Iso 29100 Standard

Authored by an internationally recognized expert in the field, this expanded, timely second edition addresses all the critical information security management issues needed to help businesses protect their valuable assets. Professionals learn how to manage business risks, governance and compliance. This updated resource provides a clear guide to ISO/IEC 27000 security standards and their implementation, focusing on the recent ISO/IEC 27001. Moreover, readers are presented with practical and logical information on standard accreditation and certification. From information security management system (ISMS) business context, operations, and risk, to leadership and support, this invaluable book is your one-stop resource on the ISO/IEC 27000 series of standards.

The censorship and surveillance of individuals, societies, and countries have been a long-debated ethical and moral issue. In consequence, it is vital to explore this controversial topic from all angles. Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications is a vital reference source on the social, moral, religious, and political aspects of censorship and surveillance. It also explores the techniques of technologically supported censorship and surveillance. Highlighting a range of topics such as political censorship, propaganda, and information privacy, this multi-volume book is geared towards government officials, leaders, professionals, policymakers, media specialists, academicians, and researchers interested in the various facets of censorship and surveillance.

Information Law Series #48 About this book: Imposing Data Sharing among Private Actors is a vital book shedding light on the nature of certain economic and societal balancing exercises required for any compulsory business-to-business (B2B) data-sharing initiatives because data sharing involves both benefits and potential costs. While the economic value originating from data sharing seems evident, identifying the legal framework to be applied to it is a challenge. This is due to the multiple claims and rights aimed at controlling, accessing or benefiting from data processing. What’s in this book: Whether these initiatives pursue economic, societal or empowerment objectives, their potential benefits must be balanced with the following three considerations that are extensively investigated in the book: the economic interests of the data holder; personal data protection considerations; and long-term and collective costs in terms of individual autonomy. The analysis elucidates how these aspects have been factored into existing compulsory B2B data-sharing initiatives so far (particularly in Europe), and on how they may be used as a source of inspiration in future initiatives. Insightful suggestions on the implementation of these balancing exercises conclude the volume. How this will help you: Based on law and literature in competition, personal data protection and intellectual property, the book greatly highlights the necessary balances underlying compulsory B2B data sharing and raises awareness about the crucial need to take the risks involved into consideration. It will be highly appreciated by policymakers, academics and private actors interested in issues linked to competition law in the digital environment, regulation of platforms, data governance or the interaction between competition law and personal data protection law.

Building an Effective Security Program for Distributed Energy Resources and Systems Build a critical and effective security program for DERs Building an Effective Security Program for Distributed Energy Resources and Systems requires a unified approach to establishing a critical security program for DER systems and Smart Grid applications. The methodology provided integrates systems security engineering principles, techniques, standards, and best practices. This publication introduces engineers on the design, implementation, and maintenance of a security program for distributed energy resources (DERs), smart grid, and industrial control systems. It provides security professionals with understanding the specific requirements of industrial control systems and real-time constrained applications for power systems. This book: Describes the cybersecurity needs for DERs and power grid as critical infrastructure Introduces the information security principles to assess and manage the security and privacy risks of the emerging Smart Grid technologies Outlines the functions of the security program as well as the scope and differences between traditional IT system security requirements and those required for industrial control systems such as SCADA systems Offers a full array of resources— cybersecurity concepts, frameworks, and emerging trends Security Professionals and Engineers can use Building an Effective Security Program for Distributed Energy Resources and Systems as a reliable resource that is dedicated to the essential topic of security for distributed energy resources and power grids. They will find standards, guidelines, and recommendations from standards organizations, such as ISO, IEC, NIST, IEEE, ENISA, ISA, ISACA, and ISF, conveniently included for reference within chapters.

Computer Safety, Reliability, and Security

The Risk-Based Approach to Data Protection

Building an Effective Security Program for Distributed Energy Resources and Systems

Handbook of Research on Entrepreneurial Ecosystems and Social Dynamics in a Globalized World

15th International Workshops IWCSN 2014, Org2 2014, PCS 2014, and QUAT 2014, Thessaloniki, Greece, October 12-14, 2014, Revised Selected Papers

Effective Cybersecurity

Algorithms, Digitization and Regulation

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.

The book includes selected high-quality research papers presented at the Third International Congress on Information and Communication Technology held at Brunel University, London on February 27–28, 2018. It discusses emerging topics pertaining to information and communication technology (ICT) for managerial applications, e-governance, e-agriculture, e-education and computing technologies, the Internet of Things (IOT), and e-mining. Written by experts and researchers working on ICT, the book is suitable for new researchers involved in advanced studies.

This book constitutes the revised selected papers of the combined workshops on Web Information Systems Engineering, WISE 2014, held in Thessaloniki, Greece, in October 2014. The 19 selected papers presented were carefully revised and report from the four workshops: computational social networks, IWCSN 2014, enterprise social networks, Org2 2014, personalization and context-awareness in cloud and service computing, PCS 2014, and data quality and trust in big data, QUAT 2014.

This book celebrates the 40th anniversary of the creation of the CRID and the 10th anniversary of its successor, the CRIDS. It gathers twenty-one very high quality contributions on extremely interesting and topical aspects of data protection. The authors come from Europe as well as from the United States of America and Canada. Their contributions have been grouped as follows: 1° ICT Governance; 2° Commodification & Competition; 3° Secret surveillance; 4° Whistleblowing; 5° Social Medias, Web Archiving & Journalism; 6° Automated individual decision-making; 7° Data Security; 8° Privacy by design; 9° Health, AI, Scientific Research & Post-Mortem Privacy. This book is intended for all academics, researchers, students and practitioners who have an interest in privacy and data protection.

Handbook of Research on Cyber Crime and Information Privacy

Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications

Digital Supply Chain and Logistics with IoT

Trust, Privacy and Security in Digital Business

Concepts, Methodologies, Tools, and Applications

Information Privacy Engineering and Privacy by Design

Data Protection and Privacy: (In)visibilities and Infrastructures

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.

This book presents the implementation of novel concepts and solutions, which allows to enhance the cyber security of administrative and industrial systems and the resilience of economies and societies to cyber and hybrid threats. This goal can be achieved by rigorous information sharing, enhanced situational awareness, advanced protection of industrial processes and critical infrastructures, and proper account of the human factor, as well as by adequate methods and tools for analysis of big data, including data from social networks, to find best ways to counter hybrid influence. The implementation of these methods and tools is examined here as part of the process of digital transformation through incorporation of advanced information technologies, knowledge management, training and testing environments, and organizational networking. The book is of benefit to practitioners and researchers in the field of cyber security and protection against hybrid threats, as well as to policymakers and senior managers with responsibilities in information and knowledge management, security policies, and human resource management and training.

This book explores how data about our everyday online behaviour are collected and how they are processed in various ways by algorithms powered by Artificial Intelligence (AI) and Machine Learning (ML). The book investigates the socioeconomic effects of these technologies, and the evolving regulatory landscape that is aiming to nurture the positive effects of these technology evolutions while at the same time curbing possible negative practices. The volume scrutinizes growing concerns on how algorithmic decisions can sometimes be biased and discriminative; how autonomous systems can possibly disrupt and impact the labour markets, resulting in job losses in several traditional sectors while creating unprecedented opportunities in others; the rapid evolution of social media that can be addictive at times resulting in associated mental health issues; and the way digital Identities are evolving around the world and their impact on provisioning of government services. The book also provides an in-depth understanding of regulations around the world to protect privacy of data subjects in the online world; a glimpse of how data is used as a digital public good in combating Covid pandemic; and how ethical standards in autonomous systems are evolving in the digital world. A timely intervention in this fast-evolving field, this book will be useful for scholars and researchers of digital humanities, business and management, internet studies, data sciences, political studies, urban sociology, law, media and cultural studies, sociology, cultural anthropology, and science and technology studies. It will also be of immense interest to the general readers seeking insights on daily digital lives.

In recent years, industries have transitioned into the digital realm, as companies and organizations are adopting certain forms of technology to assist in information storage and efficient methods of production. This dependence has significantly increased the risk of cyber crime and breaches in data security. Fortunately, research in the area of cyber security and information protection is flourishing; however, it is the responsibility of industry professionals to keep pace with the current trends within this field. The Handbook of Research on Cyber Crime and Information Privacy is a collection of innovative research on the modern methods of crime and misconduct within cyber space. It presents novel solutions to securing and preserving digital information through practical examples and case studies. While highlighting topics including virus detection, surveillance technology, and social networks, this book is ideally designed for cybersecurity professionals, researchers, developers, practitioners, programmers, computer scientists, academicians, security analysts, educators, and students seeking up-to-date research on advanced approaches and developments in cyber security and information protection.

Privacy and Identity Management. Data for Better Living: AI and Privacy

Guide to Security Assurance for Cloud Computing

AI Approaches to the Complexity of Legal Systems XI-XII

Imposing Data Sharing among Private Actors
Data-centric Living
Practical Guide, Methods, Tools and Use Cases for Industry
Inventive Approaches for Technology Integration and Information Resources Management

The privacy policies of online social network (OSN) service providers are criticised as falling short of satisfying their users' privacy expectations letting huge quantities of their personally identifiable information (PII) exposed to unknown audiences. The purpose of this paper is twofold: to assess the conformance of the privacy policies applied in the five topmost leading OSNs to an internationally acknowledged benchmark such as the ISO 29100:2011 standard, and to propose improvements based on the findings of the assessment. Further, as serious mismatches between these privacy policies and the adherence criteria set out in the ISO 29100:2011 standard were identified, a data lifecycle model is proposed as the basis for an improved OSN privacy policy. A restructuring of the existing policies according to the data lifecycle model will allow them to enjoy characteristics that are known to be important in forming users' perceptions.

Liberal Democracy and the New Media is about the relationship between the media and the liberal democratic state, which is changing rapidly under the pressures of a global communications revolution. The book uses European and international law and policy to examine how that once intimate relationship is being transformed. The Media and the State explores key contemporary media issues, including the protection of cultural diversity, the promotion ofpluralism and other democratic media policies, the safeguard of state information, the protection of reputation and privacy, and the control of harmful and offensive content. It captures the extraordinary impact ofthe liberal media model on European and international law as well as exploring its profound weaknesses.

The first work to examine data privacy laws across Asia, covering all 26 countries and separate jurisdictions, and with in-depth analysis of the 14 which have specialised data privacy laws. Professor Greenleaf demonstrates the increasing world-wide significance of data privacy and the international context of the development of national data privacy laws as well as assessing the laws, their powers and their enforcement against international standards.

This book presents selected examples of digitalization in the age of digital change. It is divided into two sections: "Digital Innovation," which features new technologies that stimulate and enable new business opportunities; and "Digital Business Transformation," comprising business and management concepts that employ specific technological solutions for their practical implementation. Combining new insights from research, teaching and management, including digital transformation, e-business, knowledge representation, human-computer interaction, and business optimization, the book highlights the breadth of research as well as its meaningful and relevant transfer into practice. It is intended for academics seeking inspiration, as well as for leaders wanting to tap the potential of the latest trends to take society and their business to the next level.

7th International Symposium, ISoLA 2016, Imperial, Corfu, Greece, October 10–14, 2016, Proceedings, Part I
Transportation and Power Grid in Smart Cities
New Trends in Business Information Systems and Technology
Privacy and Data Protection Challenges in the Distributed Era
Communication Networks and Services
Towards Improving Existing Online Social Networks' Privacy Policies
12th International Conference, TrustBus 2015, Valencia, Spain, September 1-2, 2015, Proceedings

ISO/IEC 27701:2019: An introduction to privacy information management offers a concise introduction to the Standard, aiding those organisations looking to improve their privacy information management regime, particularly where ISO/IEC 27701:2019 is involved. This practical and didactic text/reference discusses the leading edge of secure cloud computing, exploring the essential concepts and principles, tools, techniques and deployment models in this field. Enlightening perspectives are presented by an international collection of pre-eminent authorities in cloud security assurance from both academia and industry. Topics and features: · Describes the important general concepts and principles of security assurance in cloud-based environments · Presents applications and approaches to cloud security that illustrate the current state of the art · Reviews pertinent issues in relation to challenges that prevent organizations moving to cloud architectures · Provides relevant theoretical frameworks and the latest empirical research findings · Discusses real-world vulnerabilities of cloud-based software in order to address the challenges of securing distributed software · Highlights the practicalities of cloud security, and how applications can assure and comply with legislation · Includes review questions at the end of each chapter This Guide to Security Assurance for Cloud Computing will be of great benefit to a broad audience covering enterprise architects, business analysts and leaders, IT infrastructure managers, cloud security engineers and consultants, and application developers involved in system design and implementation. The work is also suitable as a textbook for university instructors, with the outline for a possible course structure suggested in the preface. The

editors are all members of the Computing and Mathematics Department at the University of Derby, UK, where Dr. Shao Ying Zhu serves as a Senior Lecturer in Computing, Dr. Richard Hill as a Professor and Head of the Computing and Mathematics Department, and Dr. Marcello Trovati as a Senior Lecturer in Mathematics. The other publications of the editors include the Springer titles Big-Data Analytics and Cloud Computing, Guide to Cloud Computing and Cloud Computing for Enterprise Architectures.

This Research Handbook is an insightful overview of the key rules, concepts and tensions in privacy and data protection law. It highlights the increasing global significance of this area of law, illustrating the many complexities in the field through a blend of theoretical and empirical perspectives.

With the increasing worldwide trend in population migration into urban centers, we are beginning to see the emergence of the kinds of mega-cities which were once the stuff of science fiction. It is clear to most urban planners and developers that accommodating the needs of the tens of millions of inhabitants of those megalopolises in an orderly and uninterrupted manner will require the seamless integration of and real-time monitoring and response services for public utilities and transportation systems. Part speculative look into the future of the world’s urban centers, part technical blueprint, this visionary book helps lay the groundwork for the communication networks and services on which tomorrow’s “smart cities” will run. Written by a uniquely well-qualified author team, this book provides detailed insights into the technical requirements for the wireless sensor and actuator networks required to make smart cities a reality.

European and International Media Law

13th International Conference, TrustBus 2016, Porto, Portugal, September 7-8, 2016, Proceedings

Digital Transformation, Cyber Security and Resilience of Modern Societies

Third International Congress on Information and Communication Technology

Leveraging Applications of Formal Methods, Verification and Validation: Foundational Techniques

AICOL International Workshops 2018 and 2020: AICOL-XI@JURIX 2018, AICOL-XII@JURIX 2020, XAILA@JURIX 2020, Revised Selected Papers

A Value-Based System Design Approach

The Practical, Comprehensive Guide to Applying Cybersecurity Best Practices and Standards in Real Environments In Effective Cybersecurity, William Stallings introduces the technology, operational procedures, and management practices needed for successful cybersecurity. Stallings makes extensive use of standards and best practices documents that are often used to guide or mandate cybersecurity implementation. Going beyond these, he offers in-depth tutorials on the “how” of implementation, integrated into a unified framework and realistic plan of action. Each chapter contains a clear technical overview, as well as a detailed discussion of action items and appropriate policies. Stallings offers many pedagogical features designed to help readers master the material: clear learning objectives, keyword lists, review questions, and QR codes linking to relevant standards documents and web resources. Effective Cybersecurity aligns with the comprehensive Information Security Forum document “The Standard of Good Practice for Information Security,” extending ISF’s work with extensive insights from ISO, NIST, COBIT, other official standards and guidelines, and modern professional, academic, and industry literature. • Understand the cybersecurity discipline and the role of standards and best practices • Define security governance, assess risks, and manage strategy and tactics • Safeguard information and privacy, and ensure GDPR compliance • Harden systems across the system development life cycle (SDLC) • Protect servers, virtualized systems, and storage • Secure networks and electronic communications, from email to VoIP • Apply the most appropriate methods for user authentication • Mitigate security risks in supply chains and cloud environments This knowledge is indispensable to every cybersecurity professional. Stallings presents it systematically and coherently, making it practical and actionable.

This book constitutes the refereed proceedings of the 12th International Conference on Trust, Privacy and Security in Digital Business, TrustBus 2015, held in Valencia, Spain, in September 2015 in conjunction with DEXA 2015. The 17 revised full papers presented were carefully reviewed and selected from 45 submissions. The papers are organized in the following topical sections: access control; trust and reputation in pervasive environments; trust and privacy issues in mobile environments; security and privacy in the cloud; security policies/usability issues; and privacy requirements and privacy audit.

The concept of a risk-based approach to data protection came to the fore during the overhaul process of the EU's General Data Protection Regulation (GDPR). At its core, it consists of endowing the regulated organizations that process personal data with increased responsibility for complying with data protection mandates. Such increased compliance duties are performed through risk management tools. This book provides a comprehensive analysis of this legal and policy development, which considers a legal, historical, and theoretical perspective. By framing the risk-based approach as a sui generis implementation of a specific regulation model 'known as meta regulation, this book provides a recollection of the policy developments that led to the adoption of the risk-based approach in light of regulation theory and debates. It also discusses a number of salient issues pertaining to the risk-based approach, such as its rationale, scope, and meaning; the role for regulators; and its potential and limits. The book also looks at they way it has been undertaken in major statutes with a focus on key provisions, such as data protection impact assessments or accountability. Finally, the book devotes considerable attention to the notion of risk. It explains key terms such as risk assessment and management. It discusses in-depth the role of harms in data protection, the meaning of a data protection risk, and the difference between risks and harms. It also critically analyses prevalent data protection risk management methodologies and explains the most important caveats for managing data protection risks.

Explaining how ubiquitous computing is rapidly changing our private and professional lives, Ethical IT Innovation: A Value-Based System Design Approach stands at the intersection of computer science, philosophy, and management and integrates theories and frameworks from all three domains. The book explores the latest thinking on computer ethics, including the normative ethical theories currently shaping the debate over the good and bad consequences of technology. It begins by making the case as to why IT professionals, managers, and engineers must consider the ethical issues when designing IT systems, and then uses

a recognized system development process model as the structural baseline for subsequent chapters. For each system development phase, the author discusses: the ethical issues that must be considered, who must consider them, and how that thought process can be most productive. In this way, an 'Ethical SDLC' (System Development Life Cycle) is created. The book presents an extensive case study that applies the "Ethical SDLC" to the example of privacy protection in RFID enabled environments. It explains how privacy can be built into systems and illustrates how ethical decisions can be consciously made at each stage of development. The final chapter revisits the old debate of engineers' ethical accountability as well as the role of management. Explaining the normative theories of computer ethics, the book explores the ethical accountability of developers as well as stakeholders. It also provides questions at the end of each chapter that examine the ethical dimensions of the various development activities.
Security and Privacy in the Internet of Things: Challenges and Solutions
Cyber Security

Privacy and Identity Management. Time for a Revolution?
Values, Norms and Global Politics
SAFECOMP 2019 Workshops, ASSURE, DECSoS, SASSUR, STRIVE, and WAISE, Turku, Finland, September 10, 2019, Proceedings
Trade and Human Rights Perspectives

Today□s management world continually relies on technological efficiency to function and perform at a high standard. As technology becomes a greater part in many fields, understanding and managing this factor is integral for organizations. Inventive Approaches for Technology Integration and Information Resources Management provides an overview and analysis of knowledge management in sustainability, emergency preparedness, and IT, among other fields integral to the modern technological era. By providing a foundation for innovative practices in using technology and information resources, this publication is essential for practitioners and professionals, as well as undergraduate/graduate students and academicians.

The two-volume set LNCS 9952 and LNCS 9953 constitutes the refereed proceedings of the 7th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation, ISoLA 2016, held in Imperial, Corfu, Greece, in October 2016. The papers presented in this volume were carefully reviewed and selected for inclusion in the proceedings. Featuring a track introduction to each section, the papers are organized in topical sections named: statistical model checking; evaluation and reproducibility of program analysis and verification; ModSyn-PP: modular synthesis of programs and processes; semantic heterogeneity in the formal development of complex systems; static and runtime verification: competitors or friends?; rigorous engineering of collective adaptive systems; correctness-by-construction and post-hoc verification: friends or foes?; privacy and security issues in information systems; towards a unified view of modeling and programming; formal methods and safety certification: challenges in the railways domain; RVE: runtime verification and enforcement, the (industrial) application perspective; variability modeling for scalable software evolution; detecting and understanding software doping; learning systems: machine-learning in software products and learning-based analysis of software systems; testing the internet of things; doctoral symposium; industrial track; RERS challenge; and STRESS.

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

Privacy for the Smart Grid provides easy-to-understand guidance on data privacy issues and the implications for creating privacy risk management programs, along with privacy policies and practices required to ensure Smart Grid privacy. It addresses privacy in electric, natural gas, and water grids from two different perspectives of the topic, one from a Smart Grid expert and another from a privacy and information security expert. While considering privacy in the Smart Grid, the book also examines the data created by Smart Grid technologies and machine-to-machine applications.

Web Information Systems Engineering – WISE 2014 Workshops
Data Privacy for the Smart Grid
Implementing the ISO/IEC 27001:2013 ISMS Standard
Cybersecurity Law, Standards and Regulations, 2nd Edition

1979-2019 Celebrating 40 Years of Privacy and Data Protection at the CRIDS
Digital Innovation and Digital Business Transformation
ICICT 2018, London

Organizations of all kinds are recognizing the crucial importance of protecting privacy. Their customers, employees, and other stakeholders demand it. Today, failures to safeguard privacy can destroy organizational reputations – and even the organizations themselves. But implementing effective privacy protection is difficult, and there are few comprehensive resources for those tasked with doing so. In Information Privacy Engineering and Privacy by Design, renowned information technology author William Stallings brings together the comprehensive and practical guidance you need to succeed. Stallings shows how to apply today's consensus best practices and widely-accepted standards documents in your environment, leveraging policy, procedures, and technology to meet legal and regulatory requirements and protect everyone who depends on you. Like Stallings' other award-winning texts, this guide is designed to help readers quickly find the information and gain the mastery needed to implement effective privacy. Coverage includes: Planning for privacy: Approaches for managing and controlling the privacy control function; how to define your IT environment's requirements; and how to develop appropriate policies and procedures for it Privacy threats: Understanding and identifying the full range of threats to privacy in information collection, storage, processing, access, and dissemination Information privacy technology: Satisfying the privacy requirements you've defined by using technical controls, privacy policies, employee awareness, acceptable use policies, and other techniques Legal and regulatory requirements: Understanding GDPR as well as the current spectrum of U.S. privacy regulations, with insight for mapping regulatory requirements to IT actions

The Internet of Things (IoT) can be defined as any network of things capable of generating, storing and exchanging data, and in some cases acting on it. This new form of seamless connectivity has many applications: smart cities, smart grids for energy management, intelligent transport, environmental monitoring, healthcare systems, etc. and EU policymakers were quick to realize that machine-to-machine communication and the IoT were going to be vital to economic development. It was also clear that the security of such systems would be of paramount importance and, following the European Commission's Cybersecurity Strategy of the European Union in 2013, the EU's Horizon 2020 programme was set up to explore available options and possible approaches to addressing the security and privacy issues of the IoT. This book presents 10 papers which have emerged from the research of the Horizon 2020 and CHIST-ERA programmes, and which address a wide cross-section of projects ranging from the secure management of personal data and the specific challenges of the IoT with respect to the GDPR, through access control within a highly dynamic IoT environment and increasing trust with distributed ledger technologies, to new cryptographic approaches as a counter-measure for side-channel attacks and the vulnerabilities of IoT-based ambient assisted living systems. The security and safety of the Internet of Things will remain high on the agenda of policymakers for the foreseeable future, and this book provides an overview for all those with an interest in the field.

Web Information Systems Engineering – WISE 2014 Workshops15th International Workshops IWCSN 2014, Org2 2014, PCS 2014, and QUAT 2014, Thessaloniki, Greece, October 12-14, 2014, Revised Selected PapersSpringer

El objetivo del libro es presentar a lectores (juristas o no) interesados varias impresiones sobre las características del Derecho y el Estado de la sociedad en red en estos momentos, , iniciada la segunda década del siglo XXI, según la libre visión de los autores expresada desde su respectivo contexto y experiencia: trabajan, conjuntamente, en Facultades de Derecho en Europa (España, Reino Unido y Finlandia) y Brasil.

Research Handbook on Privacy and Data Protection Law

10th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School, Edinburgh, UK, August 16-21, 2015, Revised Selected Papers

14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers

A Guide to Using Best Practices and Standards

ISO/IEC 27701:2019: An introduction to privacy information management

Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices

A Tale of Evolving Balances

Globalization demands the construction of new business methods to enable companies to remain highly competitive. Due to this demand, cultural differences are now being implemented into policies and procedures as companies expand and seek to collaborate with international entrepreneurs. The Handbook of Research on Entrepreneurial Ecosystems and Social Dynamics in a Globalized World is a pivotal reference source for emergent aspects of internationalization and regional development in an entrepreneurial context. Featuring extensive coverage on relevant areas such as digital entrepreneurship, sustainability, and financial performance, this publication is an ideal resource for academics, public and private institutions, developers, professors, researchers, and post-graduate students seeking current research on globalized entrepreneurship.

Technological advancement saves time, ease of mobility, providing better communication means, cost efficiency, improved banking, better learning techniques, though safety and security are still questionable in aspects mentioned above. Cyber-attacks, crime,

fraudulent are still increasing in recent years. Today, cyber security is widely viewed as a matter of pressing national importance. Many elements of cyberspace are notoriously vulnerable to an expanding range of attacks by a spectrum of hackers, criminals and terrorists. This book aims to collect the information both thematic as well as research-oriented from various personnel working in the various fields having different experiences to provide the essentials regarding what Cyber security is really about and not the perception of it being related purely to hacking activity. It will provide the fundamental considerations for those who are interested in or thinking of changing career into the field of Cyber Security. It will also improve a reader's understanding of key terminology commonly used, nowadays, surrounding internet issues as they arise. The focus of the authors of various chapters in this book is on cyber security, cyber attacks, cyber crime, cloud security, cyber law, protection of women and children in cyber world & cyber space, analysis of cyber feminist campaign, data privacy and security issues in cloud computing, Mobile or Media addiction, Ransomewares, social networking, threats and impacts of cyber security.

This book constitutes the proceedings of the Workshops held in conjunction with SAFECOMP 2019, 38th International Conference on Computer Safety, Reliability and Security, in September 2019 in Turku, Finland. The 32 regular papers included in this volume were carefully reviewed and selected from 43 submissions; the book also contains two invited papers. The workshops included in this volume are: ASSURE 2019: 7th International Workshop on Assurance Cases for Software-Intensive Systems DECSoS 2019: 14th ERCIM/EWICS/ARTEMIS Workshop on Dependable Smart Embedded and Cyber-Physical Systems and Systems-of-Systems SASSUR 2019: 8th International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems STRIVE 2019: Second International Workshop on Safety, securiTy, and pRivacy In automotiVe systEms WAISE 2019: Second International Workshop on Artificial Intelligence Safety Engineering

This book contains selected papers presented at the 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School on Privacy and Identity Management, held in Windisch, Switzerland, in August 2019. The 22 full papers included in this volume were carefully reviewed and selected from 31 submissions. Also included are reviewed papers summarizing the results of workshops and tutorials that were held at the Summer School as well as papers contributed by several of the invited speakers. The papers combine interdisciplinary approaches to bring together a host of perspectives, which are reflected in the topical sections: language and privacy; law, ethics and AI; biometrics and privacy; tools supporting data protection compliance; privacy classification and security assessment; privacy enhancing technologies in specific contexts. The chapters "What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking" and "Privacy Implications of Voice and Speech Analysis - Information Disclosure by Inference" are open access under a CC BY 4.0 license at link.springer.com.

Research Anthology on Privatizing and Securing Data

Liberal Democracy, Trade, and the New Media

Deep Diving into Data Protection

Asian Data Privacy Laws

El derecho de la sociedad en red

Ethical IT Innovation

This book constitutes the refereed proceedings of the 13th International Conference on Trust, Privacy and Security in Digital Business, TrustBus 2016, held in Porto, Portugal, in September 2016 in conjunction with DEXA 2016. The 8 revised full papers presented were carefully reviewed and selected from 18 submissions. The papers are organized in the following topical sections: security, privacy and trust in eServices; security and privacy in cloud computing; privacy requirements; and information audit and trust.

This book contains a range of keynote papers and submitted papers presented at the 10th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School, held in Edinburgh, UK, in August 2015. The 14 revised full papers included in this volume were carefully selected from a total of 43 submissions and were subject to a two-step review process. In addition, the volume contains 4 invited keynote papers. The papers cover a wide range of topics: cloud computing, privacy-enhancing technologies, accountability, measuring privacy and understanding risks, the future of privacy and data protection regulation, the US privacy

perspective, privacy and security, the PRISMS Decision System, engineering privacy, cryptography, surveillance, identity management, the European General Data Protection Regulation framework, communicating privacy issues to the general population, smart technologies, technology users' privacy preferences, sensitive applications, collaboration between humans and machines, and privacy and ethics.