Foundations Of Information Security Based On Iso27001 And Iso27002

As technological and legal changes have hollowed out the protections that reporters and news organizations have depended upon for decades, information security concerns facing journalists as they report, produce, and disseminate the news have only intensified. From source prosecutions to physical attacks and online harassment, the last two decades have seen a dramatic increase in the risks faced by journalists at all levels even as the media industry confronts drastic cutbacks in budgets and staff. As a result, few professional or aspiring journalists have a comprehensive understanding of what is required to keep their sources, stories, colleagues, and reputations safe. This book is an essential guide to protecting news writers, sources, and organizations in the digital era. Susan E. McGregor provides a systematic understanding of the key technical, legal, and conceptual issues that anyone teaching, studying, or practicing journalism should know. Bringing together expert insights from both leading academics and security professionals who work at and with news organizations from BuzzFeed to the Associated Press, she lays out key principles and approaches for building information security into journalistic practice. McGregor draws on firsthand experience as a Wall Street Journal staffer, followed by a decade of researching, testing, and developing information security tools and practices. Filled with practical but evergreen advice that can enhance the security and efficacy of everything from daily beat reporting to long-term investigative projects, Information Security Essentials is a vital tool for journalists at all levels.
High-level overview of the information security field. Covers key concepts like confidentiality, integrity, and availability, then dives into practical applications of these ideas in the areas of operational, physical, network, application, and operating system security. In this high-level survey of the information security field, best-selling author Jason Andress covers the basics of a wide variety of topics, from authentication and authorization to maintaining confidentiality and performing penetration testing. Using real-world security breaches as examples, Foundations of Information Security explores common applications of these concepts, such as operations security, network design, hardening and patching operating systems, securing mobile devices, as well as tools for assessing the security of hosts and applications. You'll also learn the basics of topics like: • Multifactor authentication and how biometrics and hardware tokens can be used to harden the authentication process • The principles behind modern cryptography, including symmetric and asymmetric algorithms, hashes, and certificates • The laws and regulations that protect systems and data • Anti-malware tools, firewalls, and intrusion detection systems • Vulnerabilities such as buffer overflows and race conditions A valuable resource for beginning security professionals, network systems administrators, or anyone new to the field, Foundations of Information Security is a great place to start your journey into the

dynamic and rewarding field of information security.

This book features a wide spectrum of the latest computer science research relating to cyber warfare, including military and policy dimensions. It is the first book to explore the scientific foundation of cyber warfare and features research from the areas of artificial intelligence, game theory, programming languages, graph theory and more. The high-level approach and emphasis on scientific rigor provides insights on ways to improve cyber warfare defense worldwide. Cyber Warfare: Building the Scientific Foundation targets researchers and practitioners working in cyber security, especially government employees or contractors. Advanced-level students in computer science and electrical engineering with an interest in security will also find this content valuable as a secondary textbook or reference.

This handbook offers a comprehensive overview of cloud computing security technology and implementation while exploring practical solutions to a wide range of cloud computing security issues. As more organizations use cloud computing and cloud providers for data operations, the need for proper security in these and other potentially vulnerable areas has become a global priority for organizations of all sizes. Research efforts from academia and industry as conducted and reported by experts in all aspects of security related to cloud computing are gathered within one reference guide. Features • Covers patching and configuration vulnerabilities of a cloud server • Evaluates methods for data encryption and long-term storage in a cloud server • Demonstrates how to verify identity using a certificate chain and how to detect inappropriate changes to data or system configurations John R. Vacca is an information technology consultant and internationally known author of more than 600 articles in the areas of advanced storage, computer security, and aerospace technology. John was also a configuration management specialist, computer specialist, and the computer security official (CSO) for NASA’s space station program (Freedom) and the International Space Station Program from 1988 until his 1995 retirement from NASA.

The world of IT is always evolving, but in every area there arestable, core concepts that anyone just setting out needed to knowlast year, needs to know this year, and will still need to knownext year. The purpose of the Foundations series is to identifythese concepts and present them in a way that gives you thestrongest possible starting point, no matter what your endeavor. Network Security Foundations provides essential knowledgeabout the principles and techniques used to protect computers andnetworks from hackers, viruses, and other threats. What you learnhere will benefit you in the short term, as you acquire andpractice your skills, and in the long term, as you use them. Topicscovered include: Why and how hackers do what they do How encryption and authentication work How firewalls work Understanding Virtual Private Networks (VPNs) Risks posed by remote access Setting up protection against viruses, worms, and spyware Securing Windows computers Securing UNIX and

Linux computers Securing Web and email servers Detecting attempts by hackers

The topic of information theoretic security is introduced and the principal results in this area are reviewed. The basic wire-tap channel model is considered first, and then several specific types of wire-tap channels are considered, including Gaussian, multi-input multi-output (MIMO), compound, and feedback wire-tap channels, as well as the wire-tap channel with side information. Practical code design techniques to achieve secrecy for wire-tap channels are also introduced. The wire-tap formalism is then extended to the basic channels of multi-user networks, including broadcast channels, multiple-access channels (MACs), interference channels, relay channels and two-way channels. For all of these models, results on the fundamental communication limits under secrecy constraints and corresponding coding schemes are reviewed. Furthermore, several related topics including key agreement through common randomness, secure network coding, authentication, cross-layer design, and secure source coding are discussed.

Hardware-intrinsic security is a young field dealing with secure secret key storage. By generating the secret keys from the intrinsic properties of the silicon, e.g., from intrinsic Physical Unclonable Functions (PUFs), no permanent secret key storage is required anymore, and the key is only present in the device for a minimal amount of time. The field is extending to hardware-based security primitives and protocols such as block ciphers and stream ciphers entangled with the hardware, thus improving IC security. While at the application level there is a growing interest in hardware security for RFID systems and the necessary accompanying system architectures. This book brings together contributions from researchers and practitioners in academia and industry, an interdisciplinary group with backgrounds in physics, mathematics, cryptography, coding theory and processor theory. It will serve as important background material for students and practitioners, and will stimulate much further research and development.

Information Security Foundation based on ISO/IEC 27002 Courseware is for anyone who wants to deliver courses aimed at passing the ISFS (Information Security Foundation) exam of EXIN. This courseware is primarily developed for a classroom training in Information Security Foundation based on ISO/IEC 27002. The basis for this courseware is the 3rd revised edition of the study book Foundations of Information Security Based on ISO27001 and ISO27002. The various modules in the courseware relate to paragraphs of this study book, per slide pointing out where additional information on each subject can be found. In Module 7, an ISFS model exam training from the book is given, including an explanation to all multiple choice options, so that it can be used during a training for the ISFS exam. The courseware contains the following: • Module 1: About EXIN • Module 2: Information and security, ISO 2700x • Module 4: Approach and organization Security policy and security organization Components Incident management • Module 5: Measures Importance of measures Physical security measures Technical measures Organizational measures • Module 6: Legislation

Legislation and regulations • Module 7: Exam training (from book) • Module 8: Exam • EXIN Sample exam • EXIN Preparation Guide The Certificate EXIN Information Security Foundation based on ISO/IEC 27002 is part of the qualification program Information Security. The module is followed up by the Certificates EXIN Information Security Management Advanced based on ISO/IEC 27002 and EXIN Information Security Management Expert based on ISO/IEC 27002.

“It is about time that a book like The New School came along. The age of security as pure technology is long past, and modern practitioners need to understand the social and cognitive aspects of security if they are to be successful. Shostack and Stewart teach readers exactly what they need to know--I just wish I could have had it when I first started out.” --David Mortman, CSO-in-Residence Echelon One, former CSO Siebel Systems Why is information security so dysfunctional? Are you wasting the money you spend on security? This book shows how to spend it more effectively. How can you make more effective security decisions? This book explains why professionals have taken to studying economics, not cryptography--and why you should, too. And why security breach notices are the best thing to ever happen to information security. It’s about time someone asked the biggest, toughest questions about information security. Security experts Adam Shostack and Andrew Stewart don’t just answer those questions--they offer honest, deeply troubling answers. They explain why these critical problems exist and how to solve them. Drawing on powerful lessons from economics and other disciplines, Shostack and Stewart offer a new way forward. In clear and engaging prose, they shed new light on the critical challenges that are faced by the security field. Whether you’re a CIO, IT manager, or security specialist, this book will open your eyes to new ways of thinking about--and overcoming--your most pressing security challenges. The New School enables you to take control, while others struggle with non-stop crises. Better evidence for better decision-making Why the security data you have doesn’t support effective decision-making--and what to do about it Beyond security “silos”: getting the job done together Why it’s so hard to improve security in isolation--and how the entire industry can make it happen and evolve Amateurs study cryptography; professionals study economics What IT security leaders can and must learn from other scientific fields A bigger bang for every buck How to re-allocate your scarce resources where they’ll do the most good

As part of the Syngress Basics series, The Basics of Information Security provides you with fundamental knowledge of information security in both theoretical and practical aspects. Author Jason Andress gives you the basic knowledge needed to understand the key concepts of confidentiality, integrity, and availability, and then dives into practical applications of these ideas in the areas of operational, physical, network, application, and operating system security. The Basics of Information Security gives you clear-non-technical explanations of how infosec works and how to apply these principles whether you're in the IT field or want to understand how it affects your career

and business. The new Second Edition has been updated for the latest trends and threats, including new material on many infosec subjects. Learn about information security without wading through a huge textbook Covers both theoretical and practical aspects of information security Provides a broad view of the information security field in a concise manner All-new Second Edition updated for the latest information security trends and threats, including material on incident response, social engineering, security awareness, risk management, and legal/regulatory issues

With the prevalence of digital information, IT professionals have encountered new challenges regarding data security. In an effort to address these challenges and offer solutions for securing digital information, new research on cryptology methods is essential. Multidisciplinary Perspectives in Cryptology and Information Security considers an array of multidisciplinary applications and research developments in the field of cryptology and communication security. This publication offers a comprehensive, in-depth analysis of encryption solutions and will be of particular interest to IT professionals, cryptologists, and researchers in the field.

"This book covers basic concepts of web and information system security and provides new insights into the semantic web field and its related security challenges"--Provided by publisher.

In today’s litigious business world, cyber-related matters could land you in court. As a computer security professional, you are protecting your data, but are you protecting your company? While you know industry standards and regulations, you may not be a legal expert. Fortunately, in a few hours of reading, rather than months of classroom study, Tari Schreider’s Cybersecurity Law, Standards and Regulations (2nd Edition), lets you integrate legal issues into your security program. Tari Schreider, a board-certified information security practitioner with a criminal justice administration background, has written a much-needed book that bridges the gap between cybersecurity programs and cybersecurity law. He says, “My nearly 40 years in the fields of cybersecurity, risk management, and disaster recovery have taught me some immutable truths. One of these truths is that failure to consider the law when developing a cybersecurity program results in a protective façade or false sense of security.” In a friendly style, offering real-world business examples from his own experience supported by a wealth of court cases, Schreider covers the range of practical information you will need as you explore – and prepare to apply – cybersecurity law. His practical, easy-to-understand explanations help you to: Understand your legal duty to act reasonably and responsibly to protect assets and information. Identify which cybersecurity laws have the potential to impact your cybersecurity program. Upgrade cybersecurity policies to comply with state, federal, and regulatory statutes. Communicate effectively about cybersecurity law with corporate legal department and counsel. Understand the implications of emerging legislation for your cybersecurity program. Know how to avoid losing a cybersecurity court case on procedure – and develop strategies to handle a dispute out of court. Develop an international view of cybersecurity and data privacy – and international legal frameworks. Schreider takes you beyond security standards and regulatory controls to ensure that your current or future cybersecurity program complies with all laws and legal jurisdictions. Hundreds of citations and references allow you to dig deeper as you explore specific topics relevant to your organization or your studies. This book needs to be required reading before your next discussion with your corporate

legal department. This new edition responds to the rapid changes in the cybersecurity industry, threat landscape and providers. It addresses the increasing risk of zero-day attacks, growth of state-sponsored adversaries and consolidation of cybersecurity products and services in addition to the substantial updates of standards, source links and cybersecurity products.

This book constitutes the revised selected papers of the 13th International Symposium on Foundations and Practice of Security, FPS 2020, held in Montréal, QC, Canada, in December 2020. The 11full papers and 1 short paper presented in this book were carefully reviewed and selected from 23 submissions. They cover a range of topics such as Analysis and Detection; Prevention and Efficiency; and Privacy by Design.

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.

This book is the officially by Exin accredited courseware for the Information Security Management Professional training.

PART OF THE JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Revised and updated with the latest information from this fast-paced field, Fundamentals of Information System Security, Second Edition provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security. The text opens with a discussion of the new risks, threats, and vulnerabilities associated with the transformation to a digital world, including a look at how business, government, and individuals operate today. Part 2 is adapted from the Official (ISC)2 SSCP Certified Body of Knowledge and presents a high-level overview of each of the seven domains within the System Security Certified Practitioner certification. The book closes with a resource for readers who desire additional material on information security standards, education, professional certifications, and compliance laws. With its practical, conversational writing style and step-by-step examples, this text is a must-have resource for those entering the world of information systems security. New to the Second Edition: - New material on cloud computing, risk analysis, IP mobility, OMNIBus, and Agile Software Development. - Includes the most recent updates in Information Systems Security laws, certificates, standards, amendments, and the proposed Federal Information Security Amendments Act of 2013 and HITECH Act. - Provides new cases and examples pulled from real-world scenarios. - Updated data, tables, and sidebars provide the most current information in the field.

As internet technologies continue to advance, new types and methods of data and security breaches threaten national security. These potential breaches allow for information theft and can provide footholds for terrorist and criminal organizations. Developments in Information Security and Cybernetic Wars is an essential research

publication that covers cyberwarfare and terrorism globally through a wide range of security-related areas. Featuring topics such as crisis management, information security, and governance, this book is geared toward practitioners, academicians, government officials, military professionals, and industry professionals.

Information Security and Optimization maintains a practical perspective while offering theoretical explanations. The book explores concepts that are essential for academics as well as organizations. It discusses aspects of techniques and tools—definitions, usage, and analysis—that are invaluable for scholars ranging from those just beginning in the field to established experts. What are the policy standards? What are vulnerabilities and how can one patch them? How can data be transmitted securely? How can data in the cloud or cryptocurrency in the blockchain be secured? How can algorithms be optimized? These are some of the possible queries that are answered here effectively using examples from real life and case studies. Features: A wide range of case studies and examples derived from real-life scenarios that map theoretical explanations with real incidents. Descriptions of security tools related to digital forensics with their unique features, and the working steps for acquiring hands-on experience. Novel contributions in designing organization security policies and lightweight cryptography. Presentation of real-world use of blockchain technology and biometrics in cryptocurrency and personalized authentication systems. Discussion and analysis of security in the cloud that is important because of extensive use of cloud services to meet organizational and research demands such as data storage and computing requirements. Information Security and Optimization is equally helpful for undergraduate and postgraduate students as well as for researchers working in the domain. It can be recommended as a reference or textbook for courses related to cybersecurity.

Provides statistical modeling and simulating approaches to address the needs for intrusion detection and protection. Covers topics such as network traffic data, anomaly intrusion detection, and prediction events.

Information security issues impact all organizations; however measures used to implement effective measures are often viewed as a businesses barrier costing a great deal of money. This practical title clearly explains the approaches that most organizations can consider and implement which helps turn Information Security management into an approachable, effective and well-understood tool. It covers: The quality requirements an organization may have for information; The risks associated with these quality requirements; The countermeasures that are necessary to mitigate these risks; Ensuring business continuity in the event of a disaster; When and whether to report incidents outside the organization. All information security concepts in this book are based on the ISO/IEC 27001 and ISO/IEC 27002 standards. But the text also refers to the other relevant international standards for information security. The text is structures as follows: Fundamental Principles of Security and Information security and Risk management. Architecture, processes and information, needed for basic understanding of what information security is about. Business Assets are discussed. Measures that can be taken to protect information assets. (Physical measures, technical measures and finally the organizational measures.) The book also contains many Case Studies which usefully demonstrate how theory translates into an operating environment This book is primarily developed as a study book for anyone who wants to

pass the ISFS (Information Security Foundation) exam of EXIN. In an appendix an ISFS model exam is given, with feedback to all multiple choice options, so that it can be used as a training for the 'real' ISFS exam.

The book has two parts and contains fifteen chapters. First part discussed the theories and foundations of information security. Second part covers the technologies and application of security.

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.

Software developers need to worry about security as never before. They need clear guidance on safe coding practices, and that's exactly what this book delivers. The book does not delve deep into theory, or rant about the politics of security. Instead, it clearly and simply lays out the most common threats that programmers need to defend against. It then shows programmers how to make their defense. The book takes a broad focus, ranging over SQL injection, worms and buffer overflows, password security, and more. It sets programmers on the path towards successfully defending against the entire gamut of security threats that they might face.

This book is intended for everyone in an organization who wishes to have a basic understanding of information security. Knowledge about information security is important to all employees. It makes no difference if you work in a profit- or non-profit organization because the risks that organizations face are similar for all organizations.It clearly explains the approaches that most organizations can consider and implement which helps turn Information Security management into an approachable, effective and well-understood tool. It covers: The quality requirements an organization may have for information; The risks associated with these quality requirements; The countermeasures that are necessary to mitigate these risks; Ensuring business continuity in the event of a disaster; When and whether to report incidents outside the organization.The information security concepts in this revised edition are based on the ISO/IEC27001:2013 and ISO/IEC27002:2013 standards. But the text also refers to the other relevant international standards for information security. The text is structured as

follows: Fundamental Principles of Security and Information security and Risk management. Architecture, processes and information, needed for basic understanding of what information security is about. Business Assets are discussed. Measures that can be taken to protect information assets. (Physical measures, technical measures and finally the organizational measures.)The primary objective of this book is to achieve awareness by students who want to apply for a basic information security examination. It is a source of information for the lecturer who wants to question information security students about their knowledge. Each chapter ends with a case study. In order to help with the understanding and coherence of each subject, these case studies include questions relating to the areas covered in the relevant chapters. Examples of recent events that illustrate the vulnerability of information are also included.This book is primarily developed as a study book for anyone who wants to pass the ISFS (Information Security Foundation) exam of EXIN. In an appendix an ISFS model exam is given, with feedback to all multiple choice options, so that it can be used as a training for the real ISFS exam.

Building a Practical Information Security Program provides users with a strategic view on how to build an information security program that aligns with business objectives. The information provided enables both executive management and IT managers not only to validate existing security programs, but also to build new business-driven security programs. In addition, the subject matter supports aspiring security engineers to forge a career path to successfully manage a security program, thereby adding value and reducing risk to the business. Readers learn how to translate technical challenges into business requirements, understand when to "go big or go home," explore in-depth defense strategies, and review tactics on when to absorb risks. This book explains how to properly plan and implement an infosec program based on business strategy and results. Provides a roadmap on how to build a security program that will protect companies from intrusion Shows how to focus the security program on its essential mission and move past FUD (fear, uncertainty, and doubt) to provide business value Teaches how to build consensus with an effective business-focused program

Protect your business and family against cyber attacks Cybersecurity is the protection against the unauthorized or criminal use of electronic data and the practice of ensuring the integrity, confidentiality, and availability of information. Being "cyber-secure" means that a person or organization has both protected itself against attacks by cyber criminals and other online scoundrels, and ensured that it has the ability to recover if it is attacked. If keeping your business or your family safe from cybersecurity threats is on your to-do list, Cybersecurity For Dummies will introduce you to the basics of becoming cyber-secure! You'll learn what threats exist, and how to identify, protect against, detect, and respond to these threats, as well as how to recover if you have been breached! The who and why of cybersecurity threats Basic cybersecurity concepts What to do to be cyber-secure Cybersecurity careers What to think about to stay cybersecure in the future Now is the time to identify vulnerabilities that may make you a victim of cyber-crime — and to defend yourself before it is too late.

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.

Foundations of Information SecurityA Straightforward IntroductionNo Starch Press

Understanding Homeland Security is a unique textbook on homeland security that blends the latest research from the areas of immigration policy, counterterrorism research, and border security with practical insight from homeland security experts and leaders such as former Secretaries of the Department of Homeland Security Tom Ridge and Janet Napolitano. The textbook also includes: A historical overview of the origins of the homeland security enterprise as well as its post-9/11 transformation and burgeoning maturity as a profession In-depth descriptions of the state, local, and federal government entities, such as the U.S. Department of Homeland Security, that enforce and carry out the nation’s homeland security laws and policies Detailed discussion of relevant, contemporary topics such as asylum and refugee affairs, cybersecurity and hacking, border security, transportation and aviation security, and emergency management policy A chapter on homeland security privacy and civil liberties issues Unique current affairs analysis of controversial topics such as the National Security Agency’s warrantless wiretapping program, Edward Snowden, the 2016 U.S. presidential election, Russian cyberhacking efforts, and Black Lives Matter Advice, guidance, and insight for students through interviews with homeland security leaders as well as terrorism experts such as Bruce Hoffmann and biowarfare specialists such as Dr. Rebecca Katz The target audience for this text is advanced undergraduate or entry-level graduate students in criminology, intelligence analysis, public policy, public affairs, international affairs, or law programs. This textbook meets requirements for entry-level introductory courses in homeland security.

This is a graduate textbook of advanced tutorials on the theory of cryptography and computational complexity. In particular, the chapters explain aspects of garbled circuits, public-key cryptography, pseudorandom functions, one-way functions, homomorphic encryption, the simulation proof technique, and the complexity of differential privacy. Most chapters progress methodically through motivations, foundations, definitions, major results, issues surrounding feasibility, surveys of recent developments, and suggestions for further study. This book honors Professor Oded Goldreich, a pioneering scientist, educator, and mentor. Oded was instrumental in laying down the foundations of cryptography, and he inspired the contributing authors, Benny Applebaum, Boaz Barak, Andrej Bogdanov, Iftach Haitner, Shai Halevi, Yehuda Lindell, Alon Rosen, and Salil Vadhan, themselves leading researchers on the theory of cryptography and computational complexity. The book is appropriate for graduate tutorials and seminars, and for self-study by experienced researchers, assuming prior knowledge of the theory of cryptography.

"A much-needed service for society today. I hope this book reaches information managers in the organization now vulnerable to hacks that are stealing corporate

information and even holding it hostage for ransom." – Ronald W. Hull, author, poet, and former professor and university administrator A comprehensive entity security program deploys information asset protection through stratified technological and non-technological controls. Controls are necessary for counteracting threats, opportunities, and vulnerabilities risks in a manner that reduces potential adverse effects to defined, acceptable levels. This book presents a methodological approach in the context of normative decision theory constructs and concepts with appropriate reference to standards and the respective guidelines. Normative decision theory attempts to establish a rational framework for choosing between alternative courses of action when the outcomes resulting from the selection are uncertain. Through the methodological application, decision theory techniques can provide objectives determination, interaction assessments, performance estimates, and organizational analysis. A normative model prescribes what should exist according to an assumption or rule.

"This book is intended for everyone in an organization who wishes to have a basic understanding of information security. Knowledge about information security is important to all employees. It makes no difference if you work in a profit- or non-profit organization because the risks that organizations face are similar for all organizations. It clearly explains the approaches that most organizations can consider and implement which helps turn Information Security management into an approachable, effective and well-understood tool. It covers: The quality requirements an organization may have for information; The risks associated with these quality requirements; The countermeasures that are necessary to mitigate these risks; Ensuring business continuity in the event of a disaster; When and whether to report incidents outside the organization. The information security concepts in this revised edition are based on the ISO/IEC27001:2013 and ISO/IEC27002:2013 standards. But the text also refers to the other relevant international standards for information security. The text is structured as follows: Fundamental Principles of Security and Information security and Risk management. Architecture, processes and information, needed for basic understanding of what information security is about. Business Assets are discussed. Measures that can be taken to protect information assets. (Physical measures, technical measures and finally the organizational measures.) The primary objective of this book is to achieve awareness by students who want to apply for a basic information security examination. It is a source of information for the lecturer who wants to question information security students about their knowledge. Each chapter ends with a case study. In order to help with the understanding and coherence of each subject, these case studies include questions relating to the areas covered in the relevant chapters. ""

This book on computer security threats explores the computer security threats and includes a broad set of solutions to defend the computer systems from these threats. The book is triggered by the understanding that digitalization and

growing dependence on the Internet poses an increased risk of computer security threats in the modern world. The chapters discuss different research frontiers in computer security with algorithms and implementation details for use in the real world. Researchers and practitioners in areas such as statistics, pattern recognition, machine learning, artificial intelligence, deep learning, data mining, data analytics and visualization are contributing to the field of computer security. The intended audience of this book will mainly consist of researchers, research students, practitioners, data analysts, and business professionals who seek information on computer security threats and its defensive measures.

Written by a team of experts at the forefront of the cyber-physical systems (CPS) revolution, this book provides an in-depth look at security and privacy, two of the most critical challenges facing both the CPS research and development community and ICT professionals. It explores, in depth, the key technical, social, and legal issues at stake, and it provides readers with the information they need to advance research and development in this exciting area. Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon the seamless integration of computational algorithms and physical components. Advances in CPS will enable capability, adaptability, scalability, resiliency, safety, security, and usability far in excess of what today's simple embedded systems can provide. Just as the Internet revolutionized the way we interact with information, CPS technology has already begun to transform the way people interact with engineered systems. In the years ahead, smart CPS will drive innovation and competition across industry sectors, from agriculture, energy, and transportation, to architecture, healthcare, and manufacturing. A priceless source of practical information and inspiration, Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications is certain to have a profound impact on ongoing R&D and education at the confluence of security, privacy, and CPS.

This textbook presents a practical introduction to information security using the Competency Based Education (CBE) method of teaching. The content and ancillary assessment methods explicitly measure student progress in the three core categories: Knowledge, Skills, and Experience, giving students a balance between background knowledge, context, and skills they can put to work. Students will learn both the foundations and applications of information systems security; safeguarding from malicious attacks, threats, and vulnerabilities; auditing, testing, and monitoring; risk, response, and recovery; networks and telecommunications security; source code security; information security standards; and compliance laws. The book can be used in introductory courses in security (information, cyber, network or computer security), including classes that don't specifically use the CBE method, as instructors can adjust methods and ancillaries based on their own preferences. The book content is also aligned with the Cybersecurity Competency Model, proposed by department of homeland security. The author is an active member of The National Initiative for

Cybersecurity Education (NICE), which is led by the National Institute of Standards and Technology (NIST). NICE is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development.

Managing Information Security offers focused coverage of how to protect mission critical systems, and how to deploy security management systems, IT security, ID management, intrusion detection and prevention systems, computer forensics, network forensics, firewalls, penetration testing, vulnerability assessment, and more. It offers in-depth coverage of the current technology and practice as it relates to information security management solutions. Individual chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. Chapters contributed by leaders in the field covering foundational and practical aspects of information security management, allowing the reader to develop a new level of technical expertise found nowhere else Comprehensive coverage by leading experts allows the reader to put current technologies to work Presents methods of analysis and problem solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

Developing secure software requires the integration of numerous methods and tools into the development process, and software design is based on shared expert knowledge, claims, and opinions. Empirical methods, including data analytics, allow extracting knowledge and insights from the data that organizations collect from their processes and tools, and from the opinions of the experts who practice these processes and methods. This book introduces the reader to the fundamentals of empirical research methods, and demonstrates how these methods can be used to hone a secure software development lifecycle based on empirical data and published best practices.

"This book offers comprehensive explanations of topics in computer system security in order to combat the growing risk associated with technology"--Provided by publisher.

Anyone with a computer has heard of viruses, had to deal with several, and has been struggling with spam, spyware, and disk crashes. This book is intended as a starting point for those familiar with basic concepts of computers and computations and who would like to extend their knowledge into the realm of computer and network security. Its comprehensive treatment of all the major areas of computer security aims to give readers a complete foundation in the field of Computer Security. Exercises are given throughout the book and are intended to strengthening the reader's knowledge - answers are also provided. Written in a clear, easy to understand style, aimed towards advanced undergraduates and non-experts who want to know about the security problems confronting them everyday. The technical level of the book is low and requires no mathematics, and only a basic concept of computers and computations. Foundations of Computer Security will be an invaluable tool for students and professionals alike.

This book is written for the first security hire in an organization, either an individual moving into this role from within the organization or hired into the role. More and more, organizations are realizing that information security requires a dedicated team with leadership distinct from information technology, and often the people who are placed into those positions have no idea where to start or how to prioritize. There are many issues competing for their attention, standards that say do this or do that, laws, regulations, customer demands, and no guidance on what is actually effective. This book offers guidance on approaches that work for how you prioritize and build a comprehensive information security program that protects your organization. While most books targeted at information security professionals explore specific subjects with deep expertise, this book explores the depth and breadth of the field. Instead of exploring a technology such as cloud security or a technique such as risk analysis, this book places those into the larger context of how to meet an organization's needs, how to prioritize, and what success looks like. Guides to the maturation of practice are offered, along with pointers for each topic on where to go for an in-depth exploration of each topic. Unlike more typical books on information security that advocate a single perspective, this book explores competing perspectives with an eye to providing the pros and cons of the different approaches and the implications of choices on implementation and on maturity, as often a choice on an approach needs to change as an organization grows and matures.