Coso In The Cyber Age Deloitte Canada

This book explores how digital transformation is reshaping the manner in which higher education sectors emerge, work, and evolve and how auditors should respond to this challenging and risky digital audit universe in transforming the higher education system. It serves to help professionals to understand the reality of performing the Chief Audit Executive (CAE) role in today's evolving business economy, specifically in the higher education sector. It compares and contrasts the stated IIA standards with the challenges and realities auditors may face and provides alternative scenarios to gaining a "seat at the table." This book also provides insight into critical lessons learned when executing the CAE role relevant for digitally transforming universities. The main purpose of this study is to rethink the audit culture in the digital era and reveal the key characteristics that are open for improvement so that digitally transforming universities can be audited according to the higher education standards with a digitally supported value-added audit approach. Based on this approach, the audit culture is reassessed considering the digital university conceptual framework and business model. There are two main points to consider for the digital university work environment: traceability and auditability. In this respect, policy recommendations are made for best practices to achieve value-added digital audits in transforming universities. The book has been written from both the reality and academic perspectives of two experienced authors. Sezer is a past CAE, CEO, and long-term senior internal auditor who has worked in the internal audit role for various listed companies, financial institutions, and government entities. Erman has extensive information technology and university accreditation knowledge in the global higher education sector. This brings a blend of value-added approaches to the readers and speaks to issues about understanding and dealing with audit culture and business evolution in digitally transforming organizations along with the requirements for upholding IIA standards. Geared toward the experienced or new CAE, University Auditing in the Digital Era: Challenges and Lessons for Higher Education Professionals and CAEs can be a tool for all auditors to understand some of the challenges, issues, and potential alternative solutions when executing the role of university auditing. In addition, it can be a valuable reference for university administrators and CIOs, as well as academics and all stakeholders related to the higher education sector.

Enterprise Risk Management in Europe advances understanding of ERM in Europe, providing a novel and unique set of perspectives on the ongoing dynamics between ERM and corporate processes. This is an essential guide for researchers, practitioners and policy makers both in and beyond European borders.

Project governance, investment governance, and risk governance precepts are woven together in Self-Service Data Analytics and Governance for Managers, equipping managers to structure the inevitable chaos that can result as end-users take matters into their own hands Motivated by the promise of control and efficiency benefits, the widespread adoption of data analytics tools has created a new fast-moving environment of digital transformation in the finance, accounting, and operations world, where entire functions spend their days processing in spreadsheets. With the decentralization of application development as users perform their own analysis on data sets and automate spreadsheet processing without the involvement of IT, governance must be revisited to maintain process control in the new environment. In this book, emergent technologies that have given rise to data analytics and which form the evolving backdrop for digital transformation are introduced and explained, and prominent data analytics tools and capabilities will be demonstrated based on real world scenarios. The authors will provide a much-needed process discovery methodology describing how to survey the processing landscape to identify opportunities to deploy these capabilities. Perhaps most importantly, the authors will digest the mature existing data governance, IT governance, and model governance frameworks, but demonstrate that they do not comprehensively cover the full suite of data analytics builds, leaving a considerable governance gap. This book is meant to fill the gap and provide the reader with a fit-for-purpose and actionable governance framework to protect the value created by analytics deployment at scale. Project governance, investment governance, and risk governance precepts will be woven together to equip managers to structure the inevitable chaos that can result as end-users take matters into their own hands.

Cybersecurity is vital for all businesses, regardless of sector. With constant threats and potential online dangers, businesses must remain aware of the current research and information available to them in order to protect themselves and their employees. Maintaining tight cybersecurity can be difficult for businesses as there are so many moving parts to contend with, but remaining vigilant and having protective measures and training in place is essential for a successful company. The Research Anthology on Business Aspects of Cybersecurity considers all emerging aspects of cybersecurity in the business sector including frameworks, models, best practices, and emerging areas of interest. This comprehensive reference source is split into three sections with the first discussing audits and risk assessments that businesses can conduct to ensure the security of their systems. The second section covers training and awareness initiatives for staff that promotes a security culture. The final section discusses software and systems that can be used to secure and manage cybersecurity threats. Covering topics such as audit models, security behavior, and insider threats, it is ideal for businesses, business professionals, managers, security analysts, IT specialists, executives, academicians, researchers, computer engineers, graduate students, and practitioners.

Teaching and Curriculum Innovations

Audit Committee Formation in the Aftermath of 2007-2009 Global Financial Crisis, Volume II

Functions and Sustainability

The Risk IT Framework

CISA Certified Information Systems Auditor All-in-One Exam Guide, Third Edition

This book presents the contributions from a workshop entitled "Electricity security in the cyber age: Managing the increasing dependence of the electricity infrastructure on ICT," which was organized in the Netherlands in May 2009.

BUILD YOUR CYBERSECURITY PROGRAM WITH THIS COMPLETELY UPDATED GUIDE Security practitioners now have a comprehensive blueprint to build their cybersecurity programs. Building an Effective Cybersecurity Program (2nd Edition) instructs security architects, security managers, and security engineers how to properly construct effective cybersecurity programs using contemporary architectures, frameworks, and models. This comprehensive book is the result of the author’s professional experience and involvement in designing and deploying hundreds of cybersecurity programs. The extensive content includes: Recommended design approaches, Program structure, Cybersecurity technologies, Governance Policies, Vulnerability, Threat and intelligence capabilities, Risk management, Defense-in-depth, DevSecOps, Service management, ...and much more! The book is presented as a practical roadmap detailing each step required for you to build your effective cybersecurity program. It also provides many design templates to assist in program builds and all chapters include self-study questions to gauge your progress. With this new 2nd edition of this handbook, you can move forward confidently, trusting that Schreider is recommending the best components of a cybersecurity program for you. In addition, the book provides hundreds of citations and references allow you to dig deeper as you explore specific topics relevant to your organization or your studies. Whether you are a new manager or current manager involved in your organization’s cybersecurity program, this book will answer many questions you have on what is involved in building a program. You will be able to get up to speed quickly on program development practices and have a roadmap to follow in building or improving your organization’s cybersecurity program. If you are new to cybersecurity in the short period of time it will take you to read this book, you can be the smartest person in the room grasping the complexities of your organization’s cybersecurity program. If you are a manager already involved in your organization’s cybersecurity program, you have much to gain from reading this book. This book will become your go to field manual guiding or affirming your program decisions.

Contributions from city of San Francisco, Director of Emergency Services; National Science Foundation, Research Applications, Directorate; State of California, Office of Emergency Services, Seismic Safety Commission; U.S. Department of the Interior, Assistant Secretary for Energy and Minerals, Geological Survey; University of California at Los Angeles, Department of Sociology.

??letmelerde bilgi güvenli?inin sa?lanmas? temelinde Bilgi Teknolojileri (IT Security) güvenli?i ile Siber Güvenlik (Cyber Security) konular? kavramsal, kaynaklar, tehditler ve etkili güvenlik konseptini içeren çerçevede 101 soruyu yan?tlayarak anlat?lmaktad?r.

Responsibilities and Sustainability

A Practical Guide to Overcoming Challenges in a Complex World

Building Effective Cybersecurity Programs

Self-Service Data Analytics and Governance for Managers

Corporate Governance

Monthly Catalogue, United States Public Documents

This book is a roadmap to help organizations adopt corporate responsibility and sustainability practices and be fit for purpose in a digital era. It explains why corporate responsibility is the only option in the twenty-first-century post-COVID-19 world, and guides readers through the process of transforming their organizations with continued reference to the importance of technology. This is not a technical manual, and it is not an academic textbook: it is designed to be a quick, easily digested read. The first part looks at the current landscape – both of business and of the world in which it operates. The second part explains why corporate responsibility is the only realistic option for business in the twenty-first-century, post-COVID, and who needs to take responsibility for it. The third part is a step-by-step guide to putting principles into practice, covering: values, stakeholder engagement, employees, supply chain, environment, community, customers and marketing, and reporting and transparency. Each chapter is linked to relevant UN Sustainable Development Goals and supported by dozens of real-world examples. By the end of the book, business leaders will have understood the scope of the challenge involved in leading a truly socially and environmentally responsible organization, and, crucially, will have understood why such a course of action is not only desirable but essential. And they will also have been inspired by a sense of purpose. The book offers direct access to the processes, insights, and techniques for installing corporate responsibility throughout organizations large and small, based on the author’s many years’ experience working in government and with successful large corporations. It is up-to-date and relevant, addressing the implications of COVID-19 and the modern technological “Fourth Industrial Revolution.”

Why purchase this book?-Prepares supply chain,quality, engineering, and operational excellence professionals for their emerging risk roles, responsibilities, and authorities.-Illustrates how supply chain risk-controls are architected, designed, deployed, and assured.-Explains why Risk Based Problem Solving(RBPS) and Risk Based Decision Making (RBDM) are the future of SCRM. Examples are offered throughout the book.-Illustrates how supply chain management is migrating to Supply Chain Risk Management (SCRM).-Demonstrates how SCRM objectives align with the organization's strategic objectives.-Describes how to move beyond a price relationship to a value-added relationship.-Integrates the disparate elements of SCRM into a competitive business system.-Describes how to select and develop suppliers based on risk criteria.-Demonstrates how to use ISO 31000 risk management framework of SCRM.Bonus materials/resources:-Access over 1,500 risk articles through CERM Academy (http://insights.cermacademy.com/).-Get free course materials such as using FMEA's in ISO 9001:2015.-Get slide decks with specific risk information on Youtube.-Get discount for Certified Enterprise Risk Management certificate.

One thing that will never change about the business world is the presence of risk. But risk management has changed dramatically since the 2008 financial crisis. . .and new developments in technology and communications demand up-to-the-minute approaches for defending against threats-and seizing opportunities. Extensively updated, the second edition of Fundamentals of Enterprise Risk Management examines the latest technologies such as Riskonnect and High Tech Electronic Platform (HTEP), and helps readers recognize both internal and external exposures, understand crucial concepts such as risk mapping and risk identification, and align risk opportunities with their organization's business model. Packed with practical exercises and fresh case studies from organizations such as IBM, Microsoft, Apple, JPMorgan Chase,and Sony-as well as new material on topics including the new role of Risk Owner, cutting-edge collaboration methods, and the upside of risk-this critical guide provides readers with the tools and information they need to keep their organizations as blissfully risk-free as possible.

This up-to-date self-study system offers 100% coverage of every topic on the 2016 version of the CISA exam The fully revised new edition delivers complete coverage of every topic on the latest release of the Certified Information Systems Auditor (CISA) exam. Written by an IT security and auditing expert, CISA Certified Information Systems Auditor All-in-One Exam Guide, Third Edition, covers all five exam domains developed by the Information Systems Audit and Control Association (ISACA). This effective self-study system features learning objectives at the beginning of each chapter, in-depth explanations of each topic, and accurate practice questions. Each chapter includes Exam Tips that highlight key exam information, hands-on exercises, a chapter summary that serves as a quick review, and end-of-chapter questions that simulate those on the actual exam. Designed to help you pass the CISA exam with ease, this trusted guide also serves as an ideal on-the-job reference. The latest edition of this trusted resource offers complete, up-to-date coverage of all the material included on the latest release of the Certified Information Systems Auditor exam. Written by an IT security and audit expert, CISA Certified Information Systems Auditor All-in-One Exam Guide, Third Edition covers all five exam domains developed by ISACA®. You’ll find learning objectives at the beginning of each chapter, exam tips, practice exam questions, and in-depth explanations. Designed to help you pass the CISA exam with ease, this comprehensive guide also serves as an essential on-the-job reference for new and established IS auditors. COVERS ALL EXAM TOPICS, INCLUDING: • IT governance and management • Information systems audit process • Information systems life-cycle management • IT service delivery and infrastructure • Information asset protection Electronic content includes: • 400 practice exam questions in the Total Tester exam engine--take full-length practice exams or customizable quizzes by exam topic (Windows only)

Managing the Psychology That Drives Decisions and Influences Operational Risk

Securing Electricity Supply in the Cyber Age

An Interdisciplinary Introduction

A Security Manager’s Handbook

Enterprise Risk Management in Europe

COBIT 5

Keep abreast of the fast-paced changes in accounting and auditing with relevant pronouncements, exposure drafts, and other guidance recently issued in the accounting, auditing, compilation, preparation, and review arenas. This book will help accountants and financial managers sort through the most recent accounting and auditing complexities so they can identify and apply recently issued FASB, PCAOB, and AICPA standards and guidance. New topics covered include: Revenue recognition Leases Financial instruments Intangible assets Consolidation Business combinations Recently issued SAS No. 134–140 Auditing interpretations Recently proposed SSAE standards Overview of SSARS guidance

Although one finds much discussion and research on the features and functionality of Rich Internet Applications (RIAs), the 3D Web, Immersive Environments (e.g. MMORPGs) and Virtual Worlds in both scholarly and popular publications, very little is written about the issues and techniques one must consider when creating, deploying, interacting within, and managing them securely. Security in Virtual Worlds, 3D Webs, and Immersive Environments: Models for Development, Interaction, and Management brings together the issues that managers, practitioners, and researchers must consider when planning, implementing, working within, and managing these promising virtual technologies for secure processes and initiatives. This publication discusses the uses and potential of these virtual technologies and examines secure policy formation and practices that can be applied specifically to each.

Corporate governance has evolved as a central issue for public companies in the aftermath of the 2007–2009 global financial crisis. Corporate governance is a process (journey) of managing corporate affairs to create shareholder value and protect interests of other stakeholders. This book presents a road map for various functions and measures of corporate governance. The participants in the corporate governance process are the board of directors, executives, stakeholders, internal and external auditors, financial analysts, legal counsel, and regulators. This book is organized into four separate volumes; each volume can be utilized separately or in an integrated form. The first volume consists of five chapters that address the relevance and importance of corporate governance as well as the framework and structure of corporate governance. The second volume consists of four chapters that present the three prevailing corporate governance functions of oversight, management, and monitoring. The third volume consists of four chapters that address corporate governance functions performed by corporate gatekeepers, including policy makers, regulators, standard-setters, internal auditors, external auditors, legal counsel, and financial advisors. The fourth volume consists of five chapters that address the emerging issues in corporate governance, including governance for private companies and nonprofit organizations and convergence in global corporate governance.

A Série Universitária foi desenvolvida pelo Senac São Paulo com o intuito de preparar profissionais para o mercado de trabalho. Os títulos abrangem diversas áreas, abordando desde conhecimentos teóricos e práticos adequados às exigências profissionais até a formação ética e sólida. Normas e práticas de contabilidade do setor público vem trazer mais luz ao processo de gestão pública e visa a auxiliar os atuais gestores e os pretendentes a participar da administração pública, por meio da aprovação em concursos. O livro aborda diferentes aspectos e especificidades da contabilidade pública, desde a normatização contábil até as práticas de transparência e governança. Também são discutidos e detalhados os procedimentos contábeis patrimoniais e específicos, as modalidades de licitações (incluindo a migração da tradicional Lei no 8.666 para a legislação aprovada em 2021), as normas e padronizações, a auditoria e controladoria e a função dos tribunais de contas. Por fim, a obra trata ainda da metodologia Coso, do balanço social e da Lei de Responsabilidade Fiscal.

Encyclopedia of Organizational Knowledge, Administration, and Technology

Completing In the Age of Disruption

IT Security Governance Innovations: Theory and Research

Achieving Organizational Agility, Intelligence, and Resilience Through Information Systems

Monthly Catalog of United States Government Publications

Corporate Governance 5ed

Are your accounting and auditing skills up-to-date and on-par with industry standards? This guide provides updates on the latest standards, including accounting, auditing, compilation, preparation, and review. It covers important industry changes such as revenue recognition, leases, financial instruments, and SASs, and includes practical applications for each, to help you understand and apply the standards to real-life scenarios. Key topics covered include: Accounting, auditing, and attestation standards updates FASB projects and exposure drafts Private company financial reporting Revenue Recognition Leases, Financial Instruments, Peer Review, Trust Services, Cyber Security, SSAEs Going Concern; Private company financial reporting

Why Purchase this Book? · Prepares supply chain, quality, engineering, and operational excellence professionals for their emerging risk roles, responsibilities, and authorities. · Illustrates how supply chain risk-controls are architected, designed, deployed, and assured. · Explains why Risk Based Problem Solving (RBPS) and Risk Based Decision Making (RBDM) are the future of SCRM. Examples are offered throughout the book. · Illustrates how supply chain management is migrating to Supply Chain Risk Management (SCRM). · Demonstrates how SCRM objectives align with the organization’s strategic objectives. · Describes how to move beyond a price relationship to a value-added relationship. · Integrates the disparate elements of SCRM into a competitive business system. · Describes how to select and develop suppliers based on risk criteria. · Demonstrates how to use ISO 31000 risk management framework of SCRM. Bonus Materials/Resources: · Access over 1,500 risk articles through CERM Academy (http://insights.cermacademy. com/). · Get free course materials such as using FMEA’s in ISO 9001:2015. · Get slide decks with specific risk information on YouTube. · Get discount for Certified Enterprise Risk Manager® certificate.

Information technology in the workplace is vital to the management of workflow in the company; therefore, IT security is no longer considered a technical issue but a necessity of an entire corporation. The practice of IT security has rapidly expanded to an aspect of Corporate Governance so that the understanding of the risks and prospects of IT security are being properly managed at an executive level. IT Security Governance Innovations: Theory and Research provides extraordinary research which highlights the main contributions and characteristics of existing approaches, standards, best practices, and new trends in IT Security Governance. With theoretical and practical perspectives, the book aims to address IT Security Governance implementation in corporate organizations. This collection of works serves as a reference for CEOs and CIOs, security managers, systems specialists, computer science students, and much more.

As technology continues to be a ubiquitous force that propels businesses to success, it is imperative that updated studies are continuously undertaken to ensure that the most efficient tools and techniques are being utilized. In the current business environment, organizations that can improve their agility and business intelligence are able to become much more resilient and viable competitors in the global economy. Achieving Organizational Agility, Intelligence, and Resilience Through Information Systems is a critical reference book that provides the latest empirical studies, conceptual research, and methodologies that enable organizations to enhance and improve their agility, competitiveness, and sustainability in order to position them for paramount success in today’s economy. Covering topics that include knowledge management, human development, and sustainable development, this book is ideal for managers, executives, entrepreneurs, IT specialists and consultants, academicians, researchers, and students.

Building an Effective Cybersecurity Program, 2nd Edition

The Handbook of Student Affairs Administration

Security in Virtual Worlds, 3D Webs, and Immersive Environments: Models for Development, Interaction, and Management

University Auditing in the Digital Era

Earthquake Prediction, Opportunity to Avert Disaster

Research Anthology on Business Aspects of Cybersecurity

BUILD YOUR CYBERSECURITY PROGRAM WITH THIS COMPLETELY UPDATED GUIDE Security practitioners now have a comprehensive blueprint to build their cybersecurity programs. Building an Effective Cybersecurity Program (2nd Edition) instructs security architects, security managers, and security engineers how to properly construct effective cybersecurity programs using contemporary architectures, frameworks, and models. This comprehensive book is the result of the author ’ s professional experience and involvement in designing and deploying hundreds of cybersecurity programs. The extensive content includes: Recommended design approaches, Program structure, Cybersecurity technologies, Governance Policies, Vulnerability, Threat and intelligence capabilities, Risk management, Defense-in-depth, DevSecOps, Service management, ···and much more! The book is presented as a practical roadmap detailing each step required for you to build your effective cybersecurity program. It also provides many design templates to assist in program builds and all chapters include self-study questions to gauge your progress.

With this new 2nd edition of this handbook, you can move forward confidently, trusting that Schreider is recommending the best components of a cybersecurity program for you. In addition, the book provides hundreds of citations and references allow you to dig deeper as you explore specific topics relevant to your organization or your studies. Whether you are a new manager or current manager involved in your organization ’ s cybersecurity program, this book will answer many questions you have on what is involved in building a program. You will be able to get up to speed quickly on program development practices and have a roadmap to follow in building or improving your organization ’ s cybersecurity program. If you are new to cybersecurity in the short period of time it will take you to read this book, you can be the smartest person in the room grasping the complexities of your organization ’ s cybersecurity program. If you are a manager already involved in your organization ’ s cybersecurity program, you have much to gain from reading this book. This book will become your go to field manual guiding or affirming your program decisions.

The psychological dimension of managing risk is of crucial importance, and its study has led to the identification of specific do's and don'ts. Those with an understanding of the psychology underlying risk and the skills to recognize its manifestation in practice, have the opportunity to develop frameworks that embody the do's and don'ts, thereby producing sound judgments and good decisions. Those lacking the understanding and the skills are destined to be more hit and miss in their approach to risk management, doing the don'ts and not doing the do's. Virtually every major risk management catastrophe in the last fifteen years has psychological pitfalls at its root. The list of catastrophes includes the 2008 bankruptcy of Lehman Brothers and subsequent global financial crisis, the 2010 explosion at BP's Macondo well in the Gulf of Mexico and the 2011 nuclear meltdown at the Fukushima Daiichi power plant. A critical lesson from psychological studies for those involved in risk management is that people's judgments and decisions about risk vary with type of circumstance. In Behavioral Risk Management readers will learn that there are specific actions that organizations can undertake to incorporate understanding, recognition, and behavioral interventions into the practice of risk management. There are many examples throughout the book that illustrate doing the don'ts. The chapters in the first part of the book introduce the main ideas, and the chapters in the latter part provide insight into how to apply those ideas to the practical world in which risk managers operate.

The Wiley CPAexcel Study Guide: Business Environment and Concepts arms CPA test-takers with detailed text and skill-building problems to help identify, focus on, and master the specific topics that may need additional reinforcement to pass the BEC section of the CPA Exam. This essential study guide: Covers the complete AICPA content blueprint in BEC Explains every topic tested with 662 pages of study text, 599 multiple-choice questions, and 6 task-based simulations in BEC Organized in Bite-Sized Lesson format with 149 lessons in BEC Maps perfectly to the Wiley CPAexcel online course; may be used to complement the course or as a stand-alone study tool

Computer and Information Security Handbook, Third Edition, provides the most current and complete reference on computer security available in one volume. The book offers deep coverage of an extremely wide range of issues in computer and cybersecurity theory, applications, and best practices, offering the latest insights into established and emerging technologies and advancements. With new parts devoted to such current topics as Cloud Security, Cyber-Physical Security, and Critical Infrastructure Security, the book now has 100 chapters written by leading experts in their fields, as well as 12 updated appendices and an expanded glossary. It continues its successful format of offering problem-solving techniques that use real-life case studies, checklists, hands-on exercises, question and answers, and summaries. Chapters new to this edition include such timely topics as Cyber Warfare, Endpoint Security, Ethical Hacking, Internet of Things Security, Nanoscale Networking and Communications Security, Social Engineering, System Forensics, Wireless Sensor Network Security, Verifying User and Host Identity, Detecting System Intrusions, Insider Threats, Security Certification and Standards Implementation, Metadata Forensics, Hard Drive Imaging, Context-Aware Multi-Factor Authentication, Cloud Security, Protecting Virtual Infrastructure, Penetration Testing, and much more. Written by leaders in the field Comprehensive and up-to-date coverage of the latest security technologies, issues, and best practices Presents methods for analysis, along with problem-solving techniques for implementing practical solutions

Computer and Information Security Handbook

Exploring the Risks of Information and Communication Technology in Tomorrow's Electricity Infrastructure

Annual Update for Accountants and Auditors: 2020

Managing Country Risk in an Age of Globalization

A Practitioner ’ s Roadmap for Corporate Responsibility in the Digital Age

Business Environment and Concepts

This volume of Advances in Accounting Education consists of three themes: (1) Capacity Building and Program Leadership, (2) Classroom Innovation and Pedagogy, and (3) Engagement with Professionals Through Advisory Councils.

For any organization to be successful, it must operate in such a manner that knowledge and information, human resources, and technology are continually taken into consideration and managed effectively. Business concepts are always present regardless of the field or industry – in education, government, healthcare, not-for-profit, engineering, hospitality/tourism, among others. Maintaining organizational awareness and a strategic frame of mind is critical to meeting goals, gaining competitive advantage, and ultimately ensuring sustainability. The Encyclopedia of Organizational Knowledge, Administration, and Technology is an inaugural five-volume publication that offers 193 completely new and previously unpublished articles authored by leading experts on the latest concepts, issues, challenges, innovations, and opportunities covering all aspects of modern organizations. Moreover, it is comprised of content that highlights major breakthroughs, discoveries, and authoritative research results as they pertain to all aspects of organizational growth and development including methodologies that can help companies thrive and analytical tools that assess an organization’s internal health and performance. Insights are offered in key topics such as organizational structure, strategic leadership, information technology management, and business analytics, among others. The knowledge compiled in this publication is designed for entrepreneurs, managers, executives, investors, economic analysts, computer engineers, software programmers, human resource departments, and other industry professionals seeking to understand the latest tools to emerge from this field and who are looking to incorporate them in their practice. Additionally, academicians, researchers, and students in fields that include but are not limited to business, management science, organizational development, entrepreneurship, sociology, corporate psychology, computer science, and information technology will benefit from the research compiled within this publication.

This book analyses and discusses current issues and trends in finance with a special focus on technological developments and innovations. The book presents an overview of the classical and traditional approaches of financial management in companies and discusses its key strategic role in corporate performance. Furthermore, the volume illustrates how the emerging technological innovations will shape the theory and practice of financial management, focusing especially on the decentralized financial ecosystems that blockchain and its related technologies allow.

"Drawing upon a wealth of experience from academia, industry, and government service, this book details and dissects current organizational cybersecurity policy issues on a global scale. Using simple language, it includes a thorough description of each issue, lists pros and cons, documents policy alternatives for the sake of clarity with respect to policy alone, and dives into organizational implementation issues. It also equips the reader with descriptions of the impact of specific policy choices, both positive and negative. This book gives students, scholars, and technical decision-makers the necessary knowledge of cybersecurity policy in order to make more informed decisions"--Provided by publisher.

Fundamentals of Enterprise Risk Management

Annual Accounting and Auditing Workshop

Supply Chain Risk Management

Behavioral Risk Management

Cyber Security Policy Guidebook

Advances in Accounting Education

Corporate Governance (Fourth Edition) continues to inform on all aspects of corporate governance, while keeping readers up to date with the latest developments. It is now established as the leading South African work on the subject. The past five years since publication of the third edition has seen a number of changes in the application of corporate governance in South Africa and beyond. Locally, we have seen the application of the 2008 Companies Act, and in the United Kingdom, a new Corporate Governance Code has been introduced. Significant developments have taken place in the area of corporate reporting, via the appearance of an International Integrated Reporting Framework, widening the scope of the traditional annual report. The Fourth Edition deals with these changes. Key additions are chapters on types of entities, and a comparison of local and international practice. Corporate Governance was first published in 2002 shortly after the publication of the original King Report, to help explain the need for corporate governance in the private and public sectors and to provide South African executives and professionals with a practical framework to establish governance systems and practices in their own organisations.

You know by now that your company could not survive without the Internet. Not in today’s market. You are either part of the digital economy or reliant upon it. With critical information assets at risk, your company requires a state-of-the-art cybersecurity program. But how do you achieve the best possible program? Tari Schreider, in Building Effective Cybersecurity Programs: A Security Manager’s Handbook, lays out the step-by-step roadmap to follow as you build or enhance your cybersecurity program. Over 30+ years, Tari Schreider has designed and implemented cybersecurity programs throughout the world, helping hundreds of companies like yours. Building on that experience, he has created a clear roadmap that will allow the process to go more smoothly for you. Building Effective Cybersecurity Programs: A Security Manager’s Handbook is organized around the six main steps on the roadmap that will put your cybersecurity program in place: Design a Cybersecurity Program Establish a Foundation of Governance Build a Threat, Vulnerability Detection, and Intelligence Capability Build a Cyber Risk Management Capability Implement a Defense-in-Depth Strategy Apply Service Management to Cybersecurity Programs Because Schreider has researched and analyzed over 150 cybersecurity architectures, frameworks, and models, he has saved you hundreds of hours of research. He sets you up for success by talking to you directly as a friend and colleague, using practical examples. His book helps you to: Identify the proper cybersecurity program roles and responsibilities. Classify assets and identify vulnerabilities. Define an effective cybersecurity governance foundation. Evaluate the top governance frameworks and models. Automate your governance program to make it more effective. Integrate security into your application development process. Apply defense-in-depth as a multi-dimensional strategy. Implement a service management approach to implementing countermeasures. With this handbook, you can move forward confidently, trusting that Schreider is recommending the best components of a cybersecurity program for you. In addition, the book provides hundreds of citations and references allow you to dig deeper as you explore specific topics relevant to your organization or your studies.

Building an Effective Cybersecurity Program, 2nd EditionRothstein Publishing

What does Corporate Governance mean in the post Steinhoff-collapse era in South Africa? It has become more important than ever, and this established work by top directors from accounting and legal backgrounds is an essential handbook for all Company Directors, their advisers, and those who have aspirations to be business leaders.A new & significantly expanded edition of this leading reference on Corporate Governance in South Africa, this book incorporates a new and comprehensive Summary of the King IV code, as well updated examples and current thinking on an increasingly important sphere.

Global Approaches and New Opportunities

Financial Ecosystem and Strategy in the Digital Era

Models for Development, Interaction, and Management

Wiley CPAexcel Exam Review April 2017 Study Guide

Corporate Responsibility in the Digital Age

How Top Companies Assess Risk, Manage Exposure, and Seize Opportunity

Cybersecurity Foundations provides all of the information readers need to become contributing members of the cybersecurity community. The book provides critical knowledge in the six disciplines of cybersecurity: (1) Risk Management; (2) Law and Policy; (3) Management Theory and Practice; (4) Computer Science Fundamentals and Operations; (5) Private Sector Applications of Cybersecurity; (6) Cybersecurity Theory and Research Methods. Cybesecurity Foundations was written by cybersecurity professionals with decades of combined experience working in both the public and private sectors.

Datenschutz stellt eine große Herausforderung für privatwirtschaftliche Unternehmen dar. Elektronische Datenbestände müssen laut der EU-Datenschutz-Grundverordnung (DSGVO), die nach einer zweijährigen Übergangsfrist im Mai 2018 verbindlich wird, die Sicherheit vor unbefugtem Zugriff und vor allem Transparenz im internen Umgang der Daten sicherstellen. Mit der Einrichtung von Compliance-Systemen, die für die Einhaltung von rechtlichen Rahmenbedingungen sorgen sollen, haben Unternehmen bereits ein potenzielles Instrumentarium, um auch Datenschutzbelange abzusichern. Das vorliegende Buch bietet einen Überblick über die Entwicklung, Grundsätze und Öffnungsklauseln der EU-DSGVO. Weiterhin werden diverse Compliance-Management-Systeme und Control-Frameworks für die IT-Compliance bzw. IT-Sicherheit angeführt, um darauf aufbauend die Perspektive auf die Herausforderungen des in der DSGVO neu geregelten Datenschutzes zu lenken.

This book provides an up-to-date guide to managing Country Risk. It tackles its various and interlinked dimensions including sovereign risk, socio-political risk, and macroeconomic risk for foreign investors, creditors, and domestic residents. It shows how they are accentuated in the global economy together with new risks such as terrorism, systemic risk, environmental risk, and the rising trend of global volatility and contagion. The book also assesses the limited usefulness of traditional yardsticks of Country Risk, such as ratings and rankings, which at best reflect the market consensus without predictive value and at worst amplify risk aversion and generate crisis contamination. This book goes further than comparing a wide range of risk management methods in that it provides operational and forward-looking warning signs of Country Risk. The combination of the authors ’ academic and market-based backgrounds makes the book a useful tool for scholars, analysts, and practitioners.

The audit committee has gained considerable attention in the aftermath of 2007-2009 global financial crisis. The audit committee ’ s role has evolved from a voluntary liaison between management and external auditors to the standing committee of the board of directors in overseeing all aspects of corporate governance, financial reporting, internal controls, risk assessment, and audit activities. This book addresses the determinants of audit committee oversight effectiveness, including their composition, independence, authority, resources, diligence, and activities. The book is organized into three separate volumes and each volume can be utilized separately or in an integrated form. The first volume consists of five chapters, which examine the relevance and fundamentals of the audit committees as well as the determinants of audit committee effectiveness. The second volume consists of nine chapters on financial, auditing, internal control, risk management, ethics and compliance, antifraud, and other oversight functions of the audit committee. The third volume consists of five chapters on the emerging issues of audit committees pertaining to evaluation, education, reporting, and accountability as well as audit committees of private companies, governmental entities and not-for-profit organizations.

(Sponsored by NASPA, Student Affairs Administrators in Higher Education)

Normas e práticas de contabilidade do setor público

Competing in the Age of Disruption

EU-DSGVO und Compliance. Rechtliche und wirtschaftliche Herausforderungen

Challenges and Lessons for Higher Education Professionals and CAEs

Corporate Governance in the Aftermath of the Global Financial Crisis, Volume II