Iso Iec 27003 Gammassl

Internet Protocol (IP) networks increasingly mix traditional data assets with traffic related to voice, entertainment, industrial process controls, metering, and more. Due to this convergence of content, IP networks are emerging as extremely vital infrastructure components, requiring greater awareness and better security and management. Off
Implement a robust SIEM system Effectively manage the security information and events produced by your network with help from this authoritative guide. Written by IT security experts, Security Information and Event Management (SIEM) Implementation shows you how to deploy SIEM technologies to monitor, identify, document, and respond to security threats and reduce false-positive alerts. The book explains how to implement SIEM products from different vendors, and discusses the strengths, weaknesses, and advanced tuning of these systems. You'll also learn how to use SIEM capabilities for business intelligence. Real-world case studies are included in this comprehensive resource. Assess your organization's business models, threat models, and regulatory compliance requirements Determine the necessary SIEM components for small- and medium-size businesses Understand SIEM anatomy—source device, log collection, parsing/normalization of logs, rule engine, log storage, and event monitoring Develop an effective incident response program Use the inherent capabilities of your SIEM system for business intelligence Develop filters and correlated event rules to reduce false-positive alerts Implement AlienVault's Open Source Security Information Management (OSSIM) Deploy the Cisco Monitoring Analysis and Response System (MARS) Configure and use the Q1 Labs QRadar SIEM system Implement ArcSight Enterprise Security Management (ESM) v4.5 Develop your SIEM security analyst skills
The IT Security Governance Guidebook with Security Program Metrics on CD-ROM provides clear and concise explanations of key issues in information protection, describing the basic structure of information protection and enterprise protection programs. Including graphics to support the information in the text, this book includes both an overview of material as well as detailed explanations of specific issues. The accompanying CD-ROM offers a collection of metrics, formed from repeatable and comparable measurement, that are designed to correspond to the enterprise security governance model provided in the text, allowing an enterprise to measure its overall information protection program.
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.
While information security is an ever-present challenge for all types of organizations today, most focus on providing security without addressing the necessities of staff, time, or budget in a practical manner. Information Security Cost Management offers a pragmatic approach to implementing information security, taking budgetary and real
The History of Information Security
Practical Hacking Techniques and Countermeasures
Wireless Crime and Forensic Investigation
Security Information and Event Management (SIEM) Implementation
Information Assurance Architecture
Information Security Architecture

Long gone are the days when a computer took up an entire room. Now we have computers at home, laptops that travel just about anywhere, and data networks that allow us to transmit information from virtually any location in a timely and efficient manner. What have these advancements brought us? Another arena for criminal activity. If someone wants to focus and target something, more than likely they will obtain what they want. We shouldn't expect it to be any different in cyberspace. Cyber Crime Field Handbook provides the details of investigating computer crime from soup to nuts. It covers everything from what to do upon arrival at the scene until the investigation is complete, including chain of evidence. You get easy access to information such as: Questions to ask the client Steps to follow when you arrive at the client's site Procedures for collecting evidence Details on how to use various evidence collection and analysis tools How to recover lost passwords or documents that are password protected Commonly asked questions with appropriate answers Recommended reference materials A case study to see the computer forensic tools in action Commonly used UNIX/Linux commands Port number references for various services and applications Computer forensic software tools commands synopsis Attack signatures Cisco PIX firewall commands We now have software and hardware to protect our data communication systems. We have laws that provide law enforcement more teeth to take a bite out of cyber crime. Now we need to combine understanding investigative techniques and technical knowledge of cyberspace. That's what this book does. Cyber Crime Field Handbook provides the investigative framework, a knowledge of how cyberspace really works, and the tools to investigate cyber crime...tools that tell you the who, where, what, when, why, and how.
As regulation and legislation evolve, the critical need for cost-effective and efficient IT audit and monitoring solutions will continue to grow. Audit and Trace Log Management: Consolidation and Analysis offers a comprehensive introduction and explanation of requirements and problem definition, and also delivers a multidimensional solution set with broad applicability across a wide range of organizations. Itprovidesa wealth of information in the form of processwalkthroughs. These include problem determination, requirements gathering,scope definition, risk assessment, compliance objectives, systemdesign and architecture, implementation and operational challenges, productand solution evaluation, communication plans, project managementchallenges, and determining Return on Investment (ROI). By using templates, tools, and samples that enhance your understanding of processes and solution sets, the author successfully emphasizes the core themes of the book. He also includes many diagrams throughout his discussion that aid in a clear communication of process and solution recommendations. This volume enables you to gain the knowledge, perspective, and insight needed to independently implement a successful audit and monitoring management system tailored to the unique requirements of your organization.
Principles of Information SecurityCengage Learning
Discover the latest trends, developments and technology in information security today with Whitman/Mattord's market-leading PRINCIPLES OF INFORMATION SECURITY, 7th Edition. Designed specifically to meet the needs of those studying information systems, this edition's balanced focus addresses all aspects of information security, rather than simply offering a technical control perspective. This overview explores important terms and examines what is needed to manage an effective information security program. A new module details incident response and detection strategies. In addition, current, relevant updates highlight the latest practices in security operations as well as legislative issues, information management toolsets and digital forensics. Coverage of the most recent policies and guidelines that correspond to federal and international standards further prepare you for success both in information systems and as a business decision-maker. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
The Hands-On Information Security Lab Manual allows users to apply the basics of their introductory security knowledge in a hands-on environment with detailed exercises using Windows 2000, XP and Linux. This non-certification based lab manual includes coverage of scanning, OS vulnerability analysis and resolution firewalls, security maintenance, forensics, and more. A full version of the software needed to complete these projects is included on a CD with every text, so instructors can effortlessly set up and run labs to correspond with their classes. The Hands-On Information Security Lab Manual is a suitable resource for introductory, technical and managerial courses, and is a perfect supplement to the Principles of Information Security and Management of Information Security texts. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
The CISO Handbook
Information Security Risk Analysis, Second Edition
A Practical Guide to Securing Your Company
Measuring Regulatory Compliance, Operational Resilience, and ROI
Official (ISC)2 Guide to the CISSP CBK
Design, Implementation, Measurement, and Compliance
Information Security Architecture, Second Edition incorporates the knowledge developed during the past decade that has pushed the information security life cycle from infancy to a more mature, understandable, and manageable state. It simplifies security by providing clear and organized methods and by guiding you to the most effective resources available. In addition to the components of a successful Information Security Architecture (ISA) detailed in the previous edition, this volume also discusses computer incident/emergency response. The book describes in detail every one of the eight ISA components. Each chapter provides an understanding of the component and details how it relates to the other components of the architecture. The text also outlines how to establish an effective plan to implement each piece of the ISA within an organization. The second edition has been modified to provide security novices with a primer on general security methods. It has also been expanded to provide veteran security professionals with an understanding of issues related to recent legislation, information assurance, and the latest technologies, vulnerabilities, and responses.
Organizations rely on digital information today more than ever before. Unfortunately, that information is equally sought after by criminals. New security standards and regulations are being implemented to deal with these threats, but they are very broad and organizations require focused guidance to adapt the guidelines to their specific needs.
The security criteria of the International Standards Organization (ISO) provides an excellent foundation for identifying and addressing business risks through a disciplined security management process. Using security standards ISO 17799 and ISO 27001 as a basis, How to Achieve 27001 Certification: An Example of Applied Compliance Management helps an organization align its security and organizational goals so it can generate effective security, compliance, and management programs. The authors offer insight from their own experiences, providing questions and answers to determine an organization's information security strengths and weaknesses with respect to the standard. They also present step-by-step information to help an organization plan an implementation, as well as prepare for certification and audit. Security is no longer a luxury for an organization, it is a legislative mandate. A formal methodology that helps an organization define and execute an ISMS is essential in order to perform and prove due diligence in upholding stakeholder interests and legislative compliance. Providing a good starting point for novices, as well as finely tuned nuances for seasoned security professionals, this book is an invaluable resource for anyone involved with meeting an organization's security, certification, and compliance needs.
While it has become increasingly apparent that individuals and organizations need a security metrics program, it has been exceedingly difficult to define exactly what that means in a given situation. There are hundreds of metrics to choose from and an organization's mission, industry, and size will affect the nature and scope of the task as well as
Examining computer security from the hacker's perspective, Practical Hacking Techniques and Countermeasures employs virtual computers to illustrate how an attack is executed, including the script, compilation, and results. It provides detailed screen shots in each lab for the reader to follow along in a step-by-step process in order to duplicate an
Hands-On Information Security Lab Manual
Information Security Fundamentals
Fundamentals of Identity Management
How to Achieve 27001 Certification
Database and Applications Security
The Security Risk Assessment Handbook

ROADMAP TO INFORMATION SECURITY: FOR IT AND INFOSEC MANAGERS provides a solid overview of information security and its relationship to the information needs of an organization. Content is tailored to the unique needs of information systems professionals who find themselves brought in to the intricacies of information security responsibilities. The book is written for a wide variety of audiences looking to step up to emerging security challenges, ranging from students to experienced professionals. This book is designed to guide the information technology manager in dealing with the challenges associated with the security aspects of their role, providing concise guidance on assessing and improving an organization's security. The content helps IT managers to handle an assignment to an information security role in ways that conform to expectations and requirements, while supporting the goals of the manager in building and maintaining a solid information security program. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
A complete, up-to-date revision of the leading CISSP training resource from the #1 name in IT security certification and training, Shon Harris Fully revised for the latest release of the Certified Information Systems Security Professional exam, this comprehensive, up-to-date resource covers all 10 CISSP exam domains developed by the International Information Systems Security Certification Consortium (ISC2). This authoritative exam guide features learning objectives at the beginning of each chapter, exam tips, practice questions, and in-depth explanations. Written by the leading expert in IT security certification and training, CISSP All-in-One Exam Guide, Sixth Edition helps you pass the exam with ease and also serves as an essential on-the-job reference. Covers all 10 CISSP domains: Information security governance and risk management Access control Security architecture and design Physical and environmental security Telecommunications and network security Cryptography Business continuity and disaster recovery Legal, regulations, compliance, and investigations Software development security Security operations Electronic content includes: 1400+ practice exam questions in a Windows-based test engine with a new custom exam generation feature that allows you to practice by domain or take a complete CISSP practice exam Video training module from Shon Harris—single domain
The CISO Toolkit is a collection of books and software for the Chief Information Security Officer (CISO) of a substantial enterprise. The governance guidebook describes the basic structure of information protection and protection programs in enterprises. It is designed to provide clear and concise explanations of key issues in information protection with pictures that allow the material to be presented, referenced, and understood. Whether you are a professional licensed investigator or have been tasked by your employer to conduct an internal investigation, Investigations in the Workplace gives you a powerful mechanism for engineering the most successful workplace investigations possible. Corporate investigator Eugene Ferraro, CPP, CFE has drawn upon his twenty-four years of practical experience to craft a book that dispels the myths and troublesome theories promulgated by the uninitiated. He provides the back-story behind the methodology, rationale, and gritty practices that have made his workplace investigations soar. But most importantly, he shares this knowledge with you. The book is designed for easy reading and use. Although every page is filled with useful information, you do not need to read the book cover to cover. The exhaustive table of contents, innumerable references, and expansive index allow you to quickly find the immediate information you need. The Applied Strategies chapter shows you how to conduct a particular type of investigation and the action steps involved. To help capture salient points and simplify the learning process, the text is sprinkled with brief Tips and Traps that provide quick and easy lessons on how to make the best use of the information in a particular section. Few workplace activities invoke so much risk and at the same time, so much opportunity, as workplace investigations. A combination of skill, experience, and luck: successful workplace investigations are complex undertakings. An improperly conducted workplace investigation can be expensive and ruin the careers of everyone who touches it. Exploring modern investigative technique and strategies, this book gives you new solutions you need and provides the keys to master even the most complex workplace investigation.
Data processing, Computers, Management, Data security, Data storage protection, Risk assessment, Risk analysis, Data management, Information exchange, Business continuity, Anti-burglar measures, Documents, IT and Information Management: Information Security
Consolidation and Analysis
Testing Code Security
Complete Guide to Security and Privacy Metrics
Guide to Firewalls and Network Security
Information Security
Crisis Management Planning and Execution

Managing an Information Security and Privacy Awareness and Training Program provides a starting point and an all-in-one resource for infosec and privacy education practitioners who are building programs for their organizations. The author applies knowledge obtained through her work in education, creating a comprehensive resource of nearly everything involved with managing an infosec and privacy training course. This book includes examples and tools from a wide range of businesses, enabling readers to select effective components that will be beneficial to their enterprises. The text progresses from the inception of an education program through development, implementation, delivery, and evaluation.
This is the first book to provide an in-depth coverage of all the developments, issues and challenges in secure databases and applications. It provides directions for data and application security, including securing emerging applications such as bioinformatics, stream information processing and peer-to-peer computing. Divided into eight sections,
Crisis management planning refers to the methodology used by executives to respond to and manage a crisis and is an integral part of a business resumption plan. Crisis Management Planning and Execution explores in detail the concepts of crisis management planning, which involves a number of crises other than physical disaster. Defining th
User identification and authentication are essential parts of information security. Users must authenticate as they access their computer systems at work or at home every day. Yet do users understand how and why they are actually being authenticated, the security level of the authentication mechanism that they are using, and the potential impacts o
The CISO Handbook: A Practical Guide to Securing Your Company provides unique insights and guidance into designing and implementing an information security program, delivering true value to the stakeholders of a company. The authors present several essential high-level concepts before building a robust framework that will enable you to map the concepts to your company's environment. The book is presented in chapters that follow a consistent methodology – Assess, Plan, Design, Execute, and Report. The first chapter, Assess, identifies the elements that drive the need for infosec programs, enabling you to conduct an analysis of your business and regulatory requirements. Plan discusses how to build the foundation of your program, allowing you to develop an executive mandate, reporting metrics, and an organizational matrix with defined roles and responsibilities. Design demonstrates how to construct the policies and procedures to meet your identified business objectives, explaining how to perform a gap analysis between the existing environment and the desired end-state, define project requirements, and assemble a rough budget. Execute emphasizes the creation of a successful execution model for the implementation of security projects against the backdrop of common business constraints. Report focuses on communicating back to the external and internal stakeholders with information that fits the various audiences. Each chapter begins with an Overview, followed by Foundation Concepts that are critical success factors to understanding the material presented. The chapters also contain a Methodology section that explains the steps necessary to achieve the goals of the particular chapter.
CISSP All-in-One Exam Guide, Eighth Edition
Cyber Crime Investigator's Field Guide
An Example of Applied Compliance Management
A Comprehensive Handbook
802.1X Port-Based Authentication
Securing Converged IP Networks

Security is always a concern with any new technology. When we think security we typically think of stopping an attacker from breaking in or gaining access. From short text messaging to investigating war, this book explores all aspects of wireless technology, including how it is used in daily life and how it might be used in the future. It provides a one-stop resource on the types of wireless crimes that are being committed and the forensic investigation techniques that are used for wireless devices and wireless networks. The author provides a solid understanding of modern wireless technologies, wireless security techniques, and wireless crime techniques, and shows how to conduct forensic analysis on wireless devices and networks. Each chapter, while part of a greater whole, is self-contained for quick comprehension.
Firewalls are among the best-known security tools in use today, and their critical role in information security continues to grow. However, firewalls are most effective when they are backed by effective security planning, a well-designed security policy, and when they work in concert with anti-virus software, intrusion detection systems, and other tools. This book aims to explore firewalls in the context of these other elements, providing readers with a solid, in-depth introduction to firewalls that focuses on both managerial and technical aspects of security. Coverage includes packet filtering, authentication, proxy servers, encryption, bastion hosts, virtual private networks (VPNs), log file maintenance, and intrusion detection systems. The second edition offers updated content and brand new material, from enhanced coverage of non-firewall subjects like information and network security to an all-new section dedicated to intrusion detection in the context of incident response.
MyITCertificationlabs should be used in an instructor led classroom environment and are not intended for individual self-study myITcertificationlabs: CISSP is an easy-to-use exam preparation engine that tests your readiness and teaches you what you need to know to achieve (ISC)2's globally recognized CISSP credential. This web-based service has a comprehensive database of more than 500 exam questions. CISSP MyLab tests you on each exam objective, provides you with a customized learning plan complete with feedback on areas where you need further study, and then directs you to video instruction to help you fill in gaps in your knowledge. Resources from the popular CISSP Exam Cram, Second Edition, as well as instructional videos taken from instructor Shon Harris's legendary five-day boot camps, provide all the instruction you need to prepare for the CISSP exam. Once you've assessed your readiness and completed additional instruction, you can re-test your knowledge to ensure that you are ready for the exam and on your way to giving your IT career a boost!
The huge proliferation of security vulnerability exploits, worms, and viruses place an incredible drain on both cost and confidence for manufacturers and consumers. The release of trustworthy code requires a specific set of skills and techniques, but this information is often dispersed and decentralized, encrypted in its own jargon and terminology,
The risk management process supports executive decision-making, allowing managers and owners to perform their fiduciary responsibility of protecting the assets of their enterprises. This crucial process should not be a long, drawn-out affair. To be effective, it must be done quickly and efficiently. Information Security Risk Analysis, Second Edition enables CIOs, CSOs, and MIS managers to understand when, why, and how risk assessments and analyses can be conducted effectively. This book discusses the principle of risk management and its three key elements: risk analysis, risk assessment, and vulnerability assessment. It examines the differences between quantitative and qualitative risk assessment, and details how various types of qualitative risk assessment can be applied to the assessment process. The text offers a thorough discussion of recent changes to FRAAP and the need to develop a pre-screening method for risk assessment and business impact analysis.
Handbook for ISO/IEC 27001
Governance Guidebook
Readings & Cases in Information Security: Law & Ethics
The Official (ISC)2 CISSP CBK Reference

IT Security Governance Guidebook with Security Program Metrics on CD-ROM

The only official, comprehensive reference guide to the CISSP Thoroughly updated for 2021 and beyond, this is the authoritative common body of knowledge (CBK) from (ISC)2 for information security professionals charged with designing, engineering, implementing, and managing the overall information security program to protect organizations from increasingly sophisticated attacks. Vendor neutral and backed by (ISC)2, the CISSP credential meets the stringent requirements of ISO/IEC Standard 17024. This CBK covers the current eight domains of CISSP with the necessary depth to apply them to the daily practice of information security. Revised and updated by a team of subject matter experts, this comprehensive reference covers all of the more than 300 CISSP objectives and sub-objectives in a structured format with: Common and good practices for each objective Common vocabulary and definitions References to widely accepted computing standards Highlights of successful approaches through case studies Whether you've earned your CISSP credential or are looking for a valuable resource to help advance your security career, this comprehensive guide offers everything you need to apply the knowledge of the most recognized body of influence in information security
Publisher's Note: Products purchased from Third Party sellers are not guaranteed by the publisher for quality, authenticity, or access to any online entitlements included with the product. A new edition of Shon Harris' bestselling exam prep guide—fully updated for the new CISSP 2018 Common Body of Knowledge Thoroughly updated for the latest release of the Certified Information Systems Security Professional exam, this comprehensive resource covers all exam domains, as well as the new 2018 CISSP Common Body of Knowledge developed by the International Information Systems Security Certification Consortium (ISC)2®. CISSP All-in-One Exam Guide, Eighth Edition features learning objectives at the beginning of each chapter, exam tips, practice questions, and in-depth explanations. Written by leading experts in information security certification and training, this completely up-to-date self-study system helps you pass the exam with ease and also serves as an essential on-the-job reference. Covers all 8 CISSP domains: •Security and risk management•Asset security•Security architecture and engineering•Communication and network security•Identity and access management•Security assessment and testing•Security operations•Software development security Digital content includes: •1400+ practice questions, including new hot spot and drag-and-drop questions•Flashcards
As a result of a rigorous, methodical process that (ISC) follows to routinely update its credential exams, it has announced that enhancements will be made to both the Certified Information Systems Security Professional (CISSP) credential, beginning April 15, 2015. (ISC) conducts this process on a regular basis to ensure that the examinations and
Guide to Optimal Operational Risk and Basel II presents the key aspects of operational risk management that are also aligned with the Basel II requirements. This volume provides detailed guidance for the design and implementation of an efficient operational risk management system. It contains all elements of assessment, including operational risk i
Readings and Cases in Information Security: Law and Ethics provides a depth of content and analytical viewpoint not found in many other books. Designed for use with any Cengage Learning security text, this resource offers readers a real-life view of information security management, including the ethical and legal issues associated with various on-the-job experiences. Included are a wide selection of foundational readings and scenarios from a variety of experts to give the reader the most realistic perspective of a career in information security. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
Principles of Incident Response and Disaster Recovery
Principles of Information Security
The Chief Information Security Officer's Toolkit
Information Security Risk Management
Intrusion Detection and VPNs
CISSP

The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments provides detailed insight into precisely how to conduct an information security risk assessment. Designed for security professionals and their customers who want a more in-depth understanding of the risk assessment process, this volume contains real-wor
Information Security professionals, managers of IT employees, business managers, organizational security officers, network administrators, students or Business and Information Systems, IT, Accounting, Criminal Justice or IS majors.
Information Security is usually achieved through a mix of technical, organizational and legal measures. These may include the application of cryptography, the hierarchical modeling of organizations in order to assure confidentiality, or the distribution of accountability and responsibility by law, among interested parties. The history of Information Security reaches back to ancient times and starts with the emergence of bureaucracy in administration and warfare. Some aspects, such as the interception of encrypted messages during World War II, have attracted huge attention, whereas other aspects have remained largely uncovered. There has never been any effort to write a comprehensive history. This is most unfortunate, because Information Security should be perceived as a set of communicating vessels, where technical innovations can make existing legal or organisational frame-works obsolete and a breakdown of political authority may cause an exclusive reliance on technical means. This book is intended as a first field-survey. It consists of twenty-eight contributions, written by experts in such diverse fields as computer science, law, or history and political science, dealing with episodes, organisations and technical developments that may considered to be exemplary or have played a key role in the development of this field. These include: the emergence of cryptology as a discipline during the Renaissance, the Black Chambers in 18th century Europe, the breaking of German military codes during World War II, the histories of the NSA and its Soviet counterparts and contemporary cryptology. Other subjects are: computer security standards, viruses and worms on the Internet, computer transparency and free software, computer crime, export regulations for encryption software and the privacy debate. - Interdisciplinary coverage of the history Information Security - Written by top experts in law, history, computer and information science - First comprehensive work in Information Security
Port-based authentication is a "network access control" concept in which a particular device is evaluated before being permitted to communicate with other devices located on the network. 802.1X Port-Based Authentication examines how this concept can be applied and the effects of its application to the majority of computer networks in existence today. 802.1X is a standard that extends the Extensible Authentication Protocol (EAP) over a Local Area Network (LAN) through a process called Extensible Authentication Protocol Over LANs (EAPOL). The text presents an introductory overview of port-based authentication including a description of 802.1X port-based authentication, a history of the standard and the technical documents published, and details of the connections among the three network components. It focuses on the technical aspect of 802.1X and the related protocols and components involved in implementing it in a network. The book provides an in-depth discussion of technology, design, and implementation with a specific focus on Cisco devices. Including examples derived from the 802.1X implementation, it also addresses troubleshooting issues in a Cisco environment. Each chapter contains a subject overview. Incorporating theoretical and practical approaches, 802.1X Port-Based Authentication seeks to define this complex concept in accessible terms. It explores various applications to today's computer networks using this particular network protocol.
Now that information has become the lifeblood of your organization, you must be especially vigilant about assuring it. The hacker, spy, or cyber-thief of today can breach any barrier if it remains unchanged long enough or has even the tiniest leak. In Information Assurance Architecture, Keith D. Willett draws on his over 25 years of technical, security, and business experience to provide a framework for organizations to align information assurance with the enterprise and their overall mission. The Tools to Protect Your Secrets from Exposure This work provides the security industry with the know-how to create a formal information assurance architecture that complements an enterprise architecture, systems engineering, and the enterprise life cycle management (ELCM). Information Assurance Architecture consists of a framework, a process, and many supporting tools, templates and methodologies. The framework provides a reference model for the consideration of security in many contexts and from various perspectives; the process provides direction on how to apply that framework. Mr. Willett teaches readers how to identify and use the right tools for the right job. Furthermore, he demonstrates a disciplined approach in thinking about, planning, implementing and managing security, emphasizing that solid solutions can be made impenetrable when they are seamlessly integrated with the whole of an enterprise. Understand the Enterprise Context This book covers many information assurance subjects, including disaster recovery and firewalls. The objective is to present security services and security mechanisms in the context of information assurance architecture, and in an enterprise context of managing business risk. Anyone who utilizes the concepts taught in these pages will find them to be a valuable weapon in the arsenal of information protection.
Integrating Information Security and Data Management
Information Security Cost Management
A Complete Guide for Performing Security Risk Assessments, Second Edition
An Integrated Approach to Security in the Organization, Second Edition
Mechanics of User Identification and Authentication
Managing an Information Security and Privacy Awareness and Training Program

PRINCIPLES OF INCIDENT RESPONSE & DISASTER RECOVERY, 2nd Edition presents methods to identify vulnerabilities within computer networks and the countermeasures that mitigate risks and damage. From market-leading content on contingency planning, to effective techniques that minimize downtime in an emergency, to curbing losses after a breach, this text is the resource needed in case of a network intrusion. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
Guide to Optimal Operational Risk and BASEL II
Roadmap to Information Security: For IT and Infosec Managers
CISSP All-in-One Exam Guide, 6th Edition
Audit and Trace Log Management
Investigations in the Workplace
Management of Information Security