

Download Ebook 2015 Manual Review Cgeit Isaca

Recognizing the pretension ways to get this ebook **2015 Manual Review Cgeit Isaca** is additionally useful. You have remained in right site to begin getting this info. acquire the 2015 Manual Review Cgeit Isaca partner that we give here and check out the link.

You could purchase guide 2015 Manual Review Cgeit Isaca or get it as soon as feasible. You could quickly download this 2015 Manual Review Cgeit Isaca after getting deal. So, taking into account you require the books swiftly, you can straight acquire it. Its correspondingly agreed easy and so fats, isnt it? You have to favor to in this atmosphere

KEY=REVIEW - HICKS DICKERSON

CGEIT REVIEW QUESTIONS, ANSWERS AND EXPLANATIONS MANUAL 2015

CGEIT REVIEW QUESTIONS, ANSWERS AND EXPLANATIONS MANUAL 2015 SUPPLEMENT

CGEIT REVIEW MANUAL 2015

PRIVACY, REGULATIONS, AND CYBERSECURITY

THE ESSENTIAL BUSINESS GUIDE

John Wiley & Sons Protect business value, stay compliant with global regulations, and meet stakeholder demands with this privacy how-to Privacy, Regulations, and Cybersecurity: The Essential Business Guide is your guide to understanding what "privacy" really means in a corporate environment: how privacy is different from cybersecurity, why privacy is essential for your business, and how to build privacy protections into your overall cybersecurity plan. First, author Chris Moschovitis walks you through our evolving definitions of privacy, from the ancient world all the way to the General Law on Data Protection (GDPR). He then explains—in friendly, accessible language—how to orient your preexisting cybersecurity program toward privacy, and how to make sure your systems are compliant with current regulations. This book—a sequel to Moschovitis' well-received Cybersecurity Program Development for Business—explains which regulations apply in which regions, how they relate to the end goal of privacy, and how to build privacy into both new and existing cybersecurity programs. Keeping up with swiftly changing technology and business landscapes is no easy task. Moschovitis provides down-to-earth, actionable advice on how to avoid dangerous privacy leaks and protect your valuable data assets. Learn how to design your cybersecurity program with privacy in mind Apply lessons from the GDPR and other landmark laws Remain compliant and even get ahead of the curve, as privacy grows from a buzzword to a business must Learn how to protect what's of value to your company and your stakeholders, regardless of business size or industry Understand privacy regulations from a business standpoint, including which regulations apply and what they require Think through what privacy protections will mean in the post-COVID environment Whether you're new to cybersecurity or already have the fundamentals, this book will help you design and build a privacy-centric, regulation-compliant cybersecurity program.

CYBERSECURITY PROGRAM DEVELOPMENT FOR BUSINESS

THE ESSENTIAL PLANNING GUIDE

John Wiley & Sons "This is the book executives have been waiting for. It is clear: With deep expertise but in nontechnical language, it describes what cybersecurity risks are and the decisions executives need to make to address them. It is crisp: Quick and to the point, it doesn't waste words and won't waste your time. It is candid: There is no sure cybersecurity defense, and Chris Moschovitis doesn't pretend there is; instead, he tells you how to understand your company's risk and make smart business decisions about what you can mitigate and what you cannot. It is also, in all likelihood, the only book ever written (or ever to be written) about cybersecurity defense that is fun to read." —Thomas A. Stewart, Executive Director, National Center for the Middle Market and Co-Author of Woo, Wow, and Win: Service Design, Strategy, and the Art of Customer Delight Get answers to all your cybersecurity questions In 2016, we reached a tipping point—a moment where the global and local implications of cybersecurity became undeniable. Despite the seriousness of the topic, the term "cybersecurity" still exasperates many people. They feel terrorized and overwhelmed. The majority of business people have very little understanding of cybersecurity, how to manage it, and what's really at risk. This essential guide, with its dozens of examples and case studies, breaks down every element of the development and management of a cybersecurity program for the executive. From understanding the need, to core risk management principles, to threats, tools, roles and responsibilities, this book walks the reader through each step of developing and implementing a cybersecurity program. Read cover-to-cover, it's a thorough overview, but it can also function as a useful reference book as individual questions and difficulties arise. Unlike other cybersecurity books, the text is not bogged down with industry jargon Speaks specifically to the executive who is not familiar with the development or implementation of cybersecurity programs Shows you how to make pragmatic, rational, and informed decisions for your organization Written by a top-flight technologist with decades of experience and a track record of success If you're a business manager or executive who needs to make sense of cybersecurity, this book demystifies it for you.

RADICAL REORGANIZATION OF EXISTING WORK STRUCTURES THROUGH DIGITALIZATION

IGI Global Technological advancements are occurring in many areas of life and society, especially in the field of business. With the increase in advancement, digital technologies are assisting workers and making them more viable in the labor market. Radical Reorganization of Existing Work Structures Through Digitalization is a critical scholarly resource that examines the endeavors of the digitalization of skill development initiatives for sustainable and inclusive growth and development of organizations and economies worldwide. Featuring coverage on a broad range of topics such as social media, online teaching, and e-learning, this book is geared towards academicians, researchers, and students seeking current research on the advantages of a relationship between the digital world and the workforce.

FISMA COMPLIANCE HANDBOOK

SECOND EDITION

Newnes This comprehensive book instructs IT managers to adhere to federally mandated compliance requirements. FISMA Compliance Handbook Second Edition explains what the requirements are for FISMA compliance and why FISMA compliance is mandated by federal law. The evolution of Certification and Accreditation is discussed. This book walks the reader through the entire FISMA compliance process and includes guidance on how to manage a FISMA compliance project from start to finish. The book has chapters for all FISMA compliance deliverables and includes information on how to conduct a FISMA compliant security assessment. Various topics discussed in this book include the NIST Risk Management Framework, how to characterize the sensitivity level of your system, contingency plan, system security plan development, security awareness training, privacy impact assessments, security assessments and more. Readers will learn how to obtain an Authority to Operate for an information system and what actions to take in regards to vulnerabilities and audit findings. FISMA Compliance Handbook Second Edition, also includes all-new coverage of federal cloud computing compliance from author Laura Taylor, the federal government's technical lead for FedRAMP, the government program used to assess and authorize cloud products and services. Includes new information on cloud computing compliance from Laura Taylor, the federal government's technical lead for FedRAMP Includes coverage for both corporate and government IT managers Learn how to prepare for, perform, and document FISMA compliance projects This book is used by various colleges and universities in information security and MBA curriculums

GOVERNANCE OF ENTERPRISE IT BASED ON COBIT 5

A MANAGEMENT GUIDE

IT Governance Ltd Written for IT service managers, consultants and other practitioners in IT governance, risk and compliance, this practical book discusses all the key concepts of COBIT®5, and explains how to direct the governance of enterprise IT (GEIT) using the COBIT®5 framework. The book also covers the main frameworks and standards supporting GEIT, discusses the ideas of enterprise and governance, and shows the path from corporate governance to the governance of enterprise IT.

CGEIT REVIEW MANUAL 7TH EDITON

KNOWLEDGE-BASED SOFTWARE ENGINEERING: 2018

PROCEEDINGS OF THE 12TH JOINT CONFERENCE ON KNOWLEDGE-BASED SOFTWARE ENGINEERING (JCKBSE 2018) CORFU, GREECE

Springer This book summarizes the new research results presented at the 12th Joint Conference on Knowledge-Based Software Engineering (JCKBSE 2018), which took place on August 27-30, 2018 on the island of Corfu, Greece. The JCKBSE is a well-established international biennial conference that focuses on the applications of Artificial Intelligence in Software Engineering. The JCKBSE 2018 was organized by the Department of Informatics of the University of Piraeus, the Department of Computer and Information Engineering of Nippon Institute of Technology, and the Department of Informatics of Ionian University. The book will benefit not only experts and researchers in the field of (Knowledge-Based) Software Engineering, but also general readers in the fields of Artificial Intelligence, Computational Intelligence and Computer Science who wish to learn more about the field of (Knowledge-Based) Software Engineering and its applications. An extensive list of bibliographic references at the end of each paper encourages readers to probe further into the application areas that interest them most.

TRANSFORMING HEALTHCARE THROUGH INFORMATION SYSTEMS

PROCEEDINGS OF THE 24TH INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS DEVELOPMENT

Springer This book introduces ongoing reflections within the research community on established information systems development topics and emerging concepts, approaches and ideas in the field of healthcare information systems. By promoting research on theoretical and methodological issues related to both information systems development in general and healthcare information systems in particular, it presents current research in order to promote improved practice. It comprises a selection of the best papers presented at the 24th International Conference on Information Systems Development (ISD) held in Harbin, China, August 25 - 27, 2015.

SECURING THE VIRTUAL ENVIRONMENT, INCLUDED DVD

HOW TO DEFEND THE ENTERPRISE AGAINST ATTACK

John Wiley & Sons A step-by-step guide to identifying and defending against attacks on the virtual environment As more and more data is moved into virtual environments the need to secure them becomes increasingly important. Useful for service providers as well as enterprise and small business IT professionals the book offers a broad look across virtualization used in various industries as well as a narrow view of vulnerabilities unique to virtual environments. A companion DVD is included with recipes and testing scripts. Examines the difference in a virtual model versus traditional computing models and the appropriate technology and procedures to defend it from attack Dissects and exposes attacks targeted at the virtual environment and the steps necessary for defense Covers information security in virtual environments: building a virtual attack lab, finding leaks, getting a side-channel, denying or compromising services, abusing the hypervisor, forcing an interception, and spreading infestations Accompanying DVD includes hands-on examples and code This how-to guide arms IT managers, vendors, and architects of virtual environments with the tools they need to protect against common threats.

COBIT 5

IMPLEMENTATION

ISACA

CGEIT REVIEW MANUAL, 8TH EDITION

CISA EXAM-STUDY GUIDE BY HEMANG DOSHI

Independently Published After launch of Hemang Doshi's CISA Video series, there was huge demand for simplified text version for CISA Studies. This book has been designed on the basis of official resources of ISACA with more simplified and lucid language and explanation. Book has been designed considering following objectives: * CISA aspirants with non-technical background can easily grasp the subject. * Use of SmartArts to review topics at the shortest possible time.* Topics have been profusely illustrated with diagrams and examples to make the concept more practical and simple. * To get good score in CISA, 2 things are very important. One is to understand the concept and second is how to deal with same in exam. This book takes care of both the aspects.* Topics are aligned as per official CISA Review Manual. This book can be used to supplement CRM.* Questions, Answers & Explanations (QAE) are available for each topic for better understanding. QAEs are designed as per actual exam pattern. * Book contains last minute revision for each topic. * Book is designed as per exam perspective. We have purposefully avoided certain topics which have nil or negligible weightage in cisa exam. To cover entire syllabus, it is highly recommended to study CRM.* We will feel immensely rewarded if CISA aspirants find this book helpful in achieving grand success in academic as well as professional world.

GRAY HAT HACKING: THE ETHICAL HACKER'S HANDBOOK, FIFTH EDITION

McGraw Hill Professional Cutting-edge techniques for finding and fixing critical security flaws Fortify your network and avert digital catastrophe with proven strategies from a team of security experts. Completely updated and featuring 13 new chapters, Gray Hat Hacking, The Ethical Hacker's Handbook, Fifth Edition explains the enemy's current weapons, skills, and tactics and offers field-tested remedies, case studies, and ready-to-try testing labs. Find out how hackers gain access, overtake network devices, script and inject malicious code, and plunder Web applications and browsers. Android-based exploits, reverse engineering techniques, and cyber law are thoroughly covered in this state-of-the-art resource. And the new topic of exploiting the Internet of things is introduced in this edition. •Build and launch spoofing exploits with Ettercap •Induce error conditions and crash software using fuzzers •Use advanced reverse engineering to exploit Windows and Linux software •Bypass Windows Access Control and memory protection schemes •Exploit web applications with Padding Oracle Attacks •Learn the use-after-free technique used in recent zero days •Hijack web browsers with advanced XSS attacks •Understand ransomware and how it takes control of your desktop •Dissect Android malware with JEB and DAD decompilers •Find one-day vulnerabilities with binary diffing •Exploit wireless systems with Software Defined Radios (SDR) •Exploit Internet of things devices •Dissect and exploit embedded devices •Understand bug bounty programs •Deploy next-generation honeypots •Dissect ATM malware and analyze common ATM attacks •Learn the business side of ethical hacking

CRISC REVIEW MANUAL 6TH EDITION

THE RISK IT FRAMEWORK

ISACA

CISO LEADERSHIP

ESSENTIAL PRINCIPLES FOR SUCCESS

CRC Press Caught in the crosshairs of "Leadership" and "Information Technology", Information Security professionals are increasingly tapped to operate as business executives. This often puts them on a career path they did not expect, in a field not yet clearly defined. IT training does not usually includemanagerial skills such as leadership, team-building, communication, risk assessment, and corporate business savvy, needed by CISOs. Yet a lack in any of these areas can short circuit a career in information security. CISO Leadership: Essential Principles for Success captures years of hard knocks, success stories, and yes, failures. This is not a how-to book or a collection of technical data. It does not cover products or technology or provide a recapitulation of the common body of knowledge. The book delineates information needed by security leaders and includes from-the-trenches advice on how to have a successful career in the field. With a stellar panel of contributors including William H. Murray, Harry Demaio, James Christiansen, Randy Sanovic, Mike Corby, Howard Schmidt, and other thought leaders, the book brings together the collective experience of trail blazers. The authors have learned through experience—been there, done that, have the t-shirt—and yes, the scars. A glance through the contents demonstrates the breadth and depth of coverage, not only in topics included but also in expertise provided by the chapter authors. They are the pioneers, who, while initially making it up as they went along, now provide the next generation of information security professionals with a guide to success.

INFORMATION TECHNOLOGY CONTROL AND AUDIT, FIFTH EDITION

CRC Press The new fifth edition of Information Technology Control and Audit has been significantly revised to include a comprehensive overview of the IT environment, including revolutionizing technologies, legislation, audit process, governance, strategy, and outsourcing, among others. This new edition also outlines common IT audit risks, procedures, and involvement associated with major IT audit areas. It further provides cases featuring practical IT audit scenarios, as well as sample documentation to design and perform actual IT audit work. Filled with up-to-date audit concepts, tools, techniques, and references for further reading, this revised edition promotes the mastery of concepts, as well as the effective implementation and assessment of IT controls by organizations and auditors. For instructors and lecturers there are an instructor's manual, sample syllabi and course schedules, PowerPoint lecture slides, and test questions. For students there are flashcards to test their knowledge of key terms and recommended further readings. Go to <http://routledge/textbooks.com/textbooks/9781498752282/> for more information.

INNOVANDO LA EDUCACIÓN EN LA TECNOLOGÍA

ACTAS DEL II CONGRESO INTERNACIONAL DE INGENIERÍA DE SISTEMAS

Universidad de Lima Este libro recoge las conferencias magistrales y las ponencias presentadas durante el II Congreso Internacional de Ingeniería de Sistemas, denominado Innovando la Educación en Tecnología, organizado por la Carrera de Ingeniería de Sistemas de la Universidad de Lima, el cual tuvo lugar en la capital peruana los días 5 y 6 de septiembre del 2019. Su temática principal giró alrededor del impacto de las tecnologías de la información en la educación. Las ponencias magistrales y los trabajos de investigación presentados ofrecieron innovadoras experiencias de aplicación y prometedoras líneas de trabajo futuro encaminadas a la transformación de las formas tradicionales de educación hacia esquemas dinámicos y soportados fuertemente por la tecnología. La aplicación de paradigmas innovadores basados en técnicas de improvisación, gamificación, educación en ingeniería y enseñanza de la programación demostraron el potencial impacto que el binomio tecnología-educación puede generar en todos los niveles educativos y en diversos contextos de enseñanza-aprendizaje.

INFORMATION SECURITY GOVERNANCE SIMPLIFIED

FROM THE BOARDROOM TO THE KEYBOARD

CRC Press Security practitioners must be able to build a cost-effective security program while at the same time meet the requirements of government regulations. This book lays out

these regulations in simple terms and explains how to use the control frameworks to build an effective information security program and governance structure. It discusses how organizations can best ensure that the information is protected and examines all positions from the board of directors to the end user, delineating the role each plays in protecting the security of the organization.

CISA REVIEW QUESTIONS, ANSWERS AND EXPLANATIONS MANUAL, 12TH EDITION

COBIT 5: ENABLING INFORMATION

ISACA

ADVANCED PERSISTENT THREATS: HOW TO MANAGE THE RISK TO YOUR BUSINESS

Isaca

CRISC REVIEW MANUAL, 7TH EDITION

ENTERPRISE GOVERNANCE OF INFORMATION TECHNOLOGY

ACHIEVING STRATEGIC ALIGNMENT AND VALUE

Springer Enterprise governance of information technology is a relatively new concept that is gaining traction in both the academic and practitioner worlds. Going well beyond the implementation of a superior IT infrastructure, "Enterprise Governance of Information Technology" is about defining and embedding processes and structures throughout the organizations that enable both business and IT people to execute their responsibilities, while maximizing the value created from their IT-enabled investments. At the forefront of the field, the authors draw from years of research and advising corporate clients to present the first comprehensive resource on the topic. Featuring numerous case examples from companies around the world, the book integrates theoretical advances and empirical data with practical application, including in-depth discussion of such frameworks as COBIT and VALIT, which are used to measure and audit the value of IT investments and ensuring regulatory compliance. A variety of elements, including executive summaries and sidebars, extensive references, and questions and activities (with additional materials available on-line) ensure that the book will be an essential resource for professionals, researchers, and students alike.

CISA REVIEW MANUAL, 27TH EDITION

COBIT 2019 FRAMEWORK

GOVERNANCE AND MANAGEMENT OBJECTIVES

CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA) CERT GUIDE

Pearson IT Certification This is the eBook version of the print title. Note that the eBook may not provide access to the practice test software that accompanies the print book. Learn, prepare, and practice for CISA exam success with this Cert Guide from Pearson IT Certification, a leader in IT certification learning. Master CISA exam topics Assess your knowledge with chapter-ending quizzes Review key concepts with exam preparation tasks Certified Information Systems Auditor (CISA) Cert Guide is a best-of-breed exam study guide. World-renowned enterprise IT security leaders Michael Gregg and Rob Johnson share preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. The book presents you with an organized test preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your final study plan. Well-regarded for its level of detail, assessment features, and challenging review questions and exercises, this study guide helps you master the concepts and techniques that will allow you to succeed on the exam the first time. The study guide helps you master all the topics on the CISA exam, including: Essential information systems audit techniques, skills, and standards IT governance, management/control frameworks, and process optimization Maintaining critical services: business continuity and disaster recovery Acquiring information systems: build-or-buy, project management, and development methodologies Auditing and understanding system controls System maintenance and service management, including frameworks and networking infrastructure Asset protection via layered administrative, physical, and technical controls Insider and outsider asset threats: response and management

ENGLISH

CISM REVIEW QUESTIONS, ANSWERS AND EXPLANATIONS 9TH EDITION

IT CONTROL OBJECTIVES FOR SARBANES-OXLEY

THE ROLE OF IT IN THE DESIGN AND IMPLEMENTATION OF INTERNAL CONTROL OVER FINANCIAL REPORTING

ISACA

PRAGMATIC SECURITY METRICS

APPLYING METAMETRICS TO INFORMATION SECURITY

CRC Press Other books on information security metrics discuss number theory and statistics in academic terms. Light on mathematics and heavy on utility, PRAGMATIC Security Metrics: Applying Metametrics to Information Security breaks the mold. This is the ultimate how-to-do-it guide for security metrics. Packed with time-saving tips, the book offers easy-to-follow guidance for those struggling with security metrics. Step by step, it clearly explains how to specify, develop, use, and maintain an information security measurement system (a comprehensive suite of metrics) to help: Security professionals systematically improve information security, demonstrate the value they are adding, and gain management support for the things that need to be done Management address previously unsolvable problems rationally, making critical decisions such as resource allocation and prioritization of security relative to other business activities Stakeholders, both within and outside the organization, be assured that information security is being competently managed The PRAGMATIC approach lets you hone in on your problem areas and identify the few metrics that will generate real business value. The book: Helps you figure out exactly what needs to be measured, how to measure it, and most importantly, why it needs to be measured Scores and ranks more than 150 candidate security metrics to demonstrate the value of the PRAGMATIC method Highlights security metrics that are widely used and recommended, yet turn out to be rather poor in practice Describes innovative and flexible measurement approaches such as capability maturity metrics with continuous scales Explains how to minimize both measurement and security risks using complementary metrics for greater assurance in critical areas such as governance and compliance In addition to its obvious utility in the information security realm, the PRAGMATIC approach, introduced for the first time in this book, has broader application across diverse fields of management including finance, human resources, engineering, and production—in fact any area that suffers a surplus of data but a deficit of useful information. Visit Security Metametrics. Security Metametrics supports the global community of professionals adopting the innovative techniques laid out in PRAGMATIC Security Metrics. If you, too, are struggling to make much sense of security metrics, or searching for better metrics to manage and improve information security, Security Metametrics is the place. <http://securitymetametrics.com/>

THE BUSINESS MODEL FOR INFORMATION SECURITY

ISACA

COBIT 5

A BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT.

ISACA

COBIT 5 FOR RISK

ISACA Information is a key resource for all enterprises. From the time information is created to the moment it is destroyed, technology plays a significant role in containing, distributing and analysing information. Technology is increasingly advanced and has become pervasive in enterprises and the social, public and business environments.

THE CYBER RISK HANDBOOK

CREATING AND MEASURING EFFECTIVE CYBERSECURITY CAPABILITIES

John Wiley & Sons 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-versa. Every functional head of any organization must have a copy at-hand to understand their role in achieving that alignment.

ENTERPRISE GOVERNANCE OF INFORMATION TECHNOLOGY

ACHIEVING ALIGNMENT AND VALUE, FEATURING COBIT 5

Springer Featuring numerous case examples from companies around the world, this second edition integrates theoretical advances and empirical data with practical applications, including in-depth discussion on the COBIT 5 framework which can be used to build, measure and audit enterprise governance of IT approaches. At the forefront of the field, the authors of this volume draw from years of research and advising corporate clients to present a comprehensive resource on enterprise governance of IT (EGIT). Information technology (IT) has become a crucial enabler in the support, sustainability and growth of enterprises. Given this pervasive role of IT, a specific focus on EGIT has arisen over the last two decades, as an integral part of corporate governance. Going well beyond the implementation of a superior IT infrastructure, enterprise governance of IT is about defining and embedding processes and structures throughout the organization that enable boards and business and IT people to execute their responsibilities in support of business/IT alignment and value creation from their IT-enabled investments. Featuring a variety of elements, including executive summaries and sidebars, extensive references and questions and activities (with additional materials available on-line), this book will be an essential resource for professionals, researchers and students alike

COBIT 2019 FRAMEWORK

INTRODUCTION AND METHODOLOGY

CYBERSECURITY PROGRAM DEVELOPMENT FOR BUSINESS

THE ESSENTIAL PLANNING GUIDE

John Wiley & Sons "This is the book executives have been waiting for. It is clear: With deep expertise but in nontechnical language, it describes what cybersecurity risks are and the decisions executives need to make to address them. It is crisp: Quick and to the point, it doesn't waste words and won't waste your time. It is candid: There is no sure cybersecurity defense, and Chris Moschovitis doesn't pretend there is; instead, he tells you how to understand your company's risk and make smart business decisions about what you can mitigate and what you cannot. It is also, in all likelihood, the only book ever written (or ever to be written) about cybersecurity defense that is fun to read." —Thomas A. Stewart, Executive Director, National Center for the Middle Market and Co-Author of *Woo, Wow, and Win: Service Design, Strategy, and the Art of Customer Delight* Get answers to all your cybersecurity questions In 2016, we reached a tipping point—a moment where the global and local implications of cybersecurity became undeniable. Despite the seriousness of the topic, the term "cybersecurity" still exasperates many people. They feel terrorized and overwhelmed. The majority of business people have very little understanding of cybersecurity, how to manage it, and what's really at risk. This essential guide, with its dozens of examples and case studies, breaks down every element of the development and management of a cybersecurity program for the executive. From understanding the need, to core risk management principles, to threats, tools, roles and responsibilities, this book walks the reader through each step of developing and implementing a cybersecurity program. Read cover-to-cover, it's a thorough overview, but it can also function as a useful reference book as individual questions and difficulties arise. Unlike other cybersecurity books, the text is not bogged down with industry jargon Speaks specifically to the executive who is not familiar with the development or implementation of cybersecurity programs Shows you how to make pragmatic, rational, and informed decisions for your organization Written by a top-flight technologist with decades of experience and a track record of success If you're a business manager or executive who needs to make sense of cybersecurity, this book demystifies it for you.