

Iso Iec 27034 1 2011 Information Technology Security

Industrial assets (such as railway lines, roads, pipelines) are usually huge, span long distances, and can be divided into clusters or segments that provide different levels of functionality subject to different loads, degradations and environmental conditions, and their efficient management is necessary. The aim of the book is to give comprehensive understanding about the use of autonomous vehicles (context of robotics) for the utilization of inspection and maintenance activities in industrial asset management in different accessibility and hazard levels. The usability of deploying inspection vehicles in an autonomous manner is explained with the emphasis on integrating the total process. Key Features Aims for solutions for maintenance and inspection problems provided by robotics, drones, unmanned air vehicles and unmanned ground vehicles Discusses integration of autonomous vehicles for inspection and maintenance of industrial assets Covers the industrial approach to inspection needs and presents what is needed from the infrastructure end Presents the requirements for robot designers to design an autonomous inspection and maintenance system Includes practical case studies from industries

Until recently, if it has been considered at all in the context of business continuity, cyber security may have been thought of in terms of disaster recovery and little else. Recent events have shown that cyber-attacks are now an everyday occurrence, and it is becoming clear that the impact of these can have devastating effects on organizations whether large or small, public or private sector. Cyber security is one aspect of information security, since the impacts or consequences of a cyber-attack will inevitably damage one or more of the three pillars of information security: the confidentiality, integrity or availability of an organization’s information assets. The main difference between information security and cyber security is that while information security deals with all types of information assets, cyber security deals purely with those which are accessible by means of interconnected electronic networks, including the Internet. Many responsible organizations now have robust information security, business continuity and disaster recovery programs in place, and it is not the intention of this book to re-write those, but to inform organizations about the kind of precautions they should take to stave off successful cyber-attacks and how they should deal with them when they arise in order to protect the day-to-day businesses.

This is the Digital Practitioner Foundation Study Guide for the DPBoK Part 1 Examination. It gives an overview of every learning objective included in the Digital Practitioner Foundation syllabus, and provides in-depth coverage on preparing and taking the DPBoK Part 1 Examination. It is specifically designed to help individuals prepare for certification. This Study Guide is excellent material for:
• Senior digital business professionals who need an increased awareness of digital practices
• Mid-career IT professionals who need to stay relevant and validate their digital Subject Matter Expert (SME) status in specific domain areas
• Entry-level computing and digital business professionals
• College-level students and computing and digital business majors
It covers the following topics:
• An introduction to DPBoK Foundation certification, including the DPBoK Part 1 Examination
• Key terminology, key concepts, and the structure of the Body of Knowledge
• Basic concepts employed by the Digital Practitioner
• The capabilities of digital infrastructure and initial concerns for its effective, efficient, and secure operation
• The objectives and activities of application development
• Why product management is formalized as a company or team grows, and the differences between product and project management
• The key concerns and practices of work management as a team increases in size
• The basic concepts and practices of operations management in a digital/IT context
• How to coordinate as the organization grows into multiple teams and multiple products
• IT investment and portfolio management
• Organizational structure, human resources, and cultural factors
• Governance, risk, security, and compliance
• Information and data management on a large scale
• Practices and methods for managing complexity using Enterprise Architecture

International Standard ISO/IEC 27034-1:2011/Cor.1:2014Information Technology-Security Techniques-Application SecurityBusiness Continuity in a Cyber WorldSurviving CyberattacksBusiness Expert Press

Cyber Security Engineering

Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sichere Anwendungen – Standards und Practices

Information Security Technology – Controllability Evaluation Index for Security of Information Technology Products – Part 1: General Principles [After payment, write to & get a FREE-of-charge, unprotected true-PDF from: Sales@ChineseStandard.net]

Basiswissen Sicherheitstests

CompTIA Advanced Secur_o2

Zintegrowany system zarz?dzania unieszkodliwianiem azbestu w uj?ciu systemowym

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide

This is the eBook version of the print title. Note that the eBook may not provide access to the practice test software that accompanies the print book. Learn, prepare, and practice for CompTIA Advanced Security Practitioner (CASP) CAS-003 exam success with this CompTIA Approved Cert Guide from Pearson IT Certification, a leader in IT Certification learning and a CompTIA Authorized Platinum Partner. Master CompTIA Advanced Security Practitioner (CASP) CAS-003 exam topics Assess your knowledge with chapter-ending quizzes Review key concepts with exam preparation tasks CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide is a best-of-breed exam study guide. Leading security certification training experts Robin Abernathy and Troy McMillan share 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. 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, including: Enterprise security Risk management and incident response Research, analysis, and assessment Integration of computing, communications, and business disciplines Technical integration of enterprise components

Master the latest technology and developments from the field with the book specifically oriented to the needs of those learning information systems -- PRINCIPLES OF INFORMATION SECURITY, 6E. Taking a managerial approach, this bestseller emphasizes all aspects of information security, rather than just the technical control perspective. Readers gain a broad overview of the entire field of information security and related elements with the detail to ensure understanding. The book highlights terms used in the field and a history of the discipline as readers learn how to manage an information security program. This edition highlights the latest practices with fresh examples that explore the impact of emerging technologies, such as the Internet of Things, Cloud Computing, and DevOps. Updates address technical security controls, emerging legislative issues, digital forensics, and ethical issues in IS security, making this the ideal IS resource for business decision makers. Important Notice: Media content referenced within the product description or the product text may not be available in the eBook version.

The only official, comprehensive reference guide to the CISSP All new for 2019 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 new eight domains of CISSP with the necessary depth to apply them to the daily practice of information security. Written 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.

Cyber-attacks continue to rise as more individuals rely on storing personal information on networks. Even though these networks are continuously checked and secured, cybercriminals find new strategies to break through these protections. Thus, advanced security systems, rather than simple security patches, need to be designed and developed. Exploring Security in Software Architecture and Design is an essential reference source that discusses the development of security-aware software systems that are built into every phase of the software architecture. Featuring research on topics such as migration techniques, service-based software, and building security, this book is ideally designed for computer and software engineers, ICT specialists, researchers, academicians, and field experts.

ISSE 2014 Securing Electronic Business Processes

CISSP Cert Guide

Sicherheit von Webanwendungen in der Praxis

Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia

Who Owns the New Oil?

Exploring Security in Software Architecture and Design

System informatyczny GeoAzbest. Zintegrowany system zarządzania unieszkodliwianiem azbestu w ujęciu systemowym

The Digital Practitioner Pocket Guide is designed to be a handy reference guide to selected parts of the Digital Practitioner Body of Knowledge™ Standard. It is designed to help:
• Those who require a first introduction and basic understanding of the Digital Practitioner Body of Knowledge Standard
• Individuals who wish to create and manage product offerings with an increasing digital component lead their organization through Digital Transformation
• IT professionals working within any size organization, from a startup through to a large enterprise, that has adopted digital approaches
It covers the following topics:
• A brief introduction to the Digital Practitioner Body of Knowledge Standard
• An introduction to key terminology, key concepts, and the structure of the Body of Knowledge
• Basic concepts employed by the Digital Practitioner
• The capabilities of digital infrastructure and initial concerns for its effective, efficient, and secure operation
• The objectives and activities of application development
• Why product management is formalized as a company or team grows, and the differences between product and project management
• The key concerns and practices of work management as a team increases in size
• The basic concepts and practices of operations management in a digital/IT context
• How to coordinate as the organization grows into multiple teams and multiple products
• IT investment and portfolio management
• Organizational structure, human resources, and cultural factors
• Governance, risk, security, and compliance
• Information and data management on a large scale
• Practices and methods for managing complexity using Enterprise Architecture

Die Effizienz, Existenz und Zukunft eines Unternehmens sind maßgeblich abhängig von der Sicherheit und Kontinuität sowie den Risiken der Informationsverarbeitung. Die dreidimensionale IT-Sicherheitsmanagementpyramide V sowie die innovative und integrative IT-RiSiKo-Managementpyramide V liefern ein durchgängiges, praxisorientiertes und geschäftszentriertes Vorgehensmodell für den Aufbau und die Weiterentwicklung des IT-Sicherheits-, Kontinuitäts- und Risikomanagements. Mit diesem Buch identifizieren Sie Risiken, bauen wegweisendes effizienzförderndes Handlungswissen auf. Sie richten Ihre IT sowie deren Prozesse, Ressourcen und die Organisation systematisch und effektiv auf Sicherheit aus und integrieren Sicherheit in den IT-Lebenszyklus. Der Autor führt Sie von der Politik bis zu Konzepten und Maßnahmen. Beispiele und Checklisten unterstützen Sie. Der Online-Service des Autors bietet Ihnen zusätzliche News, Links und ergänzende Beiträge.

Falar de Segurança da Informação em um mundo em constante transformação é sempre um desafio. De um lado, temos a necessidade de manter os dados protegidos de todas as ameaças que existem e surgem a cada dia. Do outro lado, a preocupação de que essa proteção afete o mínimo possível na usabilidade, performance e experiência do usuário. Apesar de todo o “glamour”, o profissional da área muitas vezes é persona non grata no mundo corporativo. Carrega o estigma de ser o pessimista, aquele que atrapalha o negócio, aquele que anuncia uma tragédia que nunca ocorre e que por esse motivo exige a aplicação de uma série de controles e condições para os dados e sistemas. Esse profissional deve saber justificar suas ações através de argumentos baseados em metodologias sólidas. Deves entender e saber explicar os fundamentos técnicos falando a linguagem do negócio. Este livro é composto de uma série de artigos inéditos escritos por profissionais de destaque na área atuando no Brasil e no exterior e que entendem que Segurança da Informação não pode ser um “trilho” de maneira que imobilize a operação das organizações, mas, sim, uma “trilha”, na medida em que a proteção é dosada por meio da análise dos riscos no percurso. O leitor poderá usar o conteúdo desta obra de forma não linear, como apoio para decidir qual caminho seguir, aproveitando não somente o conteúdo técnico aqui contido, como também a experiência e as lições aprendidas de cada autor. Artigos e seus autores: Procuram-se Hackers – Adriano Mauro Cansian Gestão de Risco – Augusto Paes de Barros Cientistização em Segurança da Informação Como Processo – Anderson Ramos Gestão de Identidades e Acessos – Felipe Silva Introdução à Criptografia Aplicada – Galeno Garbe Melhores Práticas em Segurança de Redes Sem Fio – Luiz Eduardo dos Santos Gestão de Vulnerabilidades e Atualizações de Segurança – Fernando Fonseca Segurança no Desenvolvimento de Software – Wagner Elias O Papel do Usuário – Altieres Rohr Perspectiva, Desafios e Tendências em Auditoria de Tecnologia e Segurança da Informação – Ricardo Castro Estabelecendo a Resiliência Operacional: Definindo e Construindo uma Estratégia para a Continuidade dos Negócios – Eduardo Vianna de Camargo Neves Derivações para o Futuro da Segurança da Informação – Fábio F. Ramo

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 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 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.

GB/T 36630.1-2018: Translated English of Chinese Standard. (GBT 36630.1-2018, GB/T36630.1-2018, GBT36630.1-2018)

Market, Functional and Conceptual View based on SAP S/4HANA

Proceedings of the 10th International Conference on Software Process Improvement (CIMPS 2021)

Core Software Security

Information Technology-Security Techniques-Application Security

New Perspectives in Software Engineering

Robots, Drones, UAVs and UGVs for Operation and Maintenance

Computer security touches every part of our daily lives from our computers and connected devices to the wireless signals around us. Breaches have real and immediate financial, privacy, and safety consequences. This handbook has compiled advice from top professionals working in the real world about how to minimize the possibility of co your systems. Written for professionals and college students, it provides comprehensive best guidance about how to minimize hacking, fraud, human error, the effects of natural disasters, and more. This essential and highly-regarded reference maintains timeless lessons and is fully revised and updated with current information on security cloud computing, virtualization, and more.

"... an engaging book that will empower readers in both large and small software development and engineering organizations to build security into their products. ... Readers are armed with firm solutions for the fight against cyber threats." —Dr. Dena Haritos Tsamitis. Carnegie Mellon University "... a must read for security specialists, software engineers. ... should be part of every security professional's library." —Dr. Larry Ponemon, Ponemon Institute "... the definitive how-to guide for software security professionals. Dr. Ransome, Anmol Misra, and Brook Schoenfield deftly outline the procedures and policies needed to integrate real security into the software development process on the front lines of the Cyber War ..." —Cedric Leighton, Colonel, USAF (Ret.). Cedric Leighton Associates "Dr. Ransome, Anmol Misra, and Brook Schoenfield give you a magic formula in this book - the methodology and process to build security into the entire software development life cycle so that the software is secured at the source! "

Communications There is much publicity regarding network security, but the real cyber Achilles’ heel is insecure software. Millions of software vulnerabilities create a cyber house of cards, in which we conduct our digital lives. In response, security people build ever more elaborate cyber fortresses to protect this vulnerable software. Despite fortifications consistently fail to protect our digital treasures. Why? The security industry has failed to engage fully with the creative, innovative people who write software. Core Software Security expounds developer-centric software security, a holistic process to engage creativity for security. As long as software is developed by humans

fix it. Developer-centric security is not only feasible but also cost effective and operationally relevant. The methodology builds security into software development, which lies at the heart of our cyber infrastructure. Whatever development method is employed, software must be secured at the source. Book Highlights: Supplies a practitioner

Agile as a security enabler Covers the privacy elements in an SDL Outlines a holistic business-savvy SDL framework that includes people, process, and technology Highlights the key success factors, deliverables, and metrics for each phase of the SDL Examines cost efficiencies, optimized performance, and organizational structure of a developer

security program and PSIRT Includes a chapter by noted security architect Brook Schoenfield who shares his insights and experiences in applying the book’s SDL framework View the authors’ website at http://www.androidinsecurity.com/

"Ulf Mattsson leverages his decades of experience as a CTO and security expert to show how companies can achieve data compliance without sacrificing operability." Jim Ambrosini, CISSP, CRISC, Cybersecurity Consultant and Virtual CISO "Ulf Mattsson lays out not just the rationale for accountable data governance, he provides clear strategic business leader should know and put into practice. As individuals, citizens and employees, we should all take heart that following his sound thinking can provide us all with a better future." Richard Purcell, CEO Corporate Privacy Group and former Microsoft Chief Privacy Officer Many security experts excel at working with traditional technology, but it is the newer data privacy techniques to balance compliance requirements and the business utility of data. This book will help readers grow out of a siloed mentality and into an enterprise risk management approach to regulatory compliance and technical roles, including technical data privacy and security issues. The book uses practical lessons learned from concepts and tools to help security leaders and their teams craft and implement strategies. These projects deal with a variety of use cases and data types. A common goal is to find the right balance between compliance, privacy requirements, and the business utility of data. This book reviews how new and old privacy-preserving techniques for protection for data in transit, use, and rest. It positions techniques like pseudonymization, anonymization, tokenization, homomorphic encryption, dynamic masking, and more. Topics include Trends and Evolution Best Practices, Roadmap, and Vision Zero Trust Architecture Applications, Privacy by Design, and APIs Machine Learning and Analytics

Computing Blockchain and Data Lineage Hybrid Cloud, CASB, and SASE HSM, TPM, and Trusted Execution Environments Internet of Things Quantum Computing And much more!

Die Sicherheit von IT-Systemen ist heute eine der wichtigsten Qualitätseigenschaften. Wie für andere Eigenschaften gilt auch hier das Ziel, fortwährend sicherzustellen, dass ein IT-System den nötigen Sicherheitsanforderungen genügt, dass diese in einem Kontext effektiv sind und etwaige Fehlerzustände in Form von Sicherheitsproblemen beobachtet werden. geben einen fundierten, praxisorientierten Überblick über die technischen, organisatorischen, prozessoralen, aber auch menschlichen Aspekte des Sicherheitstestens und vermitteln das notwendige Praxiswissen, um für IT-Anwendungen die Sicherheit zu erreichen, die für eine wirtschaftlich sinnvolle und regulationskonforme Inbetriebnahme von IT-Systemen notwendig ist.Aus dem Inhalt:- Grundlagen des Testens der Sicherheit- Sicherheitsanforderungen und -risiken- Ziele und Strategien von Sicherheitstests- Sicherheitstestprozesse im Softwarelebenszyklus- Testen von Sicherheitsmechanismen- Auswertung von Sicherheitstests- Auswahl von Werkzeugen und Standards- Menschliche Faktoren, S

orientiert sich das Buch am Lehrplan "ISTQB® Advanced Level Specialist – Certified Security Tester" und eignet sich mit vielen erläuternden Beispielen und weiterführenden Literaturverweisen und Exkursen gleichermaßen für das Selbststudium wie als Begleitliteratur zur entsprechenden Schulung und folgender Prüfung zum ISTQB® Certified Tester – Security Tester. **Sicherheitstester.**

- Cybersecurity Law, Standards and Regulations, 2nd Edition
- Research Anthology on Agile Software, Software Development, and Testing
- The Digital Practitioner Foundation Study Guide
- Trilhas em Segurança da Informação
- Global Standards and Publications
- The Digital Practitioner Pocket Guide
- CISSP Cert Guide, 3/e_c3

Written for IT service managers, consultants and other practitioners in IT governance, risk and compliance, this practical book discusses all the key concepts of COBIT®5, and explains how to direct the governance of enterprise IT (GEIT) using the COBIT®5 framework. The book also covers the main frameworks and standards supporting GEIT, discusses the ideas of enterprise and governance, and shows the path from corporate governance to the governance of enterprise IT.

[After payment, write to & get a FREE-of-charge, unprotected true-PDF from: Sales@ChineseStandard.net] This part of GB/T 36630 specifies the concept and guarantee objectives of the controllability for security of information technology products, and gives the evaluation principles, evaluation index system and implementation process of controllability for security of information technology products.

Uluslararası bir standart olarak geliştirilen ISO 27001 Bilgi Güvenliği Yönetim Sistemi, kuruluşları'nı i? süreçlerinde oluşturulan ve ?lenen bilgilerin gizlilik, bütünlük ve erişilebilirlik boyutları'nda temel ?artları? belirlemektedir. Çe?m?zda gittikçe dijitalleşen süreçler üzerindeki tehdit ve zayıflıklar?n

yarattığı bilgi güvenliği risklerinin bir sistem dahilinde ele alınması?, de?erlendirilmesi ve ?lenmesi bilgi güvenliği kontrolleri için uygulama prensipleri gerekmektedir. Bilgi güvenliği'nin bir kurumsal yönetim unsuru olarak insan, teknoloji ve süreçler arasındaki etkileşimlerde kullanılan teknolojilerin güvenliği,

fiziksel güvenlik, risk yönetimi, i? sürekliliği ile yasa ve yönetmeliklere uyum gibi unsurlarla yakından ilgili olması?, bunları?n yanşı?ra çağdaş?anlara, i? ortakları'na, müşterilere ve topluma yönelik çe?itli yükümlülükleri bünyesinde barındırması? bu tür bir sistemin kuruluşları için ne derece önemli olduğunu göstermektedir. Bu kitapçık, ISO 27001 Bilgi güvenliği yönetim sisteminin ?artları?yla ISO 27002 Bilgi güvenliği kontrolleri için uygulama prensipleri dikkate alınarak bu konuda bünyelerinde BGYS kurmak ve bu standarda göre belgelendirilmek isteyen kuruluşlara bir rehber olmak amacıyla hazırlanmıştır.

Cyber Security Engineering is the definitive modern reference and tutorial on the full range of capabilities associated with modern cyber security engineering. Pioneering software assurance experts Dr. Nancy R. Mead and Dr. Carol C. Woody bring together comprehensive best practices for building software systems that exhibit superior operational security, and for considering security throughout your full system development and acquisition lifecycles. Drawing on their pioneering work at the Software Engineering Institute (SEI) and Carnegie Mellon University, Mead and Woody introduce seven core principles of software assurance, and show how to apply them coherently and systematically. Using these principles, they help you prioritize the wide range of possible security actions available to you, and justify the required investments. Cyber Security Engineering guides you through risk analysis, planning to manage secure software development, building organizational models, identifying required and missing competencies, and defining and structuring metrics. Mead and Woody address important topics, including the use of standards, engineering security requirements for acquiring COTS software, applying DevOps, analyzing malware to anticipate future vulnerabilities, and planning ongoing improvements. This book will be valuable to wide audiences of practitioners and managers with responsibility for systems, software, or quality engineering, reliability, security, acquisition, or operations. Whatever your role, it can help you reduce operational problems, eliminate excessive patching, and deliver software that is more resilient and secure.

Technologie informacyjno-komunikacyjna – za?enia oprogramowania. Zintegrowany system zarządania nieszkodliwianiem azbestu w ujściu systemowym

Highlights of the Information Security Solutions Europe 2014 Conference

Controlling Privacy and the Use of Data Assets - Volume 1

Systems, Software and Services Process Improvement

Wie sich Unternehmen schützen können – Hintergründe, Maßnahmen, Prüfverfahren und Prozesse

Foundations of Information Security Based on ISO27001 and ISO27002 - 3rd revised edition

Artificial Intelligence to Solve Pervasive Internet of Things Issues discusses standards and technologies and wide-ranging technology areas and their applications and challenges, including discussions on architectures, frameworks, applications, best practices, methods and techniques required for integrating AI to resolve IoT issues. Chapters also provide step-by-step measures, practices and solutions to tackle vital decision-making and practical issues affecting IoT technology, including autonomous devices and computerized systems. Such issues range from adopting, mitigating, maintaining, modernizing and protecting AI and IoT infrastructure components such as scalability, sustainability, latency, system decentralization and maintainability. The book enables readers to explore, discover and implement new solutions for integrating AI to solve IoT issues. Resolving these issues will help readers address many real-world applications in areas such as scientific research, healthcare, defense, aeronautics, engineering, social media, and many others. Discusses intelligent techniques for the implementation of Artificial Intelligence in Internet of Things

Prepared for researchers and specialists who are interested in the use and integration of IoT and Artificial Intelligence technologies

Software development continues to be an ever-evolving field as organizations require new and innovative programs that can be implemented to make processes more efficient, productive, and cost-effective. Agile practices particularly have shown great benefits for improving the effectiveness of software development and its maintenance due to their ability to adapt to change. It is integral to remain up to date with the most emerging tactics and techniques involved in the development of new and innovative software. The Research Anthology on Agile Software, Software Development, and Testing is a comprehensive resource on the emerging trends of software development and testing. This text discusses the newest developments in agile software and its usage spanning multiple industries. Featuring a collection of insights from diverse authors, this research anthology offers international perspectives on agile software. Covering topics such as global software engineering, knowledge management, and product development, this comprehensive resource is valuable to software developers, software engineers, computer engineers, IT directors, students, managers, faculty, researchers, and academicians.

Blockchain is an emerging technology for organizations to almost instantaneously make and verify transactions, streamlining business processes, saving money, and reducing the potential for fraud. This book covers the application of blockchain technology to the enterprise world, it describes the opportunities and challenges for adoption of DLT (Digital Ledger Technology) in a corporate environment, and specific use cases that may benefit from a decentralized and distributed trustless network. There are many books on blockchain, the new de-centralised ledger technology made famous (or infamous) by Bitcoin, Onecoin and others. But as cryptocurrencies and stock markets rise and fall with surprise volatility and the world economy emerges changed by coronavirus and the resulting economic crash, many in industry are looking again at the powerful features of blockchain and how these may help them adapt. This new book sets out the core features of blockchain and uniquely describes, in natural language and in real-life scenarios, how de-centralised ledgers may affect industries as varied as virus-tracking apps, finance, investment and healthcare.

This book presents the most interesting talks given at ISSE 2014 – the forum for the inter-disciplinary discussion of how to adequately secure electronic business processes. The reader may expect state-of-the-art: best papers of the Conference ISSE 2014.

Offshore Oil and Gas Installations Security

A Practical Approach for Systems and Software Assurance

The Official (ISC)2 Guide to the CISSP CBK Reference

Aus- und Weiterbildung zum ISTQB® Advanced Level Specialist – Certified Security Tester

An International Perspective

Preparation for the DPBOK® Part 1 Examination

Caminhos e ideias para a proteção de dados

Monografia dotyczca bezpieczestwa informacji w urzędach administracji terenowej podsumowujca wyniki bada? z lat 2012-2016

This book features peer reviewed contributions from across the disciplines on themes relating to protection of data and to privacy protection. The authors explore fundamental and legal questions, investigate case studies and consider concepts and tools such as privacy by design, the risks of surveillance and

fostering trust. Readers may trace both technological and legal evolution as chapters examine current developments in ICT such as cloud computing and the Internet of Things. Written during the process of the fundamental revision of revision of EU data protection law (the 1995 Data Protection Directive), this volume is highly topical. Since the European Parliament has adopted the General Data Protection Regulation (Regulation 2016/679), which will apply from 25 May 2018, there are many details to be sorted out. This volume identifies and exemplifies key, contemporary issues. From fundamental rights and offline alternatives, through transparency requirements to health data breaches, the reader is provided with a rich and detailed picture, including some daring approaches to privacy and data protection. The book will inform and inspire all stakeholders. Researchers with an interest in the philosophy of law and philosophy of technology, in computers and society, and in European and international law will all find something of value in this stimulating and engaging work.

Webanwendungen bilden in Unternehmen zahlreiche sensible Geschäftsprozesse ab – ob mit Kunden, mit Mitarbeitern, Partnern und Zulieferern. Daher sind Webapplikationen ein Sicherheitsrisiko für Unternehmen und ihr Schutz von entscheidender Bedeutung. In dem Buch beleuchtet der Autor die wichtigsten Aspekte der Webanwendungssicherheit und stützt sich dabei auf seine langjährige Erfahrung als IT-Security-Berater für Webanwendungen und Entwicklungsprozesse. Der Band bietet neben einem allgemeinen Überblick zum Thema Sicherheit von Webanwendungen ausführliche und praxisorientierte Darstellungen zu wichtigen Einzelfragen: Was sind die häufigsten Schwachstellen und mit welchen Maßnahmen lassen sich Webanwendungen am effektivsten gegen Angriffe absichern? Ein eigenes Kapitel befasst sich mit den Verfahren, die eingesetzt werden, um die Sicherheit von Anwendungen bereits im Entwicklungsprozess zu bewerten und zu überprüfen. Der Autor erläutert zudem, wie sich die Sicherheit in selbst entwickelten und zugekauften Webanwendungen durch organisatorische Prozesse nachhaltig verbessern lässt. Die zweite Auflage des 2014 erstmals erschienen Buchs wurde vor dem Hintergrund neuer Techniken zur Abwehr von Angriffen und neuer Prüfverfahren vollständig überarbeitet und aktualisiert. Auch aktuelle Beratungsprojekte des Autors haben Eingang in die Neuauflage gefunden – insbesondere dort, wo es um organisatorische Aspekte von Webanwendungssicherheit geht. Der Band richtet sich an Entwickler von Webanwendungen, IT-Security- und Qualitätsmanager genauso wie an Leser, die sich in das Thema Webanwendungssicherheit einarbeiten wollen.

The five volume set LNCS 10960 until 10964 constitutes the refereed proceedings of the 18th International Conference on Computational Science and Its Applications, ICCSA 2018, held in Melbourne, Australia, in July 2018. Apart from the general tracks, ICCSA 2018 also includes 34 international workshops in various areas of computational sciences, ranging from computational science technologies, to specific areas of computational sciences, such as computer graphics and virtual reality. The total of 265 full papers and 10 short papers presented in the 5-volume proceedings set of ICCSA 2018, were carefully reviewed and selected from 892 submissions.

Practical Technology and Use Cases of Enterprise Blockchain for the Real World

Computational Science and Its Applications – ICCSA 2018

Governance of Enterprise IT based on COBIT 5

A Reference Framework

ISO 27001 Bilgi Güvenliği Yönetim Sistemi ve ISO 27002 Uygulama Kılavuzu

Security at the Source

Principles of Information Security

Oil and natural gas, which today account for over 60% of the world's energy supply, are often produced by offshore platforms. One third of all oil and gas comes from the offshore sector. However, offshore oil and gas installations are generally considered intrinsically vulnerable to deliberate attacks. The changing security landscape and concerns about the threats of terrorism and piracy to offshore oil and gas installations are major issues for energy companies and governments worldwide. But, how common are attacks on offshore oil and gas installations? Who attacks offshore installations? Why are they attacked? How are they attacked? How is their security regulated at the international level? How has the oil industry responded? This timely and first of its kind publication answers these questions and examines the protection and security of offshore oil and gas installations from a global, industry-wide and company-level perspective. Looking at attacks on offshore installations that occurred throughout history of the offshore petroleum industry, it examines the different types of security threats facing offshore installations, the factors that make offshore installations attractive targets, the nature of attacks and the potentially devastating impacts that can result from attacks on these important facilities. It then examines the international legal framework, state practice and international oil and gas industry responses that aim to address this vital problem. Crucially, the book includes a comprehensive dataset of attacks and security incidents involving offshore oil and gas installations entitled the Offshore Installations Attack Dataset (OIAD). This is an indispensable reference work for oil and gas industry professionals, company security officers, policy makers, maritime lawyers and academics worldwide.

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.

As long as humans write software, the key to successful software security is making the software development program process more efficient and effective. Although the approach of this textbook includes people, process, and technology approaches to software security, Practical Core Software Security: A Reference Framework stresses the people element of software security, which is still the most important part to manage as software is developed, controlled, and exploited by humans. The text outlines a step-by-step process for software security that is relevant to today's technical, operational, business, and development environments. It focuses on what humans can do to control and manage a secure software development process using best practices and metrics. Although security issues will always exist, students learn how to maximize an organization's ability to minimize vulnerabilities in software products before they are released or deployed by building security into the development process. The authors have worked with Fortune 500 companies and have often seen examples of the breakdown of security development lifecycle (SDL) practices. The text takes an experience-based approach to apply components of the best available SDL models in dealing with the problems described above. Software security best practices, an SDL model, and framework are presented in this book. Starting with an overview of the SDL, the text outlines a model for mapping SDL best practices to the software development life cycle (SDLC). It explains how to use this model to build and manage a mature SDL program. Exercises and an in-depth case study aid students in mastering the SDL model. Professionals skilled in secure software development and related tasks are in tremendous demand today. The industry continues to experience exponential demand that should continue to grow for the foreseeable future. This book can benefit professionals as much as students. As they integrate the book's ideas into their software security practices, their value increases to their organizations, management teams, community, and industry. About the Authors Dr. James Ransome, PhD, CISSP, CISM is a veteran of numerous chief information security officer (CISO), chief security officer (CSO), and chief production security officer (CPSO) roles, as well as an author and co-author of numerous cybersecurity books. Anmol Misra is an accomplished leader, researcher, author, and security expert with over 16 years of experience in technology and cybersecurity. Mark S. Merkow, CISSP, CISM, CSSLP has over 25 years of experience in corporate information security and 17 years in the AppSec space helping to establish and lead application security initiatives to success and sustainment.

This book explains the functional scope, the data model, the solution architecture, the underlying engineering concepts, and the programming model of SAP S/4HANA as the most well-known enterprise resource planning (ERP) system. The approach is to start with general concepts and then to proceed step-by-step to concrete implementations in SAP S/4HANA. In the first part the reader learns about the market view of ERP solutions and vendors. The second part deals with the business processes for sales, marketing, finance, supply chain, manufacturing, services, procurement, and human resources which are covered with SAP S/4HANA. In the third part the underlying concepts of SAP S/4HANA are described, for example in-memory storage, analytics and search, artificial intelligence, process and data integration, security and compliance, lifecycle management, performance and scalability, configuration and implementation. The book is concluded with a final chapter explaining how to deploy an appliance to explore SAP S/4HANA. The target audience for the book are managers and business analysts who want to understand the market situation and future ERP trends, end users and process experts who need to comprehend the business processes and the according solution capabilities provided with SAP S/4HANA, architects and developers who have to learn the technical concepts and frameworks for enhancing SAP S/4HANA functionality, and consultants and partners who require to adopt and configure SAP S/4HANA.

Compendium on Enterprise Resource Planning

IT-Sicherheit mit System

18th International Conference, Melbourne, VIC, Australia, July 2-5, 2018, Proceedings, Part II

A Management Guide

Blockchain Applied

Computer Security Handbook, Set

Surviving Cyberattacks

This volume constitutes the refereed proceedings of the 24th EuroSPI conference, held in Ostrava, Czech Republic, in September 2017. The 56 revised full papers presented were carefully reviewed and selected from 97 submissions. They are organized in topical sections on SPI and VSEs, SPI and process models, SPI and safety, SPI and project management, SPI and implementation, SPI issues, SPI and automotive, selected key notes and workshop papers, GamifySPI, SPI in Industry 4.0, best practices in implementing traceability, good and bad practices in improvement, safety and security, experiences with agile and lean, standards and assessment models, team skills and diversity strategies.

With the immense amount of data that is now available online, security concerns have been an issue from the start, and have grown as new technologies are increasingly integrated in data collection, storage, and transmission. Online cyber threats, cyber terrorism, hacking, and other cybercrimes have begun to take advantage of this information that can be easily accessed if not properly handled. New privacy and security measures have been developed to address this cause for concern and have become an essential area of research within the past few years and into the foreseeable future. The ways in which data is secured and privatized should be discussed in terms of the technologies being used, the methods and models for security that have been developed, and the ways in which risks can be detected, analyzed, and mitigated. The Research Anthology on Privatizing and Securing Data reveals the latest tools and technologies for privatizing and securing data across different technologies and industries. It takes a deeper dive into both risk detection and mitigation, including an analysis of cybercrimes and cyber threats, along with a sharper focus on the technologies and methods being actively implemented and utilized to secure data online. Highlighted topics include information governance and privacy, cybersecurity, data protection, challenges in big data, security threats, and more. This book is essential for data analysts, cybersecurity professionals, data scientists, security analysts, IT specialists, practitioners, researchers, academicians, and students interested in the latest trends and technologies for privatizing and securing data.

Van Haren Publishing is the world's leading publisher in best practice, methods and standards within IT Management, Project Management, Enterprise Architecture and Business Management. We are the official publisher for some of the world's leading organizations and their frameworks including: The Open Group [TOGAF], IPMA-NL, ITSqc [eSCM Models], GamingWorks [ABC of ICT], ASL BiSL Foundation, IAOP®, IACCM, CRP Henri Tudor and PMI NL. This catalog will provide you with an overview of our most popular and upcoming titles, but also gives you a quality summary on internationally relevant frameworks. Van Haren Publishing is an independent, worldwide recognized publisher, well known for our extensive professional network (authors, reviewers and accreditation bodies of standards), flexibility and years of experience. We make content available in hard copy and digital formats, designed to suit your personal preference (iPad, Kindle and online), available through over 50 distribution partners (Amazon, Google Play, Barnes & Noble, Managementboek and Bol.com, etc.) and over 700 outlets worldwide. Free whitepapers are available in our eKnowledge, with a licence for our eLibrary you can download all our eBooks within your area of expertise and in our eShop you can place your order in your favorite media format: hard copy or eBook.

International Standard ISO/IEC 27034-1:2011/Cor.1:2014

Technologie informacyjno-komunikacyjne

Business Continuity in a Cyber World

24th European Conference, EuroSPI 2017, Ostrava, Czech Republic, September 6-8, 2017, Proceedings

Artificial Intelligence to Solve Pervasive Internet of Things Issues

Data Protection and Privacy: (In)visibilities and Infrastructures

Practical Core Software Security