Bs Iso Iec 27035 2011 Information Technology Security Techniques Information Security Incident Management

Handbook of Digital Forensics of Multimedia Data and DevicesJohn Wiley & Sons
This is the first digital forensics book that covers the complete lifecycle of digital evidence and the chain of custody. This comprehensive handbook includes international procedures, best practices, compliance, and a companion web site with downloadable forms. Written by world-renowned digital forensics experts, this book is a must for any digital forensics lab. It provides anyone who handles digital evidence with a guide to proper procedure throughout the chain of custody--from incident response through analysis in the lab. A step-by-step guide to designing, building and using a digital forensics lab A comprehensive guide for all roles in a digital forensics laboratory Based on international standards and certifications
This book constitutes the refereed proceedings of the 28th IFIP TC 11 International Information Security and Privacy Conference, SEC 2013, held in Auckland, New Zealand, in July 2013. The 31 revised full papers presented were carefully reviewed and selected from 83 submissions. The papers are organized in topical sections on malware, authentication and authorization, network security/cryptography, software security, policy compliance and obligations, privacy protection, risk analysis and security metrics, social engineering, and security management/forensics.
Microsystems are an important success factor in the automobile industry. In order to fulfil the customers'requests for safety convenience and vehicle economy, and to satisfy environmental requirements, microsystems are becoming indispensable. Thus a large number of microsystem applications came into the discussion. With the international conference AMAA 2001, VDI/VDE-IT provides a platform for the discussion of all MST relevant components for automotive applications. The conference proceedings gather the papers by authors from automobile suppliers and manufacrurers.
This book covers the various types of cyber threat and explains what you can do to mitigate these risks and keep your data secure. The book is crucial reading for businesses wanting to better understand security risks and ensure the safety of organisational and customer data.
CompTIA Cybersecurity Analyst (CySA+) CS0-002 Cert Guide is a best-of-breed exam study guide. Expert technology instructor and certification author Troy McMillan shares preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. The book presents you with an organized test-preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your final study plan. The companion website contains the powerful Pearson Test Prep practice test software, complete with hundreds of exam-realistic questions. The assessment engine offers you a wealth of customization options and reporting features, laying out a complete assessment of your knowledge to help you focus your study where it is needed most. Well regarded for its level of detail, assessment features, and challenging review questions and exercises, this CompTIA approved study guide helps you master the concepts and techniques that will enable you to succeed on the exam the first time. The CompTIA approved study guide helps you master all the topics on the CySA+ exam, including: - Applying environmental reconnaissance - Analyzing results of network reconnaissance - Implementing responses and countermeasures - Implementing vulnerability management processes - Analyzing scan output and identifying common vulnerabilities - Identifying incident impact and assembling a forensic toolkit - Utilizing effective incident response processes - Performing incident recovery and post-incident response - Establishing frameworks, policies, controls, and procedures - Remediating identity- and access-related security issues - Architecting security and implementing compensating controls - Implementing application security best practices - Using cybersecurity tools and technologies
Includes circuit designs and explanations for projects you can build for sensors, solare cells, and magnet and magnet sensor projects. Includes many projects appropriate for science fairs.
Tematyka badawcza monografii obejmuje opis przedsi?wzi?? projektowych w logistyce, które s? zwi?zane z dzia?aniami poprawiaj?cymi zdrowotn? jako?? ?ycia obywateli poprzez zaprezentowanie koncepcji systemu logistycznego z rozwi?zaniami sprzyjaj?cymi realizacji trwa?ego, zrównowa?onego rozwoju w gospodarce odpadami zawieraj?cymi azbest. Na poziomie teoriopoznawczym wykorzystano transdyscyplinarne podej?cie do problemu badawczego w sze?ciu obszarach wkomponowanych w rozwi?zania koncepcyjne logistyki: 1) logistyk?, 2) zarz?dzanie interesariuszami, 3) modeli biznesu, 4) zrównowa?onego rozwoju, 5) zdrowia publicznego, 6) technologii informacyjno-komunikacyjnych. W warstwie aplikacyjnej przyj?to za?o?enie, ?e wolne tempo usuwania azbestu ze ?rodowiska wynika z barier zwi?zanych z niew?a?ciwym wykorzystaniem zasobów ludzkich, finansowych, rzeczowych, informacyjnych. Przedstawione wariantowe rozwi?zania ekologistyczne posiadaj? uzasadnienie biznesowe, uwzgl?dniaj? zasad? zrównowa?onego rozwoju i powinny skutkowa? efektywniejszym wykorzystaniem zasobów i zwi?zanych z nimi procesami logistycznymi w gospodarce odpadami niebezpiecznymi.
MANAGEMENT OF INFORMATION SECURITY, Fourth Edition gives readers an overview of information security and assurance using both domestic and international standards, all from a management perspective. Beginning with the foundational and technical components of information security, this edition then focuses on access control models, information security governance, and information security program assessment and metrics. The Fourth Edition is revised and updated to reflect changes in the field, including the ISO 27000 series, so as to prepare readers to succeed in the workplace. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
IT Security governance is becoming an increasingly important issue for all levels of a company. IT systems are continuously exposed to a wide range of threats, which can result in huge risks that threaten to compromise the confidentiality, integrity, and availability of information. This book will be of use to those studying information security, as well as those in industry.

Das Buch bietet einen praxisbezogenen Leitfaden für das Informationssicherheits-, IT- und Cyber-Risikomanagement im Unternehmen – es ist branchenneutral und nimmt Bezug auf relevante Konzepte und Standards des Risikomanagements und der Governance (z.B. COBIT, NIST SP 800-30 R1, ISO 31000, ISO 22301 und ISO/IEC 270xx-Reihe). Der Autor stellt integrierte Lösungsansätze in einem Gesamt-Risikomanagement vor. Dabei behandelt er systematisch, ausgehend von der Unternehmens-Governance, die fachspezifischen Risiken in einem beispielhaften Risikomanagement-Prozess. Der Leser erhält alles, was zur Beurteilung, Behandlung und Kontrolle dieser Risiken in der Praxis methodisch erforderlich ist. Diese 5. Auflage ist auf den aktuellen Stand der Compliance-Anforderungen und der Standardisierung angepasst und geht in einem zusätzlichen, neuen Kapitel speziell auf die Cyber-Risiken und deren Besonderheiten ein. Anhand von Beispielen wird ein Ansatz für das Assessment der Cyber-Risiken sowie in der Massnahmen zur adäquaten Behandlung gezeigt.

This book constitutes the refereed proceedings of the 19th International Conference on Engineering Applications of Neural Networks, EANN 2019, held in Xersonisos, Crete, Greece, in May 2019. The 35 revised full papers and 5 revised short papers presented were carefully reviewed and selected from 72 submissions. The papers are organized in topical sections on AI in energy management - industrial applications; biomedical - bioinformatics modeling; classification - learning; deep learning; deep learning - convolutional ANN; fuzzy - vulnerability - navigation modeling; machine learning modeling - optimization; ML - DL financial modeling; security - anomaly detection; 1st PEINT workshop.

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.

Dealing with the classical processes for textile dyeing, as well as with the preparation of the material before dyeing, this book also includes recent technological developments. Both theoretical and the practical aspects are covered in order to enable the students and the technicians to understand the processes clearly.

Digital forensics and multimedia forensics are rapidly growing disciplines whereby electronic information is extracted and interpreted for use in a court of law. These two fields are finding increasing importance in law enforcement and the investigation of cybercrime as the ubiquity of personal computing and the internet becomes ever-more apparent. Digital forensics involves investigating computer systems and digital artefacts in general, while multimedia forensics is a sub-topic of digital forensics focusing on evidence extracted from both normal computer systems and special multimedia devices, such as digital cameras. This book focuses on the interface between digital forensics and multimedia forensics, bringing two closely related fields of forensic expertise together to identify and understand the current state-of-the-art in digital forensic investigation. Both fields are expertly attended to by contributions from researchers and forensic practitioners specializing in diverse topics such as forensic authentication, forensic triage, forensic photogrammetry, biometric forensics, multimedia device identification, and image forgery detection among many others. Key features: Brings digital and multimedia forensics together with contributions from academia, law enforcement, and the digital forensics industry for extensive coverage of all the major aspects of digital forensics of multimedia data and devices Provides comprehensive and authoritative coverage of digital forensics of multimedia data and devices Offers not only explanations of techniques but also real-world and simulated case studies to illustrate how digital and multimedia forensics techniques work Includes a companion website hosting continually updated supplementary materials ranging from extended and updated coverage of standards to best practice guides, test datasets and more case studies

Tough Test Questions? Missed Lectures? Not Enough Time? Fortunately, there's Schaum's. This all-in-one-package includes more than 550 fully solved problems, examples, and practice exercises to sharpen your problem-solving skills. Plus, you will have access to 30 detailed videos featuring Math instructors who explain how to solve the most commonly tested problems--it's just like having your own virtual tutor! You'll find everything you need to build confidence, skills, and knowledge for the highest score possible. More than 40 million students have trusted Schaum's to help them succeed in the classroom and on exams. Schaum's is the key to faster learning and higher grades in every subject. Each Outline presents all the essential course information in an easy-to-follow, topic-by-topic format. Helpful tables and illustrations increase your understanding of the subject at hand. This Schaum's Outline gives you 563 fully solved problems Concise explanation of all course concepts Covers first-order, second-order, and nth-order equations Fully compatible with your classroom text, Schaum's highlights all the important facts you need to know. Use Schaum's to shorten your study time--and get your best test scores! Schaum's Outlines--Problem Solved.

For the past couple of years, network automation techniques that include software-defined networking (SDN) and dynamic resource allocation schemes have been the subject of a significant research and development effort. Likewise, network functions virtualization (NFV) and the foreseeable usage of a set of artificial intelligence techniques to facilitate the processing of customers' requirements and the subsequent design, delivery, and operation of the corresponding services are very likely to dramatically distort the conception and the management of networking infrastructures. Some of these techniques are being specified within standards developing organizations while others remain perceived as a "buzz" without any concrete deployment plans disclosed by service providers. An in-depth understanding and analysis of these approaches should be conducted to help internet players in making appropriate design choices that would meet their requirements as well as their customers. This is an important area of research as these new developments and approaches will inevitably reshape the internet and the future of technology. Design Innovation and Network Architecture for the Future Internet sheds light on the foreseeable yet dramatic evolution of internet design principles and offers a comprehensive overview on the recent advances in networking techniques that are likely to shape the future internet. The chapters provide a rigorous in-depth analysis of the promises, pitfalls, and other challenges raised by these initiatives, while avoiding any speculation on their expected outcomes and technical benefits. This book covers essential topics such as content delivery networks, network functions virtualization, security, cloud computing, automation, and more. This book will be useful for network engineers, software designers, computer networking professionals, practitioners, researchers, academicians, and students looking for a comprehensive research book on the latest advancements in internet design principles and networking techniques.

This proceedings book is the fourth edition of a series of works which features emergent research trends and recent innovations

related to smart city presented at the 5th International Conference on Smart City Applications SCA20 held in Safranbolu, Turkey. This book is composed of peer-reviewed chapters written by leading international scholars in the field of smart cities from around the world. This book covers all the smart city topics including Smart Citizenship, Smart Education, Smart Mobility, Smart Healthcare, Smart Mobility, Smart Security, Smart Earth Environment & Agriculture, Smart Economy, Smart Factory and Smart Recognition Systems. This book contains a special section intended for Covid-19 pandemic researches. This book edition is an invaluable resource for courses in computer science, electrical engineering and urban sciences for sustainable development.
Cyber attacks and IT breakdowns threaten every organization. The incidents accumulate and often form the prelude to complex, existence-threatening crises. This book helps not only to manage them, but also to prepare for and prevent cyber crises. Structured in a practical manner, it is ideally suited for crisis team members, communicators, security, IT and data protection experts on a day-to-day basis. With numerous illustrations and checklists. This book is a translation of the original German 1st edition Cyber Crisis Management by Holger Kaschner, published by Springer Fachmedien Wiesbaden GmbH, part of Springer Nature in 2020. The translation was done with the help of artificial intelligence (machine translation by the service DeepL.com). A subsequent human revision was done primarily in terms of content, so that the book will read stylistically differently from a conventional translation. Springer Nature works continuously to further the development of tools for the production of books and on the related technologies to support the authors.
????? ???????????? ? ????????? ????????????? ?????????? ISO/IEC 27k, ???????????? ?????????? ? ??????? ???? (??????? ?????????? ????????????? ?????????????), ??????? ?????????? ???? ? ????????? ?????????? ??????? ????????????? ???????????? ? ?????????? ?????????????.??????????? ???-???????? ??????: http://cryptohistory.ru
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
This book constitutes the refereed proceedings of the First International Conference on Computer Science, Engineering and Information Technology, CCSEIT 2011, held in Tirunelveli, India, in September 2011. The 73 revised full papers were carefully reviewed and selected from more than 400 initial submissions. The papers feature significant contributions to all major fields of the Computer Science and Information Technology in theoretical and practical aspects.
This comprehensive handbook, widely regarded as the standard reference book for the practicing dyer and finisher, Surveys the basic chemistry both of the dyes and of the natural and man-made fibers they color. Treats theory and practice of scouring, bleaching, and dyeing and features expanded coverage of the use of polymers in finishing, reactive dyes, and dyeing materials containing mixtures of fibers. Extensive bibliography, numerous formulations, and tables of reference data make this an essential daily working tool.
This book reports on cutting-edge theories and methods for analyzing complex systems, such as transportation and communication networks and discusses multi-disciplinary approaches to dependability problems encountered when dealing with complex systems in practice. The book presents the most noteworthy methods and results discussed at the International Conference on Reliability and Statistics in Transportation and Communication (RelStat), which took place in Riga, Latvia on October 17 – 20, 2018. It spans a broad spectrum of topics, from mathematical models and design methodologies, to software engineering, data security and financial issues, as well as practical problems in technical systems, such as transportation and telecommunications, and in engineering education.
The two-volume set LNAI 10191 and 10192 constitutes the refereed proceedings of the 9th Asian Conference on Intelligent Information and Database Systems, ACIIDS 2017, held in Kanazawa, Japan, in April 2017. The total of 152 full papers accepted for publication in these proceedings was carefully reviewed and selected from 420 submissions. They were organized in topical sections named: Knowledge Engineering and Semantic Web; Social Networks and Recommender Systems; Text Processing and Information Retrieval; Intelligent Database Systems; Intelligent Information Systems; Decision Support and Control Systems; Machine Learning and Data Mining; Computer Vision Techniques; Advanced Data Mining Techniques and Applications; Intelligent and Context Systems; Multiple Model Approach to Machine Learning; Applications of Data Science; Artificial Intelligence Applications for E-services; Automated Reasoning and Proving Techniques with Applications in Intelligent Systems; Collective Intelligence for Service Innovation, Technology Opportunity, E-Learning and Fuzzy Intelligent Systems; Intelligent Computer Vision Systems and Applications; Intelligent Data Analysis, Applications and Technologies for Internet of Things; Intelligent Algorithms and Brain Functions; Intelligent Systems and Algorithms in Information Sciences; IT in Biomedicine; Intelligent Technologies in the Smart Cities in the 21st Century; Analysis of Image, Video and Motion Data in Life Sciences; Modern Applications of Machine Learning for Actionable Knowledge Extraction; Mathematics of Decision Sciences and Information Science; Scalable Data Analysis in Bioinformatics and Biomedical Informatics; and Technological Perspective of Agile Transformation in IT organizations.
For many companies, their intellectual property can often be more valuable than their physical assets. Having an effective IT governance strategy in place can protect this intellectual property, reducing the risk of theft and infringement. Data protection, privacy and breach regulations, computer misuse around investigatory powers are part of a complex and often competing range of requirements to which directors must respond. There is increasingly the need for an overarching information security framework that can provide context and coherence to compliance activity worldwide. IT Governance is a key resource for forward-thinking managers and executives at all levels, enabling them to understand how decisions about information technology in the organization should be made and monitored, and, in particular, how information security risks are best dealt with. The development of IT governance - which recognises the convergence between business practice and IT management - makes it

essential for managers at all levels, and in organizations of all sizes, to understand how best to deal with information security risk. The new edition has been full updated to take account of the latest regulatory and technological developments, including the creation of the International Board for IT Governance Qualifications. IT Governance also includes new material on key international markets - including the UK and the US, Australia and South Africa.

This textbook is for courses in cyber security education that follow National Initiative for Cybersecurity Education (NICE) KSAs work roles and framework, that adopt the Competency-Based Education (CBE) method. The book follows the CBT (KSA) general framework, meaning each chapter contains three sections, knowledge and questions, and skills/labs for Skills and Abilities. The author makes an explicit balance between knowledge and skills material in information security, giving readers immediate applicable skills. The book is divided into seven parts: Securely Provision; Operate and Maintain; Oversee and Govern; Protect and Defend; Analysis; Operate and Collect; Investigate. All classroom materials (in the book an ancillary) adhere to the NICE framework. Mirrors classes set up by the National Initiative for Cybersecurity Education (NICE) Adopts the Competency-Based Education (CBE) method of teaching, used by universities, corporations, and in government training Includes content and ancillaries that provide skill-based instruction on compliance laws, information security standards, risk response and recovery, and more

Responsive Security: Be Ready to Be Secure explores the challenges, issues, and dilemmas of managing information security risk, and introduces an approach for addressing concerns from both a practitioner and organizational management standpoint. Utilizing a research study generated from nearly a decade of action research and real-time experience, this book introduces the issues and dilemmas that fueled the study, discusses its key findings, and provides practical methods for managing information security risks. It presents the principles and methods of the responsive security approach, developed from the findings of the study, and details the research that led to the development of the approach. Demonstrates the viability and practicality of the approach in today’s information security risk environment Demystifies information security risk management in practice, and reveals the limitations and inadequacies of current approaches Provides comprehensive coverage of the issues and challenges faced in managing information security risks today The author reviews existing literature that synthesizes current knowledge, supports the need for, and highlights the significance of the responsive security approach. He also highlights the concepts, strategies, and programs commonly used to achieve information security in organizations. Responsive Security: Be Ready to Be Secure examines the theories and knowledge in current literature, as well as the practices, related issues, and dilemmas experienced during the study. It discusses the reflexive analysis and interpretation involved in the final research cycles, and validates and refines the concepts, framework, and methodology of a responsive security approach for managing information security risk in a constantly changing risk environment.

Carefully researched over ten years and eagerly anticipated by the agile community, Crystal Clear: A Human-Powered Methodology for Small Teams is a lucid and practical introduction to running a successful agile project in your organization. Each chapter illuminates a different important aspect of orchestrating agile projects. Highlights include Attention to the essential human and communication aspects of successful projects Case studies, examples, principles, strategies, techniques, and guiding properties Samples of work products from real-world projects instead of blank templates and toy problems Top strategies used by software teams that excel in delivering quality code in a timely fashion Detailed introduction to emerging best-practice techniques, such as Blitz Planning, Project 360º, and the essential Reflection Workshop Question-and-answer with the author about how he arrived at these recommendations, including where they fit with CMMI, ISO, RUP, XP, and other methodologies A detailed case study, including an ISO auditor's analysis of the project Perhaps the most important contribution this book offers is the Seven Properties of Successful Projects. The author has studied successful agile projects and identified common traits they share. These properties lead your project to success; conversely, their absence endangers your project.

Data processing, Computers, Management, Data security, Data storage protection, Anti-burglar measures, Information systems, Documents, Records (documents), Classification systems, Computer technology, Computer networks, Technical documents, Maintenance, Information exchange

Written for people who manage information security risks for their organizations, this book details a security risk evaluation approach called "OCTAVE." The book provides a framework for systematically evaluating and managing security risks, illustrates the implementation of self-directed evaluations, and shows how to tailor evaluation methods to the needs of specific organizations. A running example illustrates key concepts and techniques. Evaluation worksheets and a catalog of best practices are included. The authors are on the technical staff of the Software Engineering Institute. Annotation copyrighted by Book News, Inc., Portland, OR

Ideal for risk managers, information security managers, lead implementers, compliance managers and consultants, as well as providing useful background material for auditors, this book will enable readers to develop an ISO 27001-compliant risk assessment framework for their organisation and deliver real, bottom-line business benefits.

Tough Test Questions? Missed Lectures? Not Enough Time? Fortunately for you, there's Schaum's Outlines. More than 40 million students have trusted Schaum's to help them succeed in the classroom and on exams. Schaum's is the key to faster learning and higher grades in every subject. Each Outline presents all the essential course information in an easy-to-follow, topic-by-topic format. You also get hundreds of examples, solved problems, and practice exercises to test your skills. This Schaum's Outline gives you Practice problems with full explanations that reinforce knowledge Coverage of the most up-to-date developments in your course field In-depth review of practices and applications Fully compatible with your classroom text, Schaum's highlights all the important facts you need to know. Use Schaum's to shorten your study time-and get your best test scores! Schaum's Outlines-Problem Solved.

This is the eBook version of the print title and might not provide access to the practice test software that accompanies the print book. Learn, prepare, and practice for CompTIA Cybersecurity Analyst (CSA+) exam success with this CompTIA Authorized Cert Guide from Pearson IT Certification, a leader in IT certification learning and a CompTIA Authorized Platinum Partner. · Master CompTIA Cybersecurity Analyst (CSA+) exam topics · Assess your knowledge with chapter-ending quizzes · Review key concepts with exam preparation tasks · Practice with realistic exam questions CompTIA Cybersecurity Analyst (CSA+) Cert Guide is a best-of-breed exam study guide. Expert technology instructor and certification author Troy McMillan shares preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. The book presents you

with an organized test-preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your final study plan. The companion website contains the powerful Pearson Test Prep practice test software, complete with hundreds of exam-realistic questions. The assessment engine offers you a wealth of customization options and reporting features, laying out a complete assessment of your knowledge to help you focus your study where it is needed most. Well regarded for its level of detail, assessment features, and challenging review questions and exercises, this CompTIA authorized study guide helps you master the concepts and techniques that will enable you to succeed on the exam the first time. The CompTIA authorized study guide helps you master all the topics on the CSA+ exam, including · Applying environmental reconnaissance · Analyzing results of network reconnaissance · Implementing responses and countermeasures · Implementing vulnerability management processes · Analyzing scan output and identifying common vulnerabilities · Identifying incident impact and assembling a forensic toolkit · Utilizing effective incident response processes · Performing incident recovery and post-incident response · Establishing frameworks, policies, controls, and procedures · Remediating identity- and access-related security issues · Architecting security and implementing compensating controls · Implementing application security best practices · Using cybersecurity tools and technologies

Mit diesem Handbuch identifizieren Sie Risiken, bauen wegweisendes effizienzförderndes Handlungswissen auf und sichern so Ihr Unternehmen sowie seine Prozesse, Ressourcen und die Organisation ab. Der Autor führt Sie von den gesetzlichen, regulatorischen, normativen und geschäftspolitischen Sicherheits-, Kontinuitäts- und Risikoanforderungen bis zu Richtlinien, Konzepten und Maßnahmen. Die dreidimensionale Sicherheitsmanagementpyramide V sowie die innovative und integrative RiSiKo-Management-Pyramide V liefern ein durchgängiges, praxisorientiertes und systematisches Vorgehensmodell für den Aufbau und die Weiterentwicklung des Sicherheits-, Kontinuitäts- und Risikomanagements. Beispiele und Checklisten unterstützen Sie und der Online-Service des Autors bietet Ihnen zusätzliche News, Links und ergänzende Beiträge.