Measuring And Managing Information Risk A Fair Approach

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.

A mathematical guide to measuring and managing financial risk. Our modern economy depends on financial markets. Yet financial markets continue to grow in size and complexity. As a result, the management of financial risk has never been more important. Quantitative Financial Risk Management introduces students and risk professionals to financial risk management with an emphasis on financial models and mathematical techniques. Each chapter provides numerous sample problems and end of chapter questions. The book provides clear examples of how these models are used in practice and encourages readers to think about the limits and appropriate use of financial models. Topics include: • Value at risk • Stress testing • Credit risk • Liquidity risk • Factor analysis • Expected shortfall • Copulas • Extreme value theory • Risk model backtesting • Bayesian analysis • . . . and much more

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.

This book bridges the gap between the many different disciplines used in applications of risk analysis to real world problems. Contributed by some of the world's leading experts, it creates a common information base and language for all risk analysis practitioners, risk managers, and decision makers. Valuable as both a reference for practitioners and a comprehensive textbook for students, Fundamentals of Risk Analysis and Risk Management is a unique contribution to the field. Its broad coverage ranges from basic theory of risk analysis to practical applications, risk perception, legal and political issues, and risk management.

This book describes the thought process and specific activities a leader should consider as they interview for the IT risk/information security leader role, what they should do within their first 90 days, and how to organize, evangelize, and operate the program once they are into the job. Information technology (IT) risk and information security management are top of mind for

corporate boards and senior business leaders. Continued intensity of cyber terrorism attacks, regulatory and compliance requirements, and customer privacy concerns are driving the need for a business-minded chief information security officer (CISO) to lead organizational efforts to protect critical infrastructure and sensitive data. A CISO must be able to both develop a practical program aligned with overall business goals and objectives and evangelize this plan with key stakeholders across the organization. The modern CISO cannot sit in a bunker somewhere in the IT operations center and expect to achieve buy in and support for the activities required to operate a program. This book describes the thought process and specific activities a leader should consider as they interview for the IT risk/information security leader role, what they should do within their first 90 days, and how to organize, evangelize, and operate the program once they are into the job. It provides practical, tested strategies for designing your program and guidance to help you be successful long term. It is chock full of examples, case studies, and diagrams right out of real corporate information security programs. The Business-Minded Chief Information Security Officer is a handbook for success as you begin this important position within any company.

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 in risk management and a synthesis of research involving the latest developments in the field.

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.

Conquering cyber attacks requires a multi-sector, multi-modal approach Cyber Threat! How to Manage the Growing Risk of Cyber Attacks is an in-depth examination of the very real cyber

security risks facing all facets of government and industry, and the various factors that must align to maintain information integrity. Written by one of the nation's most highly respected cyber risk analysts, the book describes how businesses and government agencies must protect their most valuable assets to avoid potentially catastrophic consequences. Much more than just cyber security, the necessary solutions require government and industry to work cooperatively and intelligently. This resource reveals the extent of the problem, and provides a plan to change course and better manage and protect critical information. Recent news surrounding cyber hacking operations show how intellectual property theft is now a matter of national security, as well as economic and commercial security. Consequences are far-reaching, and can have enormous effects on national economies and international relations. Aggressive cyber forces in China, Russia, Eastern Europe and elsewhere, the rise of global organized criminal networks, and inattention to vulnerabilities throughout critical infrastructures converge to represent an abundantly clear threat. Managing the threat and keeping information safe is now a top priority for global businesses and government agencies. Cyber Threat! breaks the issue down into real terms, and proposes an approach to effective defense. Topics include: The information at risk The true extent of the threat The potential consequences across sectors The multifaceted approach to defense The growing cyber threat is fundamentally changing the nation's economic, diplomatic, military, and intelligence operations, and will extend into future technological, scientific, and geopolitical influence. The only effective solution will be expansive and complex, encompassing every facet of government and industry. Cyber Threat! details the situation at hand, and provides the information that can help keep the nation safe.

In any organization, risk plays a huge role in the success or failure of any business endeavour. Measuring and managing risk is a difficult and often complicated task and the global financial crisis of the late noughties can be traced to a worldwide deficiency in risk management regimes. One of the problems in understanding how best to manage risk is a lack of detailed examples of real world practice. In this accessible textbook the author sets the world of risk management in the context of the broader corporate governance agenda, as well as explaining the core elements of a risk management system. Material on the differences between risk management and internal auditing is supplemented by a section on the professionalization of risk âe" a relatively contemporary evolution. Enterprise risk management is also fully covered. With a detailed array of risk management cases âe" including Tesco, RBS and the UK government âe" lecturers will find this a uniquely well researched resource, supplemented by materials that enable the cases to be easily integrated into the classroom. Risk managers will be delighted with the case materials made available for the first time with the publication of this book.

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.

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 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 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

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.

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.

Follow step-by-step guidance to craft a successful security program. You will identify with the paradoxes of information security and discover handy tools that hook security controls into business processes. Information security is more than configuring firewalls, removing viruses, hacking machines, or setting passwords. Creating and promoting a successful security program requires skills in organizational consulting, diplomacy, change management, risk analysis, and out-of-the-box thinking. What You Will Learn: Build a security program that will fit neatly into an organization and change dynamically to suit both the needs of the organization and survive constantly changing threats Prepare for and pass such common audits as PCI-DSS, SSAE-16, and ISO 27001 Calibrate the scope, and customize security controls to fit into an organization’s culture Implement the most challenging processes, pointing out common pitfalls and distractions Frame security and risk issues to be clear and actionable so that decision makers, technical personnel, and users will listen and value your advice Who This Book Is For: IT professionals moving into the security field; new security managers, directors, project heads, and would-be CISOs; and security specialists from other disciplines moving into information security (e.g., former military security professionals, law enforcement professionals, and physical security professionals)

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.

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.
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

While it has become increasingly apparent that individuals and organizations need a security metrics program, it has been exceedingly difficult to define exactly what that means in a given situation. There are hundreds of metrics to choose from and an organization's mission, industry, and size will affect the nature and scope of the task as well as

Information Security Science: Measuring the Vulnerability to Data Compromises provides the scientific background and analytic techniques to understand and measure the risk associated with information security threats. This is not a traditional IT security book since it includes methods of information compromise that are not typically addressed in textbooks or journals. In particular, it explores the physical nature of information security risk, and in so doing exposes subtle, yet revealing, connections between information security, physical security, information technology, and information theory. This book is also a practical risk management guide, as it explains the fundamental scientific principles that are directly relevant to information security, specifies a structured methodology to evaluate a host of threats and attack vectors, identifies unique metrics that point to root causes of technology risk, and enables estimates of the effectiveness of risk mitigation. This book is the definitive reference for scientists and

engineers with no background in security, and is ideal for security analysts and practitioners who lack scientific training. Importantly, it provides security professionals with the tools to prioritize information security controls and thereby develop cost-effective risk management strategies. Specifies the analytic and scientific methods necessary to estimate the vulnerability to information loss for a spectrum of threats and attack vectors Represents a unique treatment of the nexus between physical and information security that includes risk analyses of IT device emanations, visible information, audible information, physical information assets, and virtualized IT environments Identifies metrics that point to the root cause of information technology risk and thereby assist security professionals in developing risk management strategies Analyzes numerous threat scenarios and specifies countermeasures based on derived quantitative metrics Provides chapter introductions and end-of-chapter summaries to enhance the reader’s experience and facilitate an appreciation for key concepts

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

Security Risk Assessment is the most up-to-date and comprehensive resource available on how to conduct a thorough security assessment for any organization. A good security assessment is a fact-finding process that determines an organization’s state of security protection. It exposes vulnerabilities, determines the potential for losses, and devises a plan to address these security concerns. While most security professionals have heard of a security assessment, many do not know how to conduct one, how it’s used, or how to evaluate what they have found. Security Risk Assessment offers security professionals step-by-step guidance for conducting a complete risk assessment. It provides a template draw from, giving security professionals the tools needed to conduct an assessment using the most current approaches, theories, and best practices. Discusses practical and proven techniques for effectively conducting security assessments Includes interview guides, checklists, and sample reports Accessibly written for security professionals with different levels of experience conducting security assessments

The number one guide to corporate valuation is back and better than ever Thoroughly revised and expanded to reflect business conditions in today's volatile global economy, Valuation, Fifth Edition continues the tradition of its bestselling predecessors by providing up-to-date insights and practical advice on how to create, manage, and measure the value of an organization. Along with all new case studies that illustrate how valuation techniques and principles are applied in real-world situations, this comprehensive guide has been updated to reflect new developments in corporate finance, changes in accounting rules, and an enhanced global perspective. Valuation, Fifth Edition is filled with expert guidance that managers at all levels, investors, and students can use to enhance their understanding of this important discipline. Contains strategies for multi-business valuation and valuation for corporate restructuring, mergers, and acquisitions Addresses how you can interpret the results of a valuation in light of a company's competitive situation Also available: a book plus CD-ROM package (978-0-470-42469-8) as well as a stand-alone CD-ROM (978-0-470-42457-7) containing an interactive valuation DCF model Valuation, Fifth Edition stands alone in this field with its reputation of quality and consistency. If you want to hone your valuation skills today and improve them for years to come, look no further than this book.

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.

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

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.

"Drawing on practical methods used by successful risk managers in emerging and developed markets throughout the world, the book provides specific guidance on establishing a modern risk management framework and developing efficient approaches to increase the profitability of risk management activities in emerging market settings."--BOOK JACKET.

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

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 information assurance 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 initiatives for 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 industrial control 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 Information 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 development and 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 continuity management Backup and restoration Cloud computing and outsourcing strategies Information assurance big data concerns

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.

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

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 modelling in the future of digitization, thus providing industry professionals with the tools they need to optimize the management of financial risks associated with this mega trend. The book addresses three problem areas: the valuation of digital assets, measurement of risk exposures of digital valuables, and economic modelling 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, organisation, 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 Analyses 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 cyber security 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, i.e., 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 optimisation for managing residual cyber risk Provides a case study on cyber insurance
This book addresses three main dimensions of risk management in emerging markets: 1) the effectiveness of risk management practices; 2) current issues and challenges in risk assessment and modelling in emerging market countries; 3) the responses of emerging markets to the recent financial crises and the design of risk management models.
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.

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

PART OF THE JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Revised and updated with the latest data in the field, the Second Edition of Managing Risk in Information Systems provides a comprehensive overview of the SSCP(r) Risk, Response, and Recovery Domain in addition to providing a thorough overview of risk management and its implications on IT infrastructures and compliance. Written by

industry experts, and using a wealth of examples and exercises, this book incorporates hands-on activities to walk the reader through the fundamentals of risk management, strategies and approaches for mitigating risk, and the anatomy of how to create a plan that reduces risk. Instructor's Material for Managing Risk in Information Systems include: PowerPoint Lecture Slides Instructor's Guide Course Syllabus Quiz & Exam Questions Case Scenarios/Handouts The Second Edition of this best-selling book expands its advanced approach to financial risk models by covering market, credit, and integrated risk. With new data that cover the recent financial crisis, it combines Excel-based empirical exercises at the end of each chapter with online exercises so readers can use their own data. Its unified GARCH modeling approach, empirically sophisticated and relevant yet easy to implement, sets this book apart from others. Four new chapters and updated end-of-chapter questions and exercises, as well as Excel-solutions manual and PowerPoint slides, support its step-by-step approach to choosing tools and solving problems. Examines market risk, credit risk, and operational risk Provides exceptional coverage of GARCH models Features online Excel-based empirical exercises As a security professional, have you found that you and others in your company do not always define “security” the same way? Perhaps security interests and business interests have become misaligned. Brian Allen and Rachelle Loyear offer a new approach: Enterprise Security Risk Management (ESRM). By viewing security through a risk management lens, ESRM can help make you and your security program successful. In their long-awaited book, based on years of practical experience and research, Brian Allen and Rachelle Loyear show you step-by-step how Enterprise Security Risk Management (ESRM) applies fundamental risk principles to manage all security risks. Whether the risks are informational, cyber, physical

security, asset management, or business continuity, all are included in the holistic, all-encompassing ESRM approach which will move you from task-based to risk-based security. How is ESRM familiar? As a security professional, you may already practice some of the components of ESRM. Many of the concepts – such as risk identification, risk transfer and acceptance, crisis management, and incident response – will be well known to you. How is ESRM new? While many of the principles are familiar, the authors have identified few organizations that apply them in the comprehensive, holistic way that ESRM represents – and even fewer that communicate these principles effectively to key decision-makers. How is ESRM practical? ESRM offers you a straightforward, realistic, actionable approach to deal effectively with all the distinct types of security risks facing you as a security practitioner. ESRM is performed in a life cycle of risk management including: Asset assessment and prioritization. Risk assessment and prioritization. Risk treatment (mitigation). Continuous improvement. Throughout Enterprise Security Risk Management: Concepts and Applications, the authors give you the tools and materials that will help you advance you in the security field, no matter if you are a student, a newcomer, or a seasoned professional. Included are realistic case studies, questions to help you assess your own security program, thought-provoking discussion questions, useful figures and tables, and references for your further reading. By redefining how everyone thinks about the role of security in the enterprise, your security organization can focus on working in partnership with business leaders and other key stakeholders to identify and mitigate security risks. As you begin to use ESRM, following the instructions in this book, you will experience greater personal and professional satisfaction as a security professional – and you'll become a recognized and trusted partner in the business-

critical effort of protecting your enterprise and all its assets.