Iso Iec 27034 1 2011 Information Technology Security

MCCANN LOPEZ

CISSP Cert Guide Business Expert Press
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.
Informationssicherheit und Datenschutz Springer-Verlag
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
Research Anthology on Agile Software, Software Development, and Testing CRC Press
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
IT-Sicherheit mit System Springer
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 Digital Practitioner Pocket Guide Springer Nature
The work is a context-oriented analysis and synthesis of complex engineered systems to ensure continuous and safe operations under conditions of uncertainty. The book is divided in four parts, the first one comprises an overview of the development of systems engineering: starting with basics of Systems Science and Single Systems Engineering, through System of Systems Engineering to Cognitive Systems Engineering. The Cognitive Systems Engineering model was based on the concept of imperfect knowledge acquisition and management. The second part shows the evolutionary character of the dependability concept over the last fifty years. Beginning from simple models based on the classical probability theory, through the concepts of tolerating faults, as well as resilience engineering, we come to the assumptions of Cognitive Dependability Engineering (CDE), based on the concept of continuous smart operation, both under normal and abnormal conditions. The subject of the next part is analysis and synthesis of Cyber-Physical-Social (CPS) Systems. The methodology consists of the following steps: modeling CPS systems' structure, simulating their behavior in changing conditions and in situations of disruptions, and finally assessing the dependability of the entire system based on CDE. The last part of the work answers the question of how to deal with risks in CPS systems in situations of high level of uncertainty. The concept of a Cognitive Digital Twin was introduced to support the process of solving complex problems by experts, and on this basis a framework for cognitive dependability based problemsolving in CPS Systems operating under deep uncertainty was developed. The possibilities and purposefulness of using this framework have been demonstrated with three practical examples of disasters that have happened in the past and have been thoroughly analyzed.
ISO 27001 Bilgi Güvenliği Yönetim Sistemi ve ISO 27002

Uygulama Kılavuzu CRC Press
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.
Artificial Intelligence to Solve Pervasive Internet of Things Issues Springer
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.
Research Anthology on Privatizing and Securing Data Van Haren
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.
Systems, Software and Services Process Improvement CRC Press
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.
Business Continuity in a Cyber World Academic Press
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.
Practical Core Software Security IGI Global
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.
Sicherheit von Webanwendungen in der Praxis CRC Press
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, or 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
Systems, Software and Services Process Improvement CRC Press
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.
Technologie informacyjno-komunikacyjne – założenia oprogramowania. Zintegrowany system zarządzania unieszkodliwianiem azbestu w ujęciu systemowym Springer
"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 strategies and tactics that every 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 technologies but fall apart in utilizing 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 in applying real-life 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 can provide practical 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 Secure Multiparty Computing Blockchain and Data Lineage Hybrid Cloud, CASB, and SASE HSM, TPM, and Trusted Execution Environments Internet of Things Quantum Computing And much more!
Computer Security Handbook, Set Van Haren
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
Data Protection and Privacy: (In)visibilities and Infrastructures "O'Reilly Media, Inc."
This book contains a selection of papers from the 2021 International Conference on Software Process Improvement (CIMPS'21), held between the 20th and 22th of October in Torreón Coahuila, México as virtual venue. The CIMPS'21 is a global forum for researchers and practitioners that present and discuss the most recent innovations, trends, results, experiences and concerns in the several perspectives of Software Engineering with clear relationship but not limited to software processes, Security in Information and Communication Technology and Big Data Field. The main topics covered are: Organizational Models, Standards and Methodologies, Software Process Improvement, Knowledge Management, Software Systems, Applications and Tools, Information and Communication Technologies and Processes in non-software domains (Mining, automotive, aerospace, business, health care, manufacturing, etc.) with a demonstrated relationship to Software Engineering Challenges.
Controlling Privacy and the Use of Data Assets - Volume 1 Pearson IT Certification
Blockchain is the popular name given to the exciting, evolving world of distributed ledger technology (DLT). Blockchains offer equitable and secure access to data, as well as transparency and immutability. Organisations can decide to use blockchain to upgrade whatever ledgers they are currently deploying (for example, relational databases, spreadsheets and cumbersome operating models) for their data and technology stack in terms of books and records, transactions, storage, production services and in many other areas. This book describes the applied use of blockchain technology in the enterprise world. Written by two expert practitioners in the field, the book is in two main parts: (1) an introduction to the history of, and a critical context explainer about, the emergence of blockchain written in natural language and providing a tour of the features, functionality and challenges of blockchain and DLT; and (2) a series of six applied organisational use cases in (i) trade finance, (ii) healthcare, (iii) retail savings & investments, (iv) real estate, (v) central bank digital currencies (CBDC) and (vi) fund management that offer the reader a straightforward, easy-to-read comparison between 'old world' technology (such as platforms, people and processes) versus what blockchain ledgers offer to enterprises and organisations in terms of improved efficiency, performance, security and access to business data. Blockchain is sometimes tainted by association to Bitcoin, Onecoin and others. But as cryptocurrencies and stock markets continue to rise and fall with volatility and the world economy emerges changed by

coronavirus, working from home and the threat of inflation, many enterprises, organisations and governments are looking again at the powerful features of blockchain and wondering how DLT may help them adapt. This book is an ideal introduction to the practical and applied nature of blockchain and DLT solutions for business executives, business students, managers, C-suite senior leaders, software architects and policy makers and sets out, clearly and professionally, the benefits and challenges of the actual business applications of blockchain.

Governance of Enterprise IT based on COBIT 5 European Association for Security

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.

Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia IGI Global

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.

New Perspectives in Software Engineering dpunkt.verlag

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.