Iso 27002 2013

Information Security Policy Development for Compliance
The Official (ISC)2 Guide to the CCSP CBK
ISO27001 / ISO27002
The Case for ISO27001:2013
The best practice handbook for a Microsoft® Windows® environment
Nine Steps to Success
Global Standards and Publications
Research Anthology on Business Aspects of Cybersecurity
IT Governance
Implementing the ISO/IEC 27001:2013 ISMS Standard
IT Governance and Information Security
Information Technology
Principles and Practices
Do-it-yourself and Get-certified
An International Guide to Data Security and ISO 27001/ISO 27002
An ISO27001:2013 Implementation Overview, Third edition
Information Security Risk Management for ISO27001/ISO27002
Privacy and Data Protection Challenges in the Distributed Era
IT Governance
Computer Security
Securing Critical Infrastructure Networks for

Smart Grid, SCADA, and Other Industrial Control Systems
Principles of Information Security
Information Security Risk Management for ISO 27001/ISO 27002, third edition
Developing Cybersecurity Programs and Policies
Industrial Network Security
Application security in the ISO27001:2013 Environment
ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0
Foundations of Information Security Based on Iso27001 and Iso27002
ISO 27001 controls – A guide to implementing and auditing
A Pocket Guide
Handbook of Research on Multidisciplinary Approaches to Entrepreneurship, Innovation, and ICTs
Protecting Critical Infrastructure at the State and Local Level
Guides, Standards, and Frameworks
ICCWS 2020 15th International Conference on Cyber Warfare and Security
An Introduction to Information Security and ISO27001:2013

LENNON BAILEY

Information Security Policy Development for Compliance 5starcooks Presents the compelling business case for implementing

ISO27001:2013 to protect your information assets. Perfect for supporting an ISO27001 project proposal.

The Official (ISC)2 Guide to the CCSP CBK John Wiley & Sons

"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. ""

ISO27001 / ISO27002

IGI Global

Application Security in the ISO 27001:2013 Environment explains how organisations can implement and maintain effective security practices to protect their web applications – and the servers on which they reside – as part of a wider information security management system by following the guidance set out in the international standard for information security management, ISO

27001. The book describes the methods used by criminal hackers to attack organisations via their web applications and provides a detailed explanation of how you can combat such attacks by employing the guidance and controls set out in ISO 27001. Product overviewSecond edition, updated to reflect ISO 27001:2013 as well as best practices relating to cryptography, including the PCI SSC's denigration of SSL in favour of TLS.Provides a full introduction to ISO 27001 and information security management systems, including implementation guidance.Describes risk assessment, management and treatment approaches.Examines common types of web app security attack, including injection attacks, cross-site scripting, and attacks on authentication and session management, explaining how each can compromise ISO 27001 control objectives and showing how to test for each attack type.Discusses the ISO 27001 controls relevant to application security.Lists useful web app security metrics and their relevance to ISO 27001 controls.Provides a four-step approach to threat profiling, and describes application security review and testing approaches.Sets out guidelines and the ISO 27001 controls relevant to them, covering:input validationauthenticatio

nauthorisationsensitive data handling and the use of TLS rather than SSLsession managementerror handling and loggingDescribes the importance of security as part of the web app development process The Case for ISO27001:2013 IT Governance Ltd Currently, most organizations are dependent on IS/ICT in order to support their business strategies. IS/ICT can promote the implementation of strategies and enhancers of optimization of the various aspects of the business. In market enterprises and social organizations, digital economy and ICTs are important tools that can empower social entrepreneurship initiatives to develop, fund, and implement new and innovative solutions to social, cultural, and environmental problems. The Handbook of Research on Multidisciplinary Approaches to Entrepreneurship, Innovation, and ICTs is an essential reference source that discusses the digitalization techniques of the modern workforce as well as important tools empowering social entrepreneurship initiatives. Featuring research on topics such as agile business analysis, multicultural workforce, and human resource management, this book is ideally designed for business managers, entrepreneurs, IT consultants, researchers, industry professionals, human

resource consultants, academicians, and students.

The best practice handbook for a Microsoft® Windows® environment Academic Conferences and publishing limited

The essential guide to effective IG strategy and practice Information Governance is a highly practical and deeply informative handbook for the implementation of effective Information Governance (IG) procedures and strategies. A critical facet of any mid- to large-sized company, this “super-discipline” has expanded to cover the management and output of information across the entire organization; from email, social media, and cloud computing to electronic records and documents, the IG umbrella now covers nearly every aspect of your business. As more and more everyday business is conducted electronically, the need for robust internal management and compliance grows accordingly. This book offers big-picture guidance on effective IG, with particular emphasis on document and records management best practices. Step-by-step strategy development guidance is backed by expert insight and crucial advice from a leading authority in the field. This new second edition has been updated to align with the latest practices and regulations, providing an up-to-date understanding of critical IG concepts and practices. Explore the

many controls and strategies under the IG umbrella Understand why a dedicated IG function is needed in today's organizations Adopt accepted best practices that manage risk in the use of electronic documents and data Learn how IG and IT technologies are used to control, monitor, and enforce information access and security policy IG strategy must cover legal demands and external regulatory requirements as well as internal governance objectives; integrating such a broad spectrum of demands into workable policy requires a deep understanding of key concepts and technologies, as well as a clear familiarity with the most current iterations of various requirements. Information Governance distills the best of IG into a primer for effective action.

Nine Steps to Success Springer Nature

Globally recognized and backed by the Cloud Security Alliance (CSA) and the (ISC)2 the CCSP credential is the ideal way to match marketability and credibility to your cloud security skill set. The Official (ISC)2 Guide to the CCSPSM CBK Second Edition is your ticket for expert insight through the 6 CCSP domains. You will find step-by-step guidance through real-life scenarios, illustrated examples, tables, best practices, and more. This Second Edition features clearer diagrams as well as refined explanations

based on extensive expert feedback. Sample questions help you reinforce what you have learned and prepare smarter. Numerous illustrated examples and tables are included to demonstrate concepts, frameworks and real-life scenarios. The book offers step-by-step guidance through each of CCSP's domains, including best practices and techniques used by the world's most experienced practitioners. Developed by (ISC)2, endorsed by the Cloud Security Alliance® (CSA) and compiled and reviewed by cloud security experts across the world, this book brings together a global, thorough perspective. The Official (ISC)2 Guide to the CCSP CBK should be utilized as your fundamental study tool in preparation for the CCSP exam and provides a comprehensive reference that will serve you for years to come.

Global Standards and Publications John Wiley & Sons Specifically oriented to the needs of information systems students, PRINCIPLES OF INFORMATION SECURITY, 5e delivers the latest technology and developments from the field. Taking a managerial approach, this bestseller teaches all the aspects of information security-not just the technical control perspective. It provides a broad review of the entire field of information security, background

on many related elements, and enough detail to facilitate understanding of the topic. It covers the terminology of the field, the history of the discipline, and an overview of how to manage an information security program. Current and relevant, the fifth edition includes the latest practices, fresh examples, updated material on technical security controls, emerging legislative issues, new coverage of digital forensics, and hands-on application of ethical issues in IS security. It is the ultimate resource for future business decision-makers. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Research Anthology on Business Aspects of Cybersecurity Springer Nature

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. IT Governance IT Governance Ltd Faced with the compliance requirements of increasingly punitive information and privacy-related regulation, as well as the proliferation of complex threats to information security, there is an urgent need for organizations to adopt IT governance best practice. IT Governance is a key international resource for managers in organizations of all sizes and across industries, and deals with the strategic and operational aspects of information security. Now in its seventh edition, the bestselling IT Governance provides guidance for companies looking to protect and enhance their information security management systems (ISMS) and protect themselves against cyber threats. The new edition covers changes in global regulation, particularly GDPR, and updates to standards in the ISO/IEC 27000 family, BS 7799-3:2017 (information security risk management) plus the latest standards on auditing. It also includes advice on the development and implementation of an ISMS that will meet the

ISO 27001 specification and how sector-specific standards can and should be factored in. With information on risk assessments, compliance, equipment and operations security, controls against malware and asset management, IT Governance is the definitive guide to implementing an effective information security management and governance system.

IT Governance Ltd

Machine learning and artificial intelligence are already widely applied to facilitate our daily lives, as well as scientific research, but with the world currently facing a global COVID-19 pandemic, their capacity to provide an important tool to support those searching for a way to combat the novel corona virus has never been more important. This book presents the proceedings of the International Conference on Machine Learning and Intelligent Systems (MLIS 2020), which was due to be held in Seoul, Korea, from 25-28 October 2020, but which was delivered as an online conference on the same dates due to COVID-19 restrictions. MLIS 2020 was the latest in a series of annual conferences that aim to provide a platform for exchanging knowledge about the most recent scientific and technological advances in the field of machine learning and intelligent systems. The annual conference also

strengthens links within the scientific community in related research areas. The book contains 53 papers, selected from more than 160 submissions and presented at MLIS 2020. Selection was based on the results of review and scored on: originality, scientific/practical significance, compelling logical reasoning and language. Topics covered include: data mining, image processing, neural networks, human health, natural language processing, video processing, computational intelligence, expert systems, human-computer interaction, deep learning, and robotics. Offering a current overview of research and developments in machine learning and artificial intelligence, the book will be of interest to all those working in the field.

Implementing the ISO/IEC 27001:2013 ISMS Standard Van Haren

As the sophistication of cyber-attacks increases, understanding how to defend critical infrastructure systems—energy production, water, gas, and other vital systems—becomes more important, and heavily mandated. Industrial Network Security, Second Edition arms you with the knowledge you need to understand the vulnerabilities of these distributed supervisory and control systems. The book examines the

unique protocols and applications that are the foundation of industrial control systems, and provides clear guidelines for their protection. This how-to guide gives you thorough understanding of the unique challenges facing critical infrastructures, new guidelines and security measures for critical infrastructure protection, knowledge of new and evolving security tools, and pointers on SCADA protocols and security implementation. All-new real-world examples of attacks against control systems, and more diagrams of systems Expanded coverage of protocols such as 61850, Ethernet/IP, CIP, ISA-99, and the evolution to IEC62443 Expanded coverage of Smart Grid security New coverage of signature-based detection, exploit-based vs. vulnerability-based detection, and signature reverse engineering

IT Governance and Information Security

CRC Press

Cybersecurity is vital for all businesses, regardless of sector. With constant threats and potential online dangers, businesses must remain aware of the current research and information available to them in order to protect themselves and their employees. Maintaining tight cybersecurity can be difficult for businesses as there are so many moving parts to contend with, but remaining vigilant and

having protective measures and training in place is essential for a successful company. The Research Anthology on Business Aspects of Cybersecurity considers all emerging aspects of cybersecurity in the business sector including frameworks, models, best practices, and emerging areas of interest. This comprehensive reference source is split into three sections with the first discussing audits and risk assessments that businesses can conduct to ensure the security of their systems. The second section covers training and awareness initiatives for staff that promotes a security culture. The final section discusses software and systems that can be used to secure and manage cybersecurity threats. Covering topics such as audit models, security behavior, and insider threats, it is ideal for businesses, business professionals, managers, security analysts, IT specialists, executives, academicians, researchers, computer engineers, graduate students, and practitioners.

Information Technology IOS Press

PART OF THE JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Revised and updated with the latest data in the field, the Second Edition of Managing Risk in Information Systems provides a comprehensive

overview of the SSCP(r) Risk, Response, and Recovery Domain in addition to providing a thorough overview of risk management and its implications on IT infrastructures and compliance. Written by industry experts, and using a wealth of examples and exercises, this book incorporates hands-on activities to walk the reader through the fundamentals of risk management, strategies and approaches for mitigating risk, and the anatomy of how to create a plan that reduces risk. Instructor's Material for Managing Risk in Information Systems include: PowerPoint Lecture Slides Instructor's Guide Course Syllabus Quiz & Exam Questions Case Scenarios/Handouts

Principles and Practices Van Haren

Ideal for information security managers, auditors, consultants and organisations preparing for ISO 27001 certification, this book will help readers understand the requirements of an ISMS (information security management system) based on ISO 27001.

Do-it-yourself and Get-certified CRC Press

The Complete Guide to Cybersecurity Risks and Controls presents the fundamental concepts of information and communication technology (ICT) governance and control. In this book, you will learn how to create a working, practical control structure that will

ensure the ongoing, day-to-day trustworthiness of ICT systems and data. The book explains how to establish systematic control functions and timely reporting procedures within a standard organizational framework and how to build auditable trust into the routine assurance of ICT operations. The book is based on the belief that ICT operation is a strategic governance issue rather than a technical concern. With the exponential growth of security breaches and the increasing dependency on external business partners to achieve organizational success, the effective use of ICT governance and enterprise-wide frameworks to guide the implementation of integrated security controls are critical in order to mitigate data theft. Surprisingly, many organizations do not have formal processes or policies to protect their assets from internal or external threats. The ICT governance and control process establishes a complete and correct set of managerial and technical control behaviors that ensures reliable monitoring and control of ICT operations. The body of knowledge for doing that is explained in this text. This body of knowledge process applies to all operational aspects of ICT responsibilities ranging from upper management policy making and planning, all the way down to

basic technology operation.
CreateSpace
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.

An International Guide to Data Security and ISO 27001/ISO 27002 Van Haren

Everything you need to know about information security programs and policies, in one book Clearly explains all facets of InfoSec program and policy planning, development, deployment, and management Thoroughly updated for today's challenges, laws, regulations, and best practices The perfect resource for anyone pursuing an information security management career ¿ In today's dangerous world, failures in information security can be catastrophic. Organizations must protect themselves. Protection begins with comprehensive, realistic policies. This up-to-date guide will help you create, deploy, and manage them. Complete and easy to understand, it explains key concepts and techniques through real-life examples. You'll master modern information security regulations and frameworks, and learn specific best-practice policies for key industry sectors, including finance, healthcare, online commerce, and small business. ¿ If you understand basic information security, you're ready to succeed with this book. You'll find projects, questions, exercises, examples, links to

valuable easy-to-adapt information security policies...everything you need to implement a successful information security program. ¿ Learn how to ·¿¿¿¿¿¿¿ Establish program objectives, elements, domains, and governance ·¿¿¿¿¿¿¿ Understand policies, standards, procedures, guidelines, and plans—and the differences among them ·¿¿¿¿¿¿¿ Write policies in “plain language,” with the right level of detail ·¿¿¿¿¿¿¿ Apply the Confidentiality, Integrity & Availability (CIA) security model ·¿¿¿¿¿¿¿ Use NIST resources and ISO/IEC 27000-series standards ·¿¿¿¿¿¿¿ Align security with business strategy ·¿¿¿¿¿¿¿ Define, inventory, and classify your information and systems ·¿¿¿¿¿¿¿ Systematically identify, prioritize, and manage InfoSec risks ·¿¿¿¿¿¿¿ Reduce “people-related” risks with role-based Security Education, Awareness, and Training (SETA) ·¿¿¿¿¿¿¿ Implement effective physical, environmental, communications, and operational security ·¿¿¿¿¿¿¿ Effectively manage access control ·¿¿¿¿¿¿¿ Secure the entire system development lifecycle ·¿¿¿¿¿¿¿ Respond to incidents and ensure continuity of operations ·¿¿¿¿¿¿¿ Comply with laws and regulations, including GLBA, HIPAA/HITECH, FISMA, state data security and notification rules, and PCI DSS ¿

An ISO27001:2013 Implementation

Overview, Third edition
IT Governance Publishing
Drawing on international best practice, including ISO/IEC 27005, NIST SP800-30 and BS7799-3, the book explains in practical detail how to carry out an information security risk assessment. It covers key topics, such as risk scales, threats and vulnerabilities, selection of controls, and roles and responsibilities, and includes advice on choosing risk assessment software.

Information Security Risk Management for ISO27001/ISO27002
IT Governance Publishing
Information is one of your organisation's most important resources. Keeping that information secure is therefore vital to your business. This handy pocket guide is an essential overview of two key information security standards that cover the formal requirements (ISO27001:2013) for creating an Information Security Management System (ISMS), and the best-practice recommendations (ISO27002:2013) for those responsible for initiating, implementing or maintaining it.

Privacy and Data Protection Challenges in the Distributed Era
IT Governance Ltd
Ideal for project managers, IT and security staff, this book plugs the gap in current guidance literature for ISO27001. ISO27001, the information security

management standard (ISMS), is providing a significant challenge for many organisations. One of the key areas of confusion is the relationship between the ISO27001 ISMS project manager and those responsible for implementing the technical controls.

Related with Iso 27002 2013:
© Iso 27002 2013 Wow Classic Wand Guide
© Iso 27002 2013 Wow Classic Wotlk Mining Guide
© Iso 27002 2013 Wotlk Yogg Saron Guide