Information System Security Review Methodology

This book addresses the uses and practical aspects of the analysis, design and specification of information systems security, and will represent the intersection of the work in computer security and current work in systems analysis and auditing.
Part of the Jones & Bartlett Learning Information Systems Security and Assurance Series Revised and updated to address the many changes in this evolving field, the Second Edition of Legal Issues in Information Security addresses the area where law and information security concerns intersect. Information systems security and legal compliance are now required to protect critical governmental and corporate infrastructure, intellectual property created by individuals and organizations alike, and information that individuals believe should be protected from unreasonable intrusion. Organizations must build numerous information security and privacy responses into their daily operations to protect the business itself, fully meet legal requirements, and to meet the expectations of employees and customers. Instructor Materials for Legal Issues in Information Security include: PowerPoint Lecture Slides Instructor's Guide Sample Course Syllabus Quiz & Exam Questions Case

Scenarios/Handouts New to the Second Edition: Includes discussions of amendments in several relevant federal and state laws and regulations since 2011 Reviews relevant court decisions that have come to light since the publication of the first edition Includes numerous information security data breaches highlighting new vulnerabilities" Thoroughly revised and updated to address the many changes in this evolving field, the third edition of Legal and Privacy Issues in Information Security addresses the complex relationship between the law and the practice of information security. Information systems security and legal compliance are required to protect critical governmental and corporate infrastructure, intellectual property created by individuals and organizations alike, and information that individuals believe should be protected from unreasonable intrusion. Organizations must build numerous information security and privacy responses into their daily operations to protect the business itself, fully meet legal requirements, and to meet the expectations of employees and customers. Instructor Materials for Legal Issues in Information Security include: PowerPoint Lecture Slides Instructor's Guide Sample Course Syllabus Quiz & Exam Questions Case Scenarios/Handouts New to the third Edition: • Includes discussions of amendments in several relevant federal and state laws and regulations since 2011 • Reviews relevant

court decisions that have come to light since the publication of the first edition • Includes numerous information security data breaches highlighting new vulnerabilities

Effective security rules and procedures do not exist for their own sake-they are put in place to protect critical assets, thereby supporting overall business objectives. Recognizing security as a business enabler is the first step in building a successful program. Information Security Fundamentals allows future security professionals to gain a solid understanding of the foundations of the field and the entire range of issues that practitioners must address. This book enables students to understand the key elements that comprise a successful information security program and eventually apply these concepts to their own efforts. The book examines the elements of computer security, employee roles and responsibilities, and common threats. It examines the need for management controls, policies and procedures, and risk analysis, and also presents a comprehensive list of tasks and objectives that make up a typical information protection program. The volume discusses organizationwide policies and their documentation, and legal and business requirements. It explains policy format, focusing on global, topic-specific, and application-specific policies. Following a review of asset classification, the book explores access

control, the components of physical security, and the foundations and processes of risk analysis and risk management. Information Security Fundamentals concludes by describing business continuity planning, including preventive controls, recovery strategies, and ways to conduct a business impact analysis.

WILEY CIAexcel EXAM REVIEW 2016 THE SELF-STUDY SUPPORT YOU NEED TO PASS THE CIA EXAM Part 3: Internal Audit Knowledge Elements Provides comprehensive coverage based on the exam syllabus, along with sample practice multiple-choice questions with answers and explanations Deals with governance and business ethics, risk management, information technology, and the global business environment Features a glossary of CIA Exam terms, a good source for candidates preparing for and answering the exam questions Assists the CIA Exam candidate in successfully preparing for the exam Based on the CIA body of knowledge developed by The Institute of Internal Auditors (IIA), Wiley CIAexcel Exam Review 2016 learning system provides a student-focused and learning-oriented experience for CIA candidates. Passing the CIA Exam on your first attempt is possible. We'd like to help. Feature section examines the topics of Governance and Business Ethics, Risk Management, Organizational Structure and Business Processes and Risks, Communications,

Management and Leadership Principles, IT and Business Continuity, Financial Management, and Global Business Environment

Security and Privacy in the Age of Uncertainty covers issues related to security and privacy of information in a wide range of applications including: *Secure Networks and Distributed Systems; *Secure Multicast Communication and Secure Mobile Networks; *Intrusion Prevention and Detection; *Access Control Policies and Models; *Security Protocols; *Security and Control of IT in Society. This volume contains the papers selected for presentation at the 18th International Conference on Information Security (SEC2003) and at the associated workshops. The conference and workshops were sponsored by the International Federation for Information Processing (IFIP) and held in Athens, Greece in May 2003.

FISMA and the Risk Management Framework: The New Practice of Federal Cyber Security deals with the Federal Information Security Management Act (FISMA), a law that provides the framework for securing information systems and managing risk associated with information resources in federal government agencies. Comprised of 17 chapters, the book explains the FISMA legislation and its provisions, strengths and limitations, as well as the expectations and obligations of federal agencies subject to FISMA. It also discusses the processes

and activities necessary to implement effective information security management following the passage of FISMA, and it describes the National Institute of Standards and Technology's Risk Management Framework. The book looks at how information assurance, risk management, and information systems security is practiced in federal government agencies; the three primary documents that make up the security authorization package: system security plan, security assessment report, and plan of action and milestones; and federal information security-management requirements and initiatives not explicitly covered by FISMA. This book will be helpful to security officers, risk managers, system owners, IT managers, contractors, consultants, service providers, and others involved in securing, managing, or overseeing federal information systems, as well as the mission functions and business processes supported by those systems. Learn how to build a robust, near real-time risk management system and comply with FISMA Discover the changes to FISMA compliance and beyond Gain your systems the authorization they need

Computers at Risk presents a comprehensive agenda for developing nationwide policies and practices for computer security. Specific recommendations are provided for industry and for government agencies engaged in computer security activities. The volume also outlines problems and opportunities in computer security research, recommends

ways to improve the research infrastructure, and suggests topics for investigators. The book explores the diversity of the field, the need to engineer countermeasures based on speculation of what experts think computer attackers may do next, why the technology community has failed to respond to the need for enhanced security systems, how innovators could be encouraged to bring more options to the marketplace, and balancing the importance of security against the right of privacy.

Master internal audit knowledge elements for the CIA exam Wiley CIAexcel Exam Review 2015: Part 3, Internal Audit Knowledge Elements is a comprehensive yet approachable reference that prepares you for the third part of the Certified Internal Auditor (CIA) examination. Brimming with essential concepts and practice test questions, this test prep resource is the most comprehensive of its kind on the market. With each page you will explore key subject areas, including business processes, financial accounting and finance, managerial accounting, regulatory, legal, and economics, and information technology. All of these subject areas are expertly tied to the topic of internal audit knowledge elements, and all ideas—both fundamental and complex—are presented in an easy-to-read yet thorough manner. Holding the designation of CIA will take your career to the next level, as passing the CIA exam speaks volumes about your professional skills and expertise. Leveraging the right study materials when preparing for the CIA exam is critical, as the topics that may be covered on the test are many in number. This resource presents these topics from a student's perspective, providing the details you need to master challenging concepts and practices. Access comprehensive preparation materials for the third part of the CIA exam Explore essential internal audit knowledge elements, including key concepts and practices Answer hundreds of practice test questions to gauge your

progress and focus your study sessions Improve your proficiency, understanding, and awareness of key concepts tested by the CIA examination Wiley CIAexcel Exam Review 2015: Part 3, Internal Audit Knowledge Elements is an invaluable resource for internal auditors, chief audit executives, audit managers, and staff members who are pursuing the CIA designation.

Rapid progress in information and communications technologies is dramatically enhancing the strategic role of information, positioning effective exploitation of these technology advances as a critical success factor in military affairs. These technology advances are drivers and enablers for the "nervous system" of the militaryâ€"its command, control, communications, computers, and intelligence (C4I) systemsâ€"to more effectively use the "muscle" side of the military. Authored by a committee of experts drawn equally from the military and commercial sectors, Realizing the Potential of C4I identifies three major areas as fundamental challenges to the full Department of Defense (DOD) exploitation of C4I technologyâ€"information systems security, interoperability, and various aspects of DOD process and culture. The book details principles by which to assess DOD efforts in these areas over the long term and provides specific, more immediately actionable recommendations. Although DOD is the focus of this book, the principles and issues presented are also relevant to interoperability, architecture, and security challenges faced by government as a whole and by large, complex public and private enterprises across the economy.

Understanding an organization's reliance on information systems and how to mitigate the vulnerabilities of these systems can be an intimidating challenge--especially when considering less well-known weaknesses or even unknown vulnerabilities that have not yet been exploited. The authors

introduce the Vulnerability Assessment and Mitigation methodology, a six-step process that uses a top-down approach to protect against future threats and system failures while mitigating current and past threats and weaknesses. Computers at RiskSafe Computing in the Information AgeNational Academies Press

This textbook presents a proven, mature Model-Based Systems Engineering (MBSE) methodology that has delivered success in a wide range of system and enterprise programs. The authors introduce MBSE as the state of the practice in the vital Systems Engineering discipline that manages complexity and integrates technologies and design approaches to achieve effective, affordable, and balanced system solutions to the needs of a customer organization and its personnel. The book begins with a summary of the background and nature of MBSE. It summarizes the theory behind Object-Oriented Design applied to complex system architectures. It then walks through the phases of the MBSE methodology, using system examples to illustrate key points. Subsequent chapters broaden the application of MBSE in Service-Oriented Architectures (SOA), real-time systems, cybersecurity, networked enterprises, system simulations, and prototyping. The vital subject of system and architecture governance completes the discussion. The book features exercises at the end of each chapter intended to help readers/students focus on key points, as well as extensive appendices that furnish additional detail in particular areas. The self-contained text is ideal for students in a range of courses in systems architecture and MBSE as well as for practitioners seeking a highly practical presentation of MBSE principles and techniques.

Nowadays it is impossible to imagine a business without technology as most industries are becoming "smarter" and more tech-driven, ranging from small individual tech initiatives

to complete business models with intertwined supply chains and "platform"-based business models. New ways of working, such as agile and DevOps, have been introduced, leading to new risks. These risks come in the form of new challenges for teams working together in a distributed manner, privacy concerns, human autonomy, and cybersecurity concerns. Technology is now integrated into the business discipline and is here to stay leading to the need for a thorough understanding of how to address these risks and all the potential problems that could arise. With the advent of organized crime, such as hacks and denial-of-service attacks, all kinds of malicious actors are infiltrating the digital society in new and unique ways. Systems with poor design, implementation, and configurations are easily taken advantage of. When it comes to integrating business and technology, there needs to be approaches for assuring security against risks that can threaten both businesses and their digital platforms. Strategic Approaches to Digital Platform Security Assurance offers comprehensive design science research approaches to extensively examine risks in digital platforms and offer pragmatic solutions to these concerns and challenges. This book addresses significant problems when transforming an organization embracing API-based platform models, the use of DevOps teams, and issues in technological architectures. Each section will examine the status quo for business technologies, the current challenges, and core success factors and approaches that have been used. This book is ideal for security analysts, software engineers, computer engineers, executives, managers, IT consultants, business professionals, researchers, academicians, and students who want to gain insight and deeper knowledge of security in digital platforms and gain insight into the most important success factors and approaches utilized by businesses.

This Three-Volume-Set constitutes the refereed proceedings of the Second International Conference on Software Engineering and Computer Systems, ICSECS 2011, held in Kuantan, Malaysia, in June 2011. The 190 revised full papers presented together with invited papers in the three volumes were carefully reviewed and selected from numerous submissions. The papers are organized in topical sections on software engineering; network; bioinformatics and e-health; biometrics technologies; Web engineering; neural network; parallel and distributed e-learning; ontology; image processing; information and data management; engineering; software security; graphics and multimedia; databases; algorithms; signal processing; software design/testing; e-technology; ad hoc networks; social networks; software process modeling; miscellaneous topics in software engineering and computer systems.

"This book reviews issues and trends in security and privacy at an individual user level, as well as within global enterprises, covering enforcement of existing security technologies, factors driving their use, and goals for ensuring the continued security of information systems"--Provided by publisher.

These are the proceedings of the Eleventh International Information Security Conference which was held in Cape Town, South Africa, May 1995. This conference addressed the information security requirements of the next decade and papers were presented covering a wide range of subjects including current industry expectations and current research aspects. The evolutionary development of information security as a professional

and research discipline was discussed along with security in open distributed systems and security in groupware.

Implementing Information Security in Healthcare: Building a Security Program offers a critical and comprehensive look at healthcare security concerns in an era of powerful computer technology, increased mobility, and complex regulations designed to protect personal information. Featuring perspectives from more than two dozen security experts, the book explores the tools and policies healthcare organizations need to build an effective and compliant security program. Topics include information security frameworks, risk analysis, senior management oversight and involvement, regulations, security policy development, access control, network security, encryption, mobile device management, disaster recovery, and more. Information security is a concept that has never been more important to healthcare as it is today. Special features include appendices outlining potential impacts of security objectives, technical security features by regulatory bodies (FISMA, HIPAA, PCI DSS and ISO 27000), common technical security features, and a sample risk rating chart.

Complete exam review for the third part of the Certified Internal Auditor exam The Wiley CIA 2022 Part 3 Exam Review: Business Knowledge for Internal Auditing offers students preparing for the Certified Internal Auditor 2022 exam complete coverage of the business knowledge portion of the test. Entirely consistent with the guidelines set by the Institute of Internal Auditors (IIA), this resource

covers each of the four domains explored by the test, including: Business acumen. Information security. Information technology. Financial management. This reference provides an accessible and efficient learning experience for students, regardless of their current level of comfort with the material.

FISCAM presents a methodology for performing info. system (IS) control audits of governmental entities in accordance with professional standards. FISCAM is designed to be used on financial and performance audits and attestation engagements. The methodology in the FISCAM incorp. the following: (1) A top-down, risk-based approach that considers materiality and significance in determining audit procedures; (2) Evaluation of entitywide controls and their effect on audit risk; (3) Evaluation of general controls and their pervasive impact on bus. process controls; (4) Evaluation of security mgmt. at all levels; (5) Control hierarchy to evaluate IS control weaknesses; (6) Groupings of control categories consistent with the nature of the risk. Illus.

WILEY CIAexcel EXAM REVIEW 2018 THE SELF-STUDY SUPPORT YOU NEED TO PASS THE CIA EXAM Part 3: Internal Audit Knowledge Elements Provides comprehensive coverage based on the exam syllabus, along with multiple-choice practice questions with answers and explanations Deals with governance and business ethics, risk management, information technology, and the global business environment Features a glossary of CIA Exam terms—good source for candidates preparing for and answering the exam questions Assists the CIA Exam candidate in

successfully preparing for the exam Based on the CIA body of knowledge developed by The Institute of Internal Auditors (IIA), Wiley CIAexcel Exam Review 2018 learning system provides a student-focused and learning-oriented experience for CIA candidates. Passing the CIA Exam on your first attempt is possible. We'd like to help. Feature section examines the topics of Governance and Business Ethics, Risk Management, Organizational Structure and Business Processes and Risks, Communications, Management and Leadership Principles, IT and Business Continuity, Financial Management, and Global Business Environment

The real threat to information system security comes from people, not computers. That's why students need to understand both the technical implementation of security controls, as well as the softer human behavioral and managerial factors that contribute to the theft and sabotage proprietary data. Addressing both the technical and human side of IS security, Dhillon's Princliples of Information Systems Security: Texts and Cases equips managers (and those training to be managers) with an understanding of a broad range issues related to information system security management, and specific tools and techniques to support this managerial orientation. Coverage goes well beyond the technical aspects of information system security to address formal controls (the rules and procedures that need to be established for bringing about success of technical controls), as well as informal controls that deal with the normative structures that exist within organizations.

Discusses all types of corporate risks and practical means of defending against them. Security is currently identified as a critical area of Information Technology management by a majority of government, commercial, and industrial

organizations. Offers an effective risk management program, which is the most critical function of an information security program.

Charged with ensuring the confidentiality, integrity, availability, and delivery of all forms of an entity's information, Information Assurance (IA) professionals require a fundamental understanding of a wide range of specializations, including digital forensics, fraud examination, systems engineering, security risk management, privacy, and compliance. Establishing this understanding and keeping it up to date requires a resource with coverage as diverse as the field it covers. Filling this need, the Encyclopedia of Information Assurance presents an up-to-date collection of peer-reviewed articles and references written by authorities in their fields. From risk management and privacy to auditing and compliance, the encyclopedia's four volumes provide comprehensive coverage of the key topics related to information assurance. This complete IA resource: Supplies the understanding needed to help prevent the misuse of sensitive information Explains how to maintain the integrity of critical systems Details effective tools, techniques, and methods for protecting personal and corporate data against the latest threats Provides valuable examples, case studies, and discussions on how to address common and emerging IA challenges Placing the wisdom of leading researchers and practitioners at your fingertips, this authoritative reference provides the knowledge and insight needed to avoid common pitfalls and stay one step ahead of evolving threats. Also Available Online This Taylor & Francis encyclopedia is also available through online subscription, offering a variety of extra benefits for researchers, students, and librarians, including: ? Citation tracking and alerts ? Active reference linking ? Saved searches and marked lists ? HTML and PDF format options Contact Taylor and Francis for more

information or to inquire about subscription options and print/online combination packages. US: (Tel) 1.888.318.2367; (E-mail) e-reference@taylorandfrancis.com International: (Tel) +44 (0) 20 7017 6062; (E-mail) online.sales@tandf.co.uk

The Tennessee Valley Authority (TVA), a fed. corp. and the nation's largest public power company, generates and distributes power in an area of about 80,000 square miles in the southeastern U.S. This report determines whether TVA has implemented appropriate information security practices to protect its control systems. To do this, the auditor examined the security practices in place at several TVA facilities; analyzed the agency¿s information security policies, plans, and procedures against fed. law and guidance; and interviewed agency officials who are responsible for overseeing TVA¿s control systems and their security. Includes recommendations. Charts and tables.

Considered the gold-standard reference on information security, the Information Security Management Handbook provides an authoritative compilation of the fundamental knowledge, skills, techniques, and tools required of today's IT security professional. Now in its sixth edition, this 3200 page, 4 volume stand-alone reference is organized under the C

This three-volume collection, titled Enterprise Information Systems: Concepts, Methodologies, Tools and Applications, provides a complete assessment of the latest developments in enterprise information systems research, including development, design, and emerging methodologies. Experts in the field cover all aspects of enterprise resource planning (ERP), e-commerce, and organizational, social and technological implications of enterprise information systems.

"Special attention is paid to terms which most often prevent educated readers from understanding journal articles and books in cryptology, security and information systems, and

computer science, in addition to applied fields that build on these disciplines, such as system design, security auditing, vulnerability testing, and role-based management. The emphasis throughout The Information Security Dictionary is on concepts, rather than implementations. Since concepts often complicate matters, readers may find a definition makes sense only after it has been illustrated by an example which the author provides in this dictionary." "The Dictionary of Information Security is designed for researchers, students, and practitioners in industry, as well as educated readers interested in the security field."--BOOK JACKET.

This book provides a coherent overview of the most important modelling-related security techniques available today, and demonstrates how to combine them. Further, it describes an integrated set of systematic practices that can be used to achieve increased security for software from the outset, and combines practical ways of working with practical ways of distilling, managing, and making security knowledge operational. The book addresses three main topics: (1) security requirements engineering, including security risk management, major activities, asset identification, security risk analysis and defining security requirements; (2) secure software system modelling, including modelling of context and protected assets, security risks, and decisions regarding security risk treatment using various modelling languages; and (3) secure system development, including effective approaches, pattern-driven development, and model-driven security. The primary target audience of this book is graduate students studying cyber security, software engineering and system security engineering. The book will also benefit practitioners interested in learning about

the need to consider the decisions behind secure software systems. Overall it offers the ideal basis for educating future generations of security experts.

The fast-paced world created by the accessibility of consumer information through internet-generated data requires improved information-management platforms. The continuous evaluation and evolution of these systems facilitate enhanced data reference and output. Optimizing Data and New Methods for Efficient Knowledge Discovery and Information Resources Management is a critical research publication that provides insight into the varied and rapidly changing fields of knowledge discovery and information resource management. Highlighting a range of topics such as datamining, artificial intelligence, and risk assessment, this book is essential for librarians, academicians, policymakers, information managers, professionals, and researchers in fields that include artificial intelligence, knowledge discovery, data visualization, big data, and information resources management.

Information systems have become a critical element of every organization’s structure. A malfunction of the information and communication technology (ICT) infrastructure can paralyze the whole organization and have disastrous consequences at many levels. On the other hand, modern businesses and organizations collaborate increasingly with companies, customers, and other stakeholders by technological means. This emphasizes the need for a reliable and secure ICT infrastructure for companies whose principal asset and added value is information. Information Security

Evaluation: A Holistic Approach from a Business Perspective proposes a global and systemic multidimensional integrated approach to the holistic evaluation of the information security posture of an organization. The Information Security Assurance Assessment Model (ISAAM) presented in this book is based on, and integrates, a number of information security best practices, standards, methodologies and sources of research expertise, in order to provide a generic model that can be implemented in organizations of all kinds as part of their efforts towards better governing their information security. This approach will contribute to improving the identification of security requirements, measures and controls. At the same time, it provides a means of enhancing the recognition of evidence related to the assurance, quality and maturity levels of the organization's security posture, thus driving improved security effectiveness and efficiency. The value added by this evaluation model is that it is easy to implement and operate and that through a coherent system of evaluation it addresses concrete needs in terms of reliance on an efficient and dynamic evaluation tool.

This glossary provides a central resource of definitions most commonly used in Nat. Institute of Standards and Technology (NIST) information security publications and in the Committee for National Security Systems (CNSS) information assurance publications. Each entry in the glossary points to one or more source NIST publications, and/or CNSSI-4009, and/or supplemental sources where appropriate. This is a print on demand edition of an

important, hard-to-find publication.

The rapid evolution of technology continuously changes the way people interact, work, and learn. By examining these advances from a sociological perspective, researchers can further understand the impact of cyberspace on human behavior, interaction, and cognition. Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications is a vital reference source covering the impact of social networking platforms on a variety of relationships, including those between individuals, governments, citizens, businesses, and consumers. The publication also highlights the negative behavioral, physical, and mental effects of increased online usage and screen time such as mental health issues, internet addiction, and body image. Showcasing a range of topics including online dating, smartphone dependency, and cyberbullying, this multi-volume book is ideally designed for sociologists, psychologists, computer scientists, engineers, communication specialists, academicians, researchers, and graduate-level students seeking current research on media usage and its behavioral effects.