Electronic Commerce Security Risk Management And Control

With the increasing reliance on digital means to transact goods that are retail and communication based, e-services continue to develop as key applications for business, finance, industry and innovation.Electronic Services: Concepts, Methodologies, Tools and Applications is an all-inclusive research collection covering the latest studies on the consumption, delivery and availability of e-services. This multi-volume book contains over 100 articles, making it an essential reference for the evolving e-services discipline.

Electronic Commerce Management for Business Activities and Global Enterprises: Competitive Advantages is written as an e-commerce textbook for undergraduate and graduate students in various business programs, including information systems, marketing, computer science, and MBA. In addition to serving as a textbook in e-commerce, this book also provides an excellent repository for instructors, researchers, and industry practitioners for their research ideas, theories, and practical experiences. In addition to regular topics traditionally taught in the classroom, this textbook addresses the many new emerging ideas and applications and presents tools and techniques in all aspects of e-commerce development and management in the global economy.

Interoperability is a topic of considerable interest for business entities, as the exchange and use of data is important to their success and sustainability. Electronic Business Interoperability: Concepts, Opportunities and Challenges analyzes obstacles, provides critical assessment of existing approaches, and reviews recent research efforts to overcome interoperability problems in electronic business. It serves as a source of knowledge for researchers, educators, students, and industry practitioners to share and exchange their most current research findings, ideas, practices, challenges, and opportunities concerning electronic business interoperability.

As the Internet becomes increasingly interconnected with modern society, the transition to online business has developed into a prevalent form of commerce. While there exist various advantages and disadvantages to online business, it plays a major role in contemporary business methods. Improving E-Commerce Web Applications Through Business Intelligence Techniques provides emerging research on the core areas of e-commerce web applications. While highlighting the use of data mining, search engine optimization, and online marketing to advance online business, readers will learn how the role of online commerce is becoming more prevalent in modern business. This book is an important resource for vendors, website developers, online customers, and scholars seeking current research on the development and use of e-commerce.

Towards the Knowledge Society is a state-of-the-art book covering innovative trends in the design, implementation and dissemination of eCommerce, eBusiness, and eGovernment. The book contains recent results of research and development in the areas of: - eGoverment; | - eMarkets; - eLearning; - eBusiness (B2B and B2C); - Trust, Security and Fraud; - Public Services and Health; - Design of I.S., Web and Technology Systems; - Applications and Procedures for eCommerce/eBusiness. Towards the Knowledge Society comprises the proceedings of I3E 2002, the Second International Conference on eCommerce, eBusiness, eGovernment, which was sponsored by the International Federation for Information Processing (IFIP) and held in Lisbon, Portugal in October 2002.

The new edition of a bestseller, Information Technology Control and Audit, Fourth Edition provides a comprehensive and up-to-date overview of IT governance, controls, auditing applications, systems development, and operations. Aligned to and supporting the Control Objectives for Information and Related Technology (COBIT), it examines emerging trend

"This encyclopedia offers a comprehensive knowledge of multimedia information technology from an economic and technological perspective"--Provided by publisher.

The Web is an exciting but unstable place to do business. The potential rewards are high but so are the risks, and the effective management of these risks 'online' is likely to be the greatest business enabler or destroyer of the next decade. Information security is no longer an issue confined to the IT department - it is critical to all operational functions and departments within an organization. Nor are the solutions purely technical, with two-thirds of security breaches caused by human error, management controls and processes. Risk to the integrity, availability and confidentiality of e-business activities comes in many forms - fraud, espionage, viruses, spamming, denial of service - and the potential for damage or irretrievable loss is very real. The Secure Online Business Handbook is designed as a practical guide for managers in developing and implementing appropriate strategies for online risk management. The contributions in this fully revised and updated new edition draw on a wide range of expertise and know-how, both in IT and in other disciplines such as the law, insurance, accounting and consulting. Security should not be an afterthought in developing a strategy, but an integral part of setting up sustainable new channels of communication and business.

An in-depth look at the pressing issues involved in protecting an e-business from external threats while safeguarding customer privacy With billions of dollars at stake in e-commerce, companies are becoming much more concerned about security and privacy issues. Hackers have made headlines by breaking into Web sites that aggregate sensitive information about all of us, which has caused growing public concern about personal and financial privacy. Some online businesses are inadvertently "sharing" data with others when they interoperate systems. This book examines the external threats to a company's system and explains how to react if your system and business goals diverge. It also presents a nuts-and-bolts guide to enhancing security and safeguarding gateways. Readers will find an extensive reference section for the many tools, standards, and watchdog agencies that aid in the security/privacy effort.

Managing (e)Business Transformation comprises text and cases designed to show students how a business can be transformed into an internetworked enterprise where IT infrastructures are used to link customers, suppliers, partners and employees to create superior economic value. The book is written based on the premise that integrating internet technologies throughout the value chain is crucial to building and managing customer relationships. Importantly, it underscores the centrality of basic business and economic principles within the context of a networked environment. The book builds on established business and economic theories, concepts and fundamentals to show that 'e-business' will soon be synonymous with 'business'. The book takes a strong managerial perspective, especially popular with MBA students, to argue that the internet is simply an enabling technology, which allows firms to build the infrastructure needed to operate in an evolving business world. The application of theory/concepts is emphasized throughout and contains a range of international case studies enhance the learning experience. This book is a must for all students studying e-

business strategy at undergraduate, MBA and postgraduate level. Also available is a companion website with extra features to accompany the text, please take a look by clicking below - http://www.palgrave.com/business/farhoomand/index.asp

This book is essentially for students pursuing MBA programs. It will also be very useful for the other specialized courses like diploma in electronic commerce or information technology etc. The following features make this book an indispensable text.

This book provides information on trust and risk to businesses that are developing electronic commerce systems and helps consumers understand the risks in using the Internet for purchases and show them how to protect themselves.

Security problems have evolved in the corporate world because of technological changes, such as using the Internet as a means of communication. With this, the creation, transmission, and storage of information may represent security problem. Metrics and Methods for Security Risk Management is of interest, especially since the 9/11 terror attacks, because it addresses the ways to manage risk security in the corporate world. The book aims to provide information about the fundamentals of security risks and the corresponding components, an analytical approach to risk assessments and mitigation, and quantitative methods to assess the risk components. In addition, it also discusses the physical models, principles, and quantitative methods needed to assess the risk components. The by-products of the methodology used include security standards, audits, risk metrics, and program frameworks. Security professionals, as well as scientists and engineers who are working on technical issues related to security problems will find this book relevant and useful. Offers an integrated approach to assessing security risk Addresses homeland security as well as IT and physical security issues Describes vital safeguards for ensuring true business continuity

This book expands the scope of risk management beyond insurance and finance to include accounting risk, terrorism, and other issues that can threaten an organization. It approaches risk management from five perspectives: in addition to the core perspective of financial risk management, it addresses perspectives of accounting, supply chains, information systems, and disaster management. It also covers balanced scorecards, multiple criteria analysis, simulation, data envelopment analysis, and financial risk measures that help assess risk, thereby enabling a well-informed managerial decision making. The book concludes by looking at four case studies, which cover a wide range of topics. These include such practical issues as the development and implementation of a sound risk management structure; supply chain risk and enterprise resource planning systems in information systems, and disaster management.

Enhances libraries worldwide through top research compilations from over 250 international authors in the field of e-business.

A framework for formalizing risk management thinking intoday¿s complex business environment Security Risk Management Body of Knowledge details thesecurity risk management process in a format that can easily beapplied by executive managers and security risk managementpractitioners. Integrating knowledge, competencies, methodologies,and applications, it demonstrates how to document and incorporatebest-practice concepts from a range of complementarydisciplines. Developed to align with International Standards for RiskManagement such as ISO 31000 it enables professionals to applysecurity risk management (SRM) principles to specific areas ofpractice. Guidelines are provided for: Access Management; BusinessContinuity and Resilience; Command, Control, and Communications;Consequence Management and Business Continuity Management;Counter-Terrorism; Crime Prevention through Environmental Design;Crisis Management; Environmental Security; Events and MassGatherings; Executive Protection; Explosives and Bomb Threats;Home-Based Work; Human Rights and Security; Implementing SecurityRisk Management; Intellectual Property Protection; IntelligenceApproach to SRM; Investigations and Root Cause Analysis; MaritimeSecurity and Piracy; Mass Transport Security; OrganizationalStructure; Pandemics; Personal Protective Practices; Psych-ology ofSecurity; Red Teaming and Scenario Modeling; Resilience andCritical Infrastructure Protection; Asset-, Function-, Project-,and Enterprise-Based Security Risk Assessment; SecuritySpecifications and Postures; Security Training; Supply ChainSecurity; Transnational Security; and Travel Security. Security Risk Management Body of Knowledge is supportedby a series of training courses, DVD seminars, tools, andtemplates. This is an indispensable resource for risk and securityprofessional, students, executive management, and line managerswith security responsibilities.

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

Presents theories and models associated with information privacy and safeguard practices to help anchor and guide the development of technologies, standards, and best practices. Provides recent, comprehensive coverage of all issues related to information security and ethics, as well as the opportunities, future challenges, and emerging trends related to this subject.

Electronic CommerceSecurity, Risk Management, and ControlElectronic CommerceSecurity, Risk Management, and ControlManaging E-commerce in BusinessJuta and Company Ltd

Packed with real-world examples and business cases, ELECTRONIC COMMERCE, 11E continues to lead the market with its cutting-edge coverage of all things e-commerce. Comprehensive coverage of emerging online business strategies, up-to-the-minute technologies, and the latest developments from the field equips readers with a solid understanding of the dynamics of this fast-paced industry. The new edition offers thorough discussions of e-commerce growth in China and the developing world, social media and online marketing strategies, technology-enabled outsourcing, online payment processing systems, and much more. In addition, Business Case Approaches and Learning From Failure boxes highlight the experiences of actual companies to illustrate real-world practice in action. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

"This book brings together authoritative authors to address the most pressing challenge in the IT field - how to create secure environments for the application of technology to serve our future needs"--Provided by publisher.

In the next few years, it is expected that most businesses will have transitioned to the use of electronic commerce technologies, namely e-commerce. This acceleration in the acceptance of e-commerce not only changes the face of business and retail, but also has introduced new, adaptive business models. The experience of consumers in online shopping and the popularity of the digital marketplace have changed the way businesses must meet the needs of consumers. To stay relevant, businesses must develop new techniques and strategies to remain competitive in a changing commercial atmosphere. The way in which e-commerce is being implemented, the business models that have been developed, and the applications including the benefits and challenges to e-commerce must be discussed to understand modern business. The Research Anthology on E-Commerce Adoption, Models, and Applications for Modern Business discusses the best practices, latest strategies, and newest methods for implementing and using e-commerce in modern businesses. This includes not only a view of how business models have changed and what business models have emerged, but also provides a focus on how consumers have changed in terms of their needs, their online behavior, and their use of e-commerce services. Topics including e-business, e-services, mobile commerce, usability models, website development, brand management and marketing, and online shopping will be explored in detail. This book is ideally intended for

business managers, e-commerce managers, marketers, advertisers, brand managers, executives, IT consultants, practitioners, researchers, academicians, and students interested in how e-commerce is impacting modern business models.

The Handbook of Information Security is a definitive 3-volume handbook that offers coverage of both established and cutting-edge theories and developments on information and computer security. The text contains 180 articles from over 200 leading experts, providing the benchmark resource for information security, network security, information privacy, and information warfare.

Reliability Engineering and Quality Management provides a competitive advantage and market leadership in a global environment where market barriers are fast disappearing both in the domain of cutting edge and contemporary technologies, manufacturing, process and service sectors like information technology sector. The growth of Q R has been fuelled by increasing sophistication and complexity of system and organisational awareness to produce and market high quality and reliability products and services by the consumer and global market pressures. This subject being interdisciplinary in nature has also brought about a convergence of numerous solution strategies employing Fuzzy Sets, Artificial Neural Nets, Modeling and Simulation, Knowledge Base Systems, Operations Research and Mathematical Programming to achieve high Reliability. This book is intended for both the beginner and practitioner from manufacturing and service sector, research laboratories and academic institutions. This book is unique also as it gives an insight into the current practices and future directions.

This new Edition of Electronic Commerce is a complete update of the leading graduate level/advanced undergraduate level textbook on the subject. Electronic commerce (EC) describes the manner in which transactions take place over electronic networks, mostly the Internet. It is the process of electronically buying and selling goods, services, and information. Certain EC applications, such as buying and selling stocks and airline tickets online, are reaching maturity, some even exceeding non-Internet trades. However, EC is not just about buying and selling; it also is about electronically communicating, collaborating, and discovering information. It is about e-learning, e-government, social networks, and much more. EC is having an impact on a significant portion of the world, affecting businesses, professions, trade, and of course, people. The most important developments in EC since 2014 are the continuous phenomenal growth of social networks, especially Facebook , LinkedIn and Instagram, and the trend toward conducting EC with mobile devices. Other major developments are the expansion of EC globally, especially in China where you can find the world's largest EC company. Much attention is lately being given to smart commerce and the use of AI-based analytics and big data to enhance the field. Finally, some emerging EC business models are changing industries (e.g., the shared economy models of Uber and Airbnb). The 2018 (9th) edition, brings forth the latest trends in e-commerce, including smart commerce, social commerce, social collaboration, shared economy, innovations, and mobility.

Follow step-by-step guidance to craft a successful security program. You will identify with the paradoxes of information security and discover handy tools that hook security controls into business processes. Information security is more than

configuring firewalls, removing viruses, hacking machines, or setting passwords. Creating and promoting a successful security program requires skills in organizational consulting, diplomacy, change management, risk analysis, and out-of-the-box thinking. What You Will Learn: Build a security program that will fit neatly into an organization and change dynamically to suit both the needs of the organization and survive constantly changing threats Prepare for and pass such common audits as PCI-DSS, SSAE-16, and ISO 27001 Calibrate the scope, and customize security controls to fit into an organization's culture Implement the most challenging processes, pointing out common pitfalls and distractions Frame security and risk issues to be clear and actionable so that decision makers, technical personnel, and users will listen and value your advice Who This Book Is For: IT professionals moving into the security field; new security managers, directors, project heads, and would-be CISOs; and security specialists from other disciplines moving into information security (e.g., former military security professionals, law enforcement professionals, and physical security professionals) I3E 2001 is the first in a series of conferences on e-commerce, e-business, and- government organised by the three IFIP committees TC6, TC8, and TC11. It provides a forum, where users, engineers, and scientists from academia, industry, and government can present their latest findings in e-commerce, e-business, and- government applications and the underlying technology to support those applications. The conference comprises a main track and mini tracks dedicated to special topics. The papers presented in the main track were rigorously refereed and selected by the International Programme Committee of the conference. Thematically they were grouped in the following sessions: – Sessions on security and trust, comprising nine papers referring to both trust and security in general as well as presenting specific concepts for enhancing trust in the digital society. – Session on inter-organisational transactions, covering papers related to auditing of inter-organizational trade procedures, cross-organizational workflow and transactions in Business to Business platforms. – Session on virtual enterprises, encompassing papers describing innovative approaches for creating virtual enterprises as well as describing examples of virtual enterprises in specific industries. – Session on online communities containing three papers, which provide case studies of specific online communities and various concepts on how companies can build and harness the potential of online communities. – Sessions on strategies and business models with papers describing specific business models as well as general overviews of specific approaches for E-Strategy formulation.

Information and Communication Technology (ICT) is becoming indispensable in the spheres of business, government, education and entertainment. It makes Internet marketing, e-government, e-learning and online chat services possible. And its commercial aspect, e-commerce, is part of this trend. Today, no business training is complete without the inclusion of at least the basics of e-commerce. But although e-commerce has opened up new opportunities, it also

presents threats and risks. The success of e-commerce hinges on security and trust. Every business manager should therefore have a fundamental awareness of the meaning of e-commerce and ICT security and risk management. This second edition provides guidelines for overcoming these challenges by exploring the ways in which entrepreneurs and managers should co-operate with IT experts to exploit opportunities and combat the threats imposed by new technologies.

Explores the components of e-commerce (including EDI). Shows the risks involved when using an e-commerce system. Provides controls for protecting an e-commerce site (e.g., securing financial transactions and confidential transactions). Provides COSO compliant audit approach. Provides risk/control tables and checklists. Technical topics are discussed in simple user-friendly language.

"This book presents quality articles focused on key issues concerning technology in business"--Provided by publisher.

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.

Security Risk Management is the definitive guide for building or running an information security risk management program. This book teaches practical techniques that will be used on a daily basis, while also explaining the fundamentals so students understand the rationale behind these practices. It explains how to perform risk assessments for new IT projects, how to efficiently manage daily risk activities, and how to qualify the current risk level for presentation to executive level management. While other books focus entirely on risk analysis methods, this is the first comprehensive text for managing security risks. This book will help you to break free from the so-called best practices argument by articulating risk exposures in business terms. It includes case studies to provide hands-on experience using risk assessment tools to calculate the costs and benefits of any security investment. It explores each phase of the risk management lifecycle, focusing on policies and assessment processes that should be used to properly assess and mitigate risk. It also presents a roadmap for designing and implementing a security risk management program. This book will be a valuable resource for CISOs, security managers, IT managers, security consultants, IT auditors, security analysts, and students enrolled in information security/assurance college programs. Named a 2011 Best Governance

and ISMS Book by InfoSec Reviews Includes case studies to provide hands-on experience using risk assessment tools to calculate the costs and benefits of any security investment Explores each phase of the risk management lifecycle, focusing on policies and assessment processes that should be used to properly assess and mitigate risk Presents a roadmap for designing and implementing a security risk management program

E-Commerce has brought about many changes in organizations and has had significant impacts on the quality of life that is experienced by individuals or even indirectly as members of society. The need to have fast and efficient information on products is crucial to our socially conscious and technologically dependent society; hence, information technology has increased the intolerable burden of handling the increasing amount of information and human errors which the society is expected to contend with. The Economic and Social Impacts of E-Commerce addresses issues associated with the advent of e-commerce, and its significance within society.

As a security professional, have you found that you and others in your company do not always define “security” the same way? Perhaps security interests and business interests have become misaligned. Brian Allen and Rachelle Loyear offer a new approach: Enterprise Security Risk Management (ESRM). By viewing security through a risk management lens, ESRM can help make you and your security program successful. In their long-awaited book, based on years of practical experience and research, Brian Allen and Rachelle Loyear show you step-by-step how Enterprise Security Risk Management (ESRM) applies fundamental risk principles to manage all security risks. Whether the risks are informational, cyber, physical security, asset management, or business continuity, all are included in the holistic, all-encompassing ESRM approach which will move you from task-based to risk-based security. How is ESRM familiar? As a security professional, you may already practice some of the components of ESRM. Many of the concepts – such as risk identification, risk transfer and acceptance, crisis management, and incident response – will be well known to you. How is ESRM new? While many of the principles are familiar, the authors have identified few organizations that apply them in the comprehensive, holistic way that ESRM represents – and even fewer that communicate these principles effectively to key decision-makers. How is ESRM practical? ESRM offers you a straightforward, realistic, actionable approach to deal effectively with all the distinct types of security risks facing you as a security practitioner. ESRM is performed in a life cycle of risk management including: Asset assessment and prioritization. Risk assessment and prioritization. Risk treatment (mitigation). Continuous improvement. Throughout Enterprise Security Risk Management: Concepts and Applications, the authors give you the tools and materials that will help you advance you in the security field, no matter if you are a student, a newcomer, or a seasoned professional. Included are realistic case studies, questions to help you assess your own security program, thought-provoking discussion questions, useful figures and tables, and references for your further reading. By redefining how everyone thinks about the role of security in the enterprise, your security organization can focus on working in partnership with business leaders and other key stakeholders to identify and mitigate security risks. As you begin to use ESRM, following the instructions in this book, you will experience greater personal and professional satisfaction as a security professional – and you’ll become a recognized

and trusted partner in the business-critical effort of protecting your enterprise and all its assets.

Technology is continuously advancing and changing the way aspects of business are performed. The implementation of mobile business transactions to acquire various types of goods has changed the landscape of consumerism. Apps Management and E-Commerce Transactions in Real-Time is a timely research publication that features the latest scholarly trends, issues, and implications of the use of a new technological forum in electronic buying and selling. Including extensive coverage on a number of topics and perspectives such as social networks, customer satisfaction, and cloud computing, this book is ideally designed for researchers, academicians, and students seeking current research on mobile solutions in business deals.

Compiles top research from the world's leading experts on many topics related to electronic commerce. Covers topics including mobile commerce, virtual enterprises, business-to-business applications, Web services, and enterprise methodologies.

Some analysts predict that electronic commerce will grow to more than $300 billion in the next five years. With electronic commerce growing in exponentially, staying competitive through an effect e-business strategy is a tough challenge. Electronic commerce represents one of the most promising directions for generating competitive advantage at the micro level of the organization and for increasing productivity at the macro level of the economy. Electronic Commerce: Opportunity and Challenges looks at the critical fundamental elements that could impact a user's perception of business-to-business and business-to-consumer electronic commerce. It presents a study of key components and concepts of e-commerce, evaluating the critical success factors for global e-commerce, the economics of e-commerce and the practical issues involved with e-commerce in various applications.

"This book provides high-quality research papers and industrial practice articles about information security in the financial service industry. It provides insight into current information security measures, including: technology, processes, and compliance from some of the leading researchers and practitioners in the field"--Provided by publisher.