Resources

PMBOK&® Guide is the go-to resource for project management practitioners. The project management profession has significantly evolved due to emerging technology, new approaches and rapid market changes. Reflecting this evolution, The Standard for Project Management enumer of project management and the PMBOK&® Guide &– Seventh Edition is structured around eight project performance domains.This edition is designed to address practitioners' current and future needs and to help them be more proactive, innovative and nimble in enabling desired projec edition of the PMBOK&® Guide:•Reflects the full range of development approaches (predictive, adaptive, hybrid, etc.);•Provides an entire section devoted to tailoring the development approach and processes;•Includes an expanded list of models, methods, and artifacts;•Focuses on not project outputs but also enabling outcomes; and• Integrates with PMIstandards+™ for information and standards application content based on project type, development approach, and industry sector.

Best practices for protecting critical data and systems Information Assurance Handbook: Effective Computer Security and Risk Management Strategies discusses the tools and techniques required to prevent, detect, contain, correct, and recover from security breaches and other informa failures. This practical resource explains how to integrate information assurance into your enterprise planning in a non-technical manner. It leads you through building an IT strategy and offers an organizational approach to identifying, implementing, and controlling information assurance small businesses and global enterprises alike. Common threats and vulnerabilities are described and applicable controls based on risk profiles are provided. Practical information assurance application examples are presented for select industries, including healthcare, retail, and industri systems. Chapter-ending critical thinking exercises reinforce the material covered. An extensive list of scholarly works and international government standards is also provided in this detailed guide. Comprehensive coverage includes: Basic information assurance principles and concepts assurance management system Current practices, regulations, and plans Impact of organizational structure Asset management Risk management and mitigation Human resource assurance Advantages of certification, accreditation, and assurance Information assurance in system deve acquisition Physical and environmental security controls Information assurance awareness, training, and education Access control Information security monitoring tools and methods Information assurance measurements and metrics Incident handling and computer forensics Business c management Backup and restoration Cloud computing and outsourcing strategies Information assurance big data concerns

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. Hig 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, di 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 regulation and the implication of new Basel regulations on management procedures and tools.

All investments carry with them some degree of risk. In the financial world, individuals, professional money managers, financial institutions and many others encounter and must deal with risk. The main purpose of 'Investment Risk Management' is to provide an overview of developments management and a synthesis of research involving the latest developments in the field.

Information Assurance Handbook: Effective Computer Security and Risk Management Strategies

Risk Management in Agriculture

Measuring and Managing Operational Risk

The Security Risk Assessment Handbook

How to Measure Anything

The Failure of Risk Management

The OCTAVE Approach

Includes a CD-ROM that contains Excel workbooks and a Matlab manual and software. Covers the subject without advanced or exotic material.

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.

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

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.

Practical Solutions for Creating a Sustainable Cyber Program

How to Measure Anything in Cybersecurity Risk

Managing Information Security Risks

How to Monetize, Manage, and Measure Information as an Asset for Competitive Advantage

Protect to Enable

An Integrated Approach

Information Security Risk Assessment Toolkit

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

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.

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.

When it comes to managing cybersecurity in an organization, most organizations tussle with basic foundational components. This practitioner's guide lays down those foundational components, with real client examples and pitfalls to avoid. A plethora of cybersecurity management resources are available—many with sound advice, management approaches, and technical solutions—but few with one common theme that pulls together management and technology, with a focus on executive oversight. Author Ryan Leirvik helps solve these common problems by providing a clear, easy-to-understand, and easy-to-deploy foundational cyber risk management approach applicable to your entire organization. The book provides tools and methods in a straight-forward practical manner to guide the management of your cybersecurity program and helps practitioners pull cyber from a "technical" problem to a "business risk management" problem, equipping you with a simple approach to understand, manage, and measure cyber risk for your enterprise. What You Will Learn Educate the executives/board on what you are doing to reduce risk Communicate the value of cybersecurity programs and investments through insightful risk-informative metrics Know your key performance indicators (KPIs), key risk indicators (KRIs), and/or objectives and key results Prioritize appropriate resources through identifying program-related gaps Lay down the foundational components of a program based on real examples, including pitfalls to avoid Who This Book Is For CISOs, CROs, CIOs, directors of risk management, and anyone struggling to pull together frameworks or basic metrics to quantify uncertainty and address risk

Analytical Methods for Risk Management

The New Practice of Federal Cyber Security

The Cyber Risk Handbook

Practical Assessments Through Data Collection and Data Analysis

Quantitative Risk Management: Concepts, Techniques, and Tools

The Project Risk Maturity Model

Measuring Financial Inclusion and the Fintech Revolution

Many senior executives talk about information as one of their most important assets, but few behave as if it is. They report to the board on the health of their workforce, their financials, their customers, and their partnerships, but rarely the health of their information assets. Corporations typically exhibit greater discipline in tracking and accounting for their office furniture than their data. Infonomics is the theory, study, and discipline of asserting economic significance to information. It strives to apply both economic and asset management principles and practices to the valuation, handling, and deployment of information assets. This book specifically shows: CEOs and business leaders how to more fully wield information as a corporate asset CIOs how to improve the flow and accessibility of information CFOs how to help their organizations measure the actual and latent value in their information assets. More directly, this book is for the burgeoning force of chief data officers (CDOs) and other information and analytics leaders in their valiant struggle to help their organizations become more infosavvy. Author Douglas Laney has spent years researching and developing Infonomics and advising organizations on the infinite opportunities to monetize, manage, and measure information. This book delivers a set of new ideas, frameworks, evidence, and even approaches adapted from other disciplines on how to administer, wield, and understand the value of information. Infonomics can help organizations not only to better develop, sell, and market their offerings, but to transform their organizations altogether. "Doug Laney masterfully weaves together a collection of great examples with a solid framework to guide readers on how to gain competitive advantage through what he labels "the unruly asset" – data. The framework is comprehensive, the advice practical and the success stories global and across industries and applications." Liz Rowe, Chief Data Officer, State of New Jersey "A must read for anybody who wants to survive in a data centric world." Shaun Adams, Head of Data Science, Betterbathrooms.com "Phenomenal! An absolute must read for data practitioners, business leaders and technology strategists. Doug's lucid style has a set a new standard in providing intelligible material in the field of information economics. His passion and knowledge on the subject exudes thru his literature and inspires individuals like me." Ruchi Rajasekhar, Principal Data Architect, MISO Energy "I highly recommend Infonomics to all aspiring analytics leaders. Doug Laney's work gives readers a deeper understanding of how and why information should be monetized and managed as an enterprise asset. Laney's assertion that accounting should recognize information as a capital asset is quite convincing and one I agree with. Infonomics enjoyably echoes that sentiment!" Matt Green, independent business analytics consultant, Atlanta area "If you care about the digital economy, and you should, read this book." Tanya Shuckhart, Analyst Relations Lead, IRI Worldwide

The implementation of sound quantitative risk models is a vital concern for all financial institutions, and this trend has accelerated in recent years with regulatory processes such as Basel II. This book provides a comprehensive treatment of the theoretical concepts and modelling techniques of quantitative risk management and equips readers--whether financial risk analysts, actuaries, regulators, or students of quantitative finance--with practical tools to solve real-world problems. The authors cover methods for market, credit, and operational risk modelling; place standard industry approaches on a more formal footing; and describe recent developments that go beyond, and address main deficiencies of, current practice. The book's methodology draws on diverse quantitative disciplines, from mathematical finance through statistics and econometrics to actuarial mathematics. Main concepts discussed include loss distributions, risk measures, and risk aggregation and allocation principles. A main theme is the need to satisfactorily address extreme outcomes and the dependence of key risk drivers. The techniques required derive from multivariate statistical analysis, financial time series modelling, copulas, and extreme value theory. A more technical chapter addresses credit derivatives. Based on courses taught to masters students and professionals, this book is a unique and fundamental reference that is set to become a standard in the field.

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.

Fully revised and restructured, Measuring Market Risk, Second Edition includes a new chapter on options risk management, as well as substantial new information on parametric risk, non-parametric measurements and liquidity risks, more practical information to help with specific calculations, and new examples including Q&A's and case studies.

Fundamentals of Risk Management

Business Performance Measurement and Management

Managing Cyber Risk

Managing Risk and Information Security

Understand, Manage, and Measure Cyber Risk

Measuring and Improving Risk Management Capability

Investment Risk Management

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.

Publisher Description

Measuring and managing the performance of a business is one of the most genuine desires of management. Balanced scorecard, the performance prism and activity-based management are the most popular frameworks in this setting. Based on the findings of R.G. Eccles' acclaimed "Performance Measurement Manifesto (1991)" this book introduces new contexts and themes of application and presents emerging research areas related to business performance measurement and management, e.g. SMEs and sustainability. As a result of the 1st International Summer School Piero Lunghi on "Perspectives of Business Performance Management" this book is written both for students and academics, as well as for practitioners looking for new, yet proven ways to measure and manage business performance.

Effective risk management is essential for the success of large projects built and operated by the Department of Energy (DOE), particularly for the one-of-a-kind projects that characterize much of its mission. To enhance DOEâ€™s risk management efforts, the department asked the NRC to prepare a summary of the most effective practices used by leading owner organizations. The studyâ€™s primary objective was to provide DOE project managers with a basic understanding of both the project ownerâ€™s risk management role and effective oversight of those risk management activities delegated to contractors.

Modeling, Measuring and Managing Risk

Understanding, Evaluating and Implementing Effective Risk Management

Why It's Broken and How to Fix It

Principles of Cybernomics

Creating and Measuring Effective Cybersecurity Capabilities

A Systems Engineering Perspective

Security Metrics 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.

Wiskundige analysemethoden voor het bepalen van financiele risico's in het landbouwbedrijfsbeheer

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.

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.

Emerging Global Standards and Regulations After the Financial Crisis

Security Risk Management

The Global Findex Database 2017

Performance Measurement and Management for Engineers

A FAIR Approach

An Introduction to Market Risk Measurement

Measuring and Managing Liquidity Risk

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 defendable 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

Security Metrics Management, Measuring the Effectiveness and Efficiency of a Security Program, Second Edition details the application of quantitative, statistical, and/or mathematical analyses to measure security functional trends and workload, tracking what each function is doing in terms of level of effort (LOE), costs, and productivity. This fully updated guide is the go-to reference for managing an asset protection program and related security functions through the use of metrics. It supports the security professional's position on budget matters, helping to justify the cost-effectiveness of security-related decisions to senior management and other key decision-makers. The book is designed to provide easy-to-follow guidance, allowing security professionals to confidently measure the costs of their assets protection program - their security program - as well as its successes and failures. It includes a discussion of how to use the metrics to brief management, build budgets, and provide trend analyses to develop a more efficient and effective asset protection program. Examines the latest techniques in both generating and evaluating security metrics, with guidance for creating a new metrics program or improving an existing one Features an easy-to-read, comprehensive implementation plan for establishing an asset protection program Outlines detailed strategies for creating metrics that measure the effectiveness and efficiency of an asset protection program Offers increased emphasis through metrics to justify security professionals as integral assets to the corporation Provides a detailed example of a corporation briefing for security directors to provide to executive management

A Text on the Foundation Processes, Analytical Principles, and Implementation Practices of Engineering Risk Management Drawing from the author's many years of hands-on experience in the field, Analytical Methods for Risk Management: A Systems Engineering Perspectivepresents the foundation processes and analytical practices for identifying, analyzing, measuring, and managing risk in traditional systems, systems-of-systems, and enterprise systems. Balances Risk and Decision Theory with Case Studies and Exercises After an introduction to engineering risk management, the book covers the fundamental axioms and properties of probability as well as key aspects of decision analysis, such as preference theory and risk/utility functions. It concludes with a series of essays on major analytical topics, including how to identify, write, and represent risks; prioritize risks in terms of their potential impacts on a systems project; and monitor progress when mitigating a risk's potential adverse effects. The author also examines technical performance measures and how they can combine into an index to track an engineering system's overall performance risk. In addition, he discusses risk management in the context of engineering complex, large-scale enterprise systems. Applies Various Methods to Risk Engineering and Analysis Problems This practical guide enables an understanding of which processes and analytical techniques are valid and how they are best applied to specific systems engineering environments. After reading this book, you will be on your way to managing risk on both traditional and advanced engineering systems.

This book edited by industry expert Michael Ong explores how capital is measured and managed by banks and other financial institutions and how current techniques should be improved to address the issues highlighted in the recent crisis.

For Banks and Financial Institutions

Finding the Value of Intangibles in Business

Measuring and Managing Information Risk

The Owner's Role in Project Risk Management

Building an Information Security Risk Management Program from the Ground Up

Managing and Measuring Capital

A Practitioner's Perspective

Performance Measurement and Management for Engineers introduces key concepts in finance, accounting, and management to project managers who have engineering backgrounds. It focuses these basic concepts on issues of measuring and managing enterprise value. Thus, after defining enterprise value, the book begins by explaining the ways and means of measurement. It then takes up financial measurement, describing and analyzing the typologies of financial indicators while illustrating their advantages and disadvantages. After focusing on measuring enterprise value, the second section takes up managing that value. Like the first, it pursues a double view: using indicators for internal control while employing them to analyze other companies. If engineering project managers possess a source of quantitative and qualitative information about business management, Performance Measurement and Management for Engineers will help them increase their contributions to the business. Explains how main performance indicators are related to the value of the company Reveals how to assess the financial needs of companies in relation to their financial goals and mechanisms (e.g., equity, debt, and hybrid) Describes key information and indicators for assessing the ability of enterprises to create value across time Indicates the profitability sources of different business units

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

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

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.

End the Status Quo, Start an Innovation Revolution

Measuring and Managing Operational Risks in Financial Institutions

FISMA and the Risk Management Framework

Measuring Market Risk

Digital Asset Valuation and Cyber Risk Measurement

Measuring and Managing Credit Risk

Concepts, Techniques, and Tools

In 2011 the World Bank—with funding from the Bill and Melinda Gates Foundation—launched the Global Findex database, the world's most comprehensive data set on how adults save, borrow, make payments, and manage risk. Drawing on survey data collected in collaboration with Gallup, Inc., the Global Findex database covers more than 140 economies around the world. The initial survey round was followed by a second one in 2014 and by a third in 2017. Compiled using nationally representative surveys of more than 150,000 adults age 15 and above in over 140 economies, The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution includes updated indicators on access to and use of formal and informal financial services. It has additional data on the use of financial technology (or fintech), including the use of mobile phones and the Internet to conduct financial transactions. The data reveal opportunities to expand access to financial services among people who do not have an account—the unbanked—as well as to promote greater use of digital financial services among those who do have an account. The Global Findex database has become a mainstay of global efforts to promote financial inclusion. In addition to being widely cited by scholars and development practitioners, Global Findex data are used to track progress toward the World Bank goal of Universal Financial Access by 2020 and the United Nations Sustainable Development Goals. The database, the full text of the report, and the underlying country-level data for all figures—along with the questionnaire, the survey methodology, and other relevant materials—are available at www.worldbank.org/globalfindex.

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.

The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments provides detailed insight into precisely how to conduct an information security risk assessment. Designed for security professionals and their customers who want a more in-depth understanding of the risk assessment process, this volume contains real-wor

Managing and Measuring of Risk

A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Seventh Edition and The Standard for Project Management (BRAZILIAN PORTUGUESE)