Information Technology Risk Management In Enterprise Environments A Review Of Industry Practices And A Practical Guide To Risk Management Teams

Attacks on information systems and applications have become more prevalent with new advances in technology. Management of security and quick threat identification have become imperative aspects of technological applications. Information Technology Risk Management and Compliance in Modern Organizations is a pivotal reference source featuring the latest scholarly research on the need for an effective chain of information management and clear principles of information technology governance. Including extensive coverage on a broad range of topics such as compliance programs, data leak prevention, and security architecture, this book is ideally designed for IT professionals, scholars, researchers, and academicians seeking current research on risk management and compliance.

This work adds a new perspective to the stream of organizational IT security risk management literature, one that sheds light on the importance of IT security risk perceptions. Based on a large-scale empirical study of Cloud providers located in North America, the study reveals that in many cases, the providers' decision makers significantly underestimate their services' IT security risk exposure, which inhibits the implementation of necessary safeguarding measures. The work also demonstrates that even though the prevalence of IT security risk concerns in Cloud adoption is widely recognized, providers only pay very limited attention to the concerns expressed by customers, which not only causes serious disagreements with the customers but also considerably inhibits the adoption of the services.

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

There has never been a IT Risk Management Guide like this. IT Risk Management 20 Success Secrets is not about the ins and outs of IT Risk Management. Instead, it answers the top 20 questions that we are asked and those we come across in our forums, consultancy and education programs. It tells you exactly how to deal with those questions, with tips that have never before been offered in print. Get the information you need--fast! This comprehensive guide offers a thorough view of key knowledge and detailed insight. This Guide introduces everything you want to know to be successful with IT Risk Management. A quick look inside of the subjects covered: Risk IT Principles, Risk Management Tutorial - The Substitute of Classroom Training, So You Want to Be An Audit Risk Management Analyst?, IT Risk, IT Risk Management Tips that can Help You, So, what next?, Introduction Risk management i, Risk Management Process, Risk IT Three Domains, Conclusion, Basel III, Topic: audit risk management analyst, Introduction risk management, Why Risk Management Fails in IT?, What is IT Risk, Benefits, Risk IT Framework, The Importance of IT Management Risk Planning, IT Risk Management Essentials, The role of Information Technology in a Risk Management Program, and much more...

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® Risk, Response, and Recovery Domain in addition to providing a thorough overview of risk management and its implications on IT infrastructu

Information Technology (IT) has become the driving force behind businesses and organizations. However, Information Technology comes with risks and other vulnerabilities. And by the same token, IT also poses threats to the organization. This then means that every organization must be able to contain and manage these risks and threats well, if it is to stay in the market and competitive. Information Technology Risk Management is to control Information Technology risks occurrences, acceptance and mitigate them. This means, organizations need proper precautionary measures and management tools to be able to identify risks, analyze risks, monitor the risks and have risk-reducing measures. This dissertation is about Information Technology Risk Management. Small and Medium Enterprises (SMEs) operating in South Africa tend to focus more on business operations, often neglecting the need to manage Information Technology risks effectively.

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

Discusses all types of corporate risks and practical means of defending against them. Security is currently identified as a critical area of Information Technology management by a majority of government, commercial, and industrial organizations. Offers an effective risk management program, which is the most critical function of an information security program.

This volume constitutes the refereed and revised post-conference proceedings of the 5th IFIP WG 5.15 International Conference on Information Technology in Disaster Risk

Reduction, ITDRR 2020, in Sofia, Bulgaria, in December 2020.* The 18 full papers and 6 short papers presented were carefully reviewed and selected from 52 submissions. The papers focus on various aspects and challenges of coping with disaster risk reduction. The main topics include areas such as natural disasters, remote sensing, big data, cloud computing, Internet of Things, mobile computing, emergency management, disaster information processing, disaster risk assessment and management. *The conference was held virtually.

The book examines a wide range of issues that characterize the current IT based innovation trends in organisations. It contains a collection of research papers focusing on themes of growing interest in the field of Information System, Organization Studies, and Management. The book offers a multi-disciplinary view on Information Systems aiming to disseminate academic knowledge. It might be particularly relevant to IT practitioners such as information systems managers, business managers and IT consultants. The volume is divided into XIV sections, each one focusing on a specific theme. A preface written by Joey George, president of the Association for Information Systems opens the text. The content of each section is based on a selection of the best papers (original double blind peer reviewed contributions) presented at the annual conference of the Italian chapter of AIS, which has been held in Naples, Italy, on October 2010.

Information Technology Risk Management in Enterprise EnvironmentsA Review of Industry Practices and a Practical Guide to Risk Management TeamsJohn Wiley & Sons

Since its first volume in 1960, Advances in Computers has presented detailed coverage of innovations in hardware and software and in computer theory, design, and applications. It has also provided contributorswith a medium in which they can examine their subjects in greater depth and breadth than that allowed by standard journal articles. As a result, many articles have become standard references that continue to be of significant, lasting value despite the rapid growth taking place in the field.

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.

This book is about information systems development failures and how to avoid them. It considers what goes wrong with information systems development projects and what actions may be taken to avoid potential difficulties.The reduction of the impact,or even the elimination of the problems,is discussed in terms of an information systems risk management programme. Stop I.T.Project failure helps to ensure that IS project managers are successful in helping to deliver application systems. However, IS development risk can never be entirely eliminated and consequently the practitioner needs to bear in mind that an IS development project is never without risk, and hence there is a continuing potential for something to go wrong. The book covers the key issues and variables and makes specific practical suggestions about the good management practice that is required to implement IS project risk processes. Dr. Dan Remenyi has spent more than 25 years working in the field of corporate computers and information systems. He has worked with computers as an IS professional, business consultant and user. In all these capacities he has been primarily concerned with benefit realisation and obtaining the maximum value for money from the organisations' information systems investment and effort. He has worked extensively in the field of information systems project management, specialising in the area of project risk identification and management. He has written a number of books and papers in the field of IT management and regularly conducts courses and seminars as well as working as a consultant in this area. Dr.Dan Remenyi holds a B.Soc.Sc., an MBA and a PhD. He is a Visiting Professor at Chalmers University of Technology in Gothenberg, Sweden and an associate member of faculty at Henley Management College in the United Kingdom. asks what goes wrong with IT projects shows how to perform a financial analysis for the risks looks at how to minimise the impact shows you how to manage a risk program

This book is going to help you understand the basic concept of Risk Management in reference to standards, ISO 31001:2018 and ISO 27001:2013 which are a published standard from ISO. We have tried to gather the information from various sources and providing the same at a single place to be ready to help you understand the concept of Risk Management which is now an integral part of all the new standards including, ISO 9001:2015 (quality Management System), ISO 14001:2015 (Environmental Management System), ISO 27001:2013 (Information Security Management System). In this book, we are trying to put the information from various references and rephrase the same in simple language for easy understanding. The purpose and focus of this book is the concept of Risk Management with respect to Data Security.

There has never been a IT Risk Management Guide like this. It contains 206 answers, much more than you can imagine; comprehensive answers and extensive details and references, with insights that have never before been offered in print. Get the information you need--fast! This all-embracing guide offers a thorough view of key knowledge and detailed insight. This Guide introduces what you want to know about IT Risk Management. A quick look inside of some of the subjects covered: Federal Information Security Management Act of 2002 - Continuous monitoring, Mobile security - Articles, Particle accelerator - Black hole production and public safety concerns, Software development methodology - Spiral development, Global Information Assurance Certification - Security Administration, National Institute of Standards and Technology - Committees, Network theory in risk assessment, Burson-Marsteller, Credit card Security

problems and solutions, Microsoft Office 365 Security, Information science - Information access, Information Security Forum - Methodologies and tools, Python (programming language) - Use, IT risk, Brian Wynne, Corporate governance of information technology Frameworks, ISO/IEC 27002 - Ongoing development, Information security - Definitions, Technomancy - Examples, Automated teller machine - Physical, Enterprise risk management - Internal audit role, Asset (computer security) - The CIA Triad, ISO/IEC 27003, Business continuity planning, Sylvia Kierkegaard - Recent publications, Guard (information security), Certified Ethical Hacker - Examination, Risk management - Risk Options, ISO/IEC 27006, Nuclear power, Delta Works - Delta law and conceptual framework, Operational risk management, Security risk - Psychological Factors relating to Security Risk, Security - Security management in organizations, and much more...

Every organization has a mission. In this digital era, as organizations use automated information technology (IT) systems1 to process their information for better support of their missions, risk management plays a critical role in protecting an organization's information assets, and therefore its mission, from IT-related risk. An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization. Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help organizations to better manage IT related mission risks. In addition, this guide provides information on the selection of cost effective security controls.2 These controls can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and carry this information. Organizations may choose to expand or abbreviate the comprehensive processes and steps suggested in this guide and tailor them to their environment in managing IT-related mission risks. The objective of performing risk management is to enable the organization to accomplish its mission(s) (1) by better securing the IT systems that store, process, or transmit organizational information; (2) by enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget; and (3) by assisting management in authorizing (or accrediting) the IT systems3 on the basis of the supporting documentation resulting from the performance of risk management

Are you exposing your business to IT risk, and leaving profit opportunities on the table? You might be if you are managing your IT risk using more traditional approaches. IT Risk, a new book based on research conducted by MIT s Center for Information Systems Research and Gartner, Inc., helps companies focus on the most pressing risks and leverage the upside that comes with vigilance. Traditionally, managers have grouped technology risk and funding into silos. IT Risk outlines a new model for integrated risk management, which identifies three core areas you can develop to eliminate the problems that silo strategies create. The authors also offer specific ways to make the most of your new found advantage. And because IT risk is the responsibility of all senior executives not just CIOs this book describes the tools and practices in language that general managers can understand and use. Named a top-ten managerial book of 2007 by CIO Insight magazine.

This volume constitutes the refereed and revised post-conference proceedings of the 4th IFIP TC 5 DCITDRR International Conference on Information Technology in Disaster Risk Reduction, ITDRR 2019, in Kyiv, Ukraine, in October 2019. The 17 full papers and 2 short papers presented were carefully reviewed and selected from 53 submissions. The papers focus on various aspects and challenges of coping with disaster risk reduction. The main topics include areas such as natural disasters, big data, cloud computing, Internet of Things, mobile computing, emergency management, disaster information processing, and disaster risk assessment and management.

Written for professionals in financial services with responsibility for IT and risk management, Dimitris Chorafas surveys the methodology required and IT systems and structures to support it according to Basel II. The book is consistent with the risk management certification process of GARP, as well as the accounting rules of IFRS, based on research the author conducted with IASB. The author provices an in-depth discussion of the types of risk, stress analysis and the use of scenarios, mathematical models, and IT systems and infrastructure requirements. * Written in clear, straightforward style for financial industry executives to provide necessary information for risk control decisionmaking * Consistent with GARP, IFRS and IASB risk management processes and procedures * Explains stress testing and its place in risk control

Seminar paper from the year 2011 in the subject Computer Science - Commercial Information Technology, grade: 1,0, AKAD University of Applied Sciences Stuttgart, course: Enterprise and IT Architecture Management, language: English, comment: Diese Seminararbeit wurde im Rahmen des berufsbegleitenden Master-Studiengangs "Wirtschaftsinformatik" erstellt., abstract: "In the twenty-first century, IT architecture will be the determining factor. The factor that separates the winners from the losers, the successful and the failures, the survivors from the others." (Zachman, 1996, p. 2) The author Zachman (1996, p. 7) emphasises in his article the growing significance of IT architecture for modern enterprises. According to Zachman (1996, p. 1) IT architecture aligns business strategy with information technology and enables the achievement of business goals. Therefore, an efficient IT architecture is a key factor for companies which are faced with increasing changing markets and shorter product life cycles. In contrast to that, an estimated 68% of corporate IT projects are neither on time nor on budget and they don't deliver the original stated business goals (Jeffery & Leliveld, 2004). Regarding Fairbanks (2010, p. 8) a major cause for this is an insufficient risk management in the IT architecture development in principle. Therefore many IT architects ask themselves, how they could identify and prioritize their project's most pressing risks? Which architecture and design techniques mitigate the risks and what is the amount of risk reduction? In order to answer these questions, section 2.1 defines the terms architecture and enterprise architecture before it deals with the IT architecture itself. The following section 2.2 gives an overview of risk and risk management in general. Chapter 3 presents the main chapter of this assignment. At first, it gives a brief overview of the role of IT risk management in the scope of strategic management. The next two sections illustrate t

The book provides the complete strategic understanding requisite to allow a person to create and use the RMF process recommendations for risk management. This will be the case both for

applications of the RMF in corporate training situations, as well as for any individual who wants to obtain specialized knowledge in organizational risk management. It is an all-purpose roadmap of sorts aimed at the practical understanding and implementation of the risk management process as a standard entity. It will enable an "application" of the risk management process as well as the fundamental elements of control formulation within an applied context.

The headline-grabbing financial scandals of recent years have led to a great urgency regarding organizational governance and security. Information technology is the engine that runs modern organizations, and as such, it must be well-managed and controlled. Organizations and individuals are dependent on network environment technologies, increasing the importance of security and privacy. The field has answered this sense of urgency with advances that have improved the ability to both control the technology and audit the information that is the lifeblood of modern business. Reflects the Latest Technological Advances Updated and revised, this third edition of Information Technology Control and Audit continues to present a comprehensive overview for IT professionals and auditors. Aligned to the CobiT control objectives, it provides a fundamental understanding of IT governance, controls, auditing applications, systems development, and operations. Demonstrating why controls and audits are critical, and defining advances in technology designed to support them, this volume meets the increasing need for audit and control professionals to understand information technology and the controls required to manage this key resource. A Powerful Primer for the CISA and CGEIT Exams Supporting and analyzing the CobiT model, this text prepares IT professionals for the CISA and CGEIT exams. With summary sections, exercises, review questions, and references for further readings, it promotes the mastery of the concepts and practical implementation of controls needed to effectively manage information technology resources. New in the Third Edition: Reorganized and expanded to align to the CobiT objectives Supports study for both the CISA and CGEIT exams Includes chapters on IT financial and sourcing management Adds a section on Delivery and Support control objectives Includes additional content on audit and control of outsourcing, change management, risk management, and compliance

Are you exposing your business to IT risk, and leaving profit opportunities on the table? You might be if you are managing your IT risk using more traditional approaches. The IT Risk Management Guide, a new book based on research conducted by The Art of Service and ITIL's Best Practices, helps companies focus on the most pressing risks and leverage the upside that comes with vigilance. Traditionally, managers have grouped technology risk and funding into silos. The IT Risk Management Guide outlines a new Process driven model for integrated risk management, which identifies core areas you can develop to eliminate the problems that silo strategies create. The authors also offer specific ways to make the most of your new found advantage by offering blueprints and templates, ready to use. And because IT risk is the responsibility of all senior executives and not just CIOs this book describes the tools and practices in language that general managers can understand and use.

The goal of Security Risk Management is to teach you practical techniques that will be used on a daily basis, while also explaining the fundamentals so you understand the rationale behind these practices. Security professionals often fall into the trap of telling the business that they need to fix something, but they can't explain why. This book will help you to break free from the so-called "best practices" argument by articulating risk exposures in business terms. You will learn techniques for 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 guide for managing security risks. 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

Risk Management for Computer Security provides IT professionals with an integrated plan to establish and implement a corporate risk assessment and management program. The book covers more than just the fundamental elements that make up a good risk program for computer security. It presents an integrated how-to approach to implementing a corporate program, complete with tested methods and processes, flowcharts, and checklists that can be used by the reader and immediately implemented into a computer and overall corporate security program. The challenges are many and this book will help professionals in meeting their challenges as we progress through the twenty-first century. This book is organized into five sections. Section I introduces the reader to the theories of risk management and describes the field's changing environment as well as the art of managing risks. Section II deals with threat assessment and its input to risk assessment; topics covered include the threat assessment method and an example of threat assessment. Section III focuses on operating system vulnerabilities and discusses application vulnerabilities; public domain vs. COTS; and connectivity and dependence. Section IV explains what risk assessment is and Section V explores qualitative vs. quantitative tools and types of risk assessment and concludes with an assessment of the future of risk management. Corporate security professionals around the world will find this book a highly valuable source of information. Presents material in an engaging, easy-to-follow manner that will appeal to both advanced INFOSEC career professionals and network administrators entering the information security profession Addresses the needs of both the individuals who are new to the subject as well as of experienced professionals Provides insight into the factors that need to be considered and fully explains the numerous methods, processes and procedures of risk management