Iso 27002 Version 2013

Information Security Risk Management for ISO 27001 / ISO 27002ISO27001:2013 Assessments Without TearsISO/IEC 38500: A pocket guide, second editionFundamentos de Segurança da InformaçãoInformation Security FundamentalsFoundations of Information Security Based on Iso27001 and Iso27002Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & SolutionsPrinciples of Information SecurityNine Steps to SuccessISO27001/ISO27002: Guida tascabileInformation Security based on ISO 27001/ISO 27002□□□□□□□□□□□□ISO27001 2013□□□□□□□□□□□□ISO 27001 controls – A guide to implementing and auditingInformation Security Risk Management for ISO 27001/ISO 27002, third editionEnterprise CybersecurityApplication security in the ISO27001:2013 EnvironmentIndustrial Network SecurityInformation Assurance and Security Education and TrainingISO27001 / ISO27002Information GovernanceDeveloping Cybersecurity Programs and PoliciesIT GovernanceIT GovernanceMike Meyers CompTIA Security+ Certification Passport, Sixth Edition (Exam SY0-601)Nine Steps to SuccessISO27001/ISO27002:2013Implementing Information Security based on ISO 27001/ISO 27002ECCWS2014-Proceedings of the 13th European Conference on Cyber warefare and SecurityThe Case for ISO 27001An Introduction to Information Security and ISO27001:2013Mobility in a Globalised World 2013Implementing the ISO/IEC 27001:2013 ISMS StandardUS National Cyber Security Strategy and Programs Handbook Volume 1 Strategic Information and DevelopmentsFoundations of Information Security Based on ISO27001 and ISO27002Foundations of Information Security Based on ISO27001 and ISO27002 - 3rd revised editionComputer SecurityBasiskennis informatiebeveiliging op basis van ISO27001 en ISO27002 - 2de herziene drukImplementing an Information Security Management SystemInformation Security Fundamentals, Second EditionMicrosoft Forefront Identity Manager 2010 R2 Handbook

Information Security Risk Management for ISO 27001 / ISO 27002

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.

ISO27001:2013 Assessments Without Tears

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 validationauthenticationauthorisationsensitive 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

ISO/IEC 38500: A pocket guide, second edition

Discover the simple steps to implementing information security standards using ISO 27001, the most popular information security standard across the world. You’ll see how it offers best practices to be followed, including the roles of all the stakeholders at the time of security framework implementation, post-implementation, and during monitoring of the implemented controls. Implementing an Information Security Management System provides implementation guidelines for ISO 27001:2013 to protect your information assets and ensure a safer enterprise environment. This book is a step-by-step guide on implementing secure ISMS for your organization. It will change the way you interpret and implement information security in your work area or organization. What You Will Learn Discover information safeguard methods Implement end-to-end information security Manage risk associated with information security Prepare for audit with associated roles and responsibilities Identify your information risk Protect your information assets Who This Book Is For Security professionals who implement and manage a security framework or security controls within their organization. This book can also be used by developers with a basic knowledge of security concepts to gain a strong understanding of security standards for an enterprise.

Fundamentos de Segurança da Informação

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

Information Security Fundamentals

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.

Foundations of Information Security Based on Iso27001 and Iso27002

Publisher's Note: Products purchased from Third Party sellers are not guaranteed by the publisher for quality, authenticity, or access to any online entitlements included with the product. This quick review, cram-style study guide offers 100% coverage of every topic on the latest version of the CompTIA Security+ exam This powerful exam preparation resource presents an accelerated review of the pertinent technology and covers all objectives for the CompTIA Security+ exam (exam SY0-601). Written in an all new Passport format developed by training expert Mike Meyers, the book enables you to focus on specific topics, determine areas of need, and tailor an effective course for study. Mike Meyers’ CompTIA Security+ Certification Passport, Sixth Edition (Exam SY0-601) features accurate practice exam questions and in-depth answer explanations as well as end-of-chapter bulleted summaries that reinforce salient points. Throughout, “Exam Tips” highlight important topics, “Note” icons define need-to-know terms, “Caution” notes alert you to potential pitfalls, and “Resource” icons specify resources for further information. • Provides complete coverage of every objective on exam SY0-601 • Online content includes 200 practice questions and additional performance-based questions • Written by a cybersecurity expert and edited by certification guru Mike Meyers

Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions

Developing an information security program that adheres to the principle of security as a business enabler must be the first step in an enterprise’s effort to build an effective security program. Following in the footsteps of its bestselling predecessor, Information Security Fundamentals, Second Edition provides information security professionals with a clear understanding of the fundamentals of security required to address the range of issues they will experience in the field. The book examines the elements of computer security, employee roles and responsibilities, and common threats. It discusses the legal requirements that impact security policies, including Sarbanes-Oxley, HIPAA, and the Gramm-Leach-Bliley Act. Detailing physical security requirements and controls, this updated edition offers a sample physical security policy and includes a complete list of tasks and objectives that make up an effective information protection program. Includes ten new chapters Broadens its coverage of regulations to include FISMA, PCI compliance, and foreign requirements Expands its coverage of compliance and governance issues Adds discussions of ISO 27001, ITIL, COSO, COBIT, and other frameworks Presents new information on mobile security issues Reorganizes the contents around ISO 27002 The book discusses organization-wide policies, their documentation, and legal and business requirements. It explains policy format with a focus on global, topic-specific, and application-specific policies. Following a review of asset classification, it explores access control, the components of physical security, and the foundations and processes of risk analysis and risk management. The text concludes by describing business continuity planning, preventive controls, recovery strategies, and how to conduct a business impact analysis. Each chapter in the book has been written by a different expert to ensure you gain the comprehensive understanding of what it takes to develop an effective information security program.

Principles of Information Security

All the Knowledge You Need to Build Cybersecurity Programs and Policies That Work Clearly presents best practices, governance frameworks, and key standards Includes focused coverage of healthcare, finance, and PCI DSS compliance An essential and invaluable guide for leaders, managers, and technical professionals Today, cyberattacks can place entire organizations at risk. Cybersecurity can no longer be delegated to specialists: success requires everyone to work together, from leaders on down. Developing Cybersecurity Programs and Policies offers start-to-finish guidance for establishing effective cybersecurity in any organization. Drawing on more than 20 years of real-world experience, Omar Santos presents realistic best practices for defining policy and governance, ensuring compliance, and collaborating to harden the entire organization. First, Santos shows how to develop workable cybersecurity policies and an effective framework for governing them. Next, he addresses risk management, asset management, and data loss prevention, showing how to align functions from HR to physical security. You'll discover best practices for securing communications, operations, and access; acquiring, developing, and maintaining technology; and responding to incidents. Santos concludes with detailed coverage of compliance in finance and healthcare, the crucial Payment Card Industry Data Security Standard (PCI DSS) standard, and the NIST Cybersecurity Framework. Whatever your current responsibilities, this guide will help you plan, manage, and lead cybersecurity–and safeguard all the assets that matter. Learn How To · Establish cybersecurity policies and governance that serve your organization's needs · Integrate cybersecurity program components into a coherent framework for action · Assess, prioritize, and manage security risk throughout the organization · Manage assets and prevent data loss · Work with HR to address human factors in cybersecurity · Harden your facilities and physical environment · Design effective policies for securing communications, operations, and access · Strengthen security throughout the information systems lifecycle · Plan for quick, effective incident response and ensure business continuity · Comply with rigorous regulations in finance and healthcare · Plan for PCI compliance to safely process payments · Explore and apply the guidance provided by the NIST Cybersecurity Framework

Nine Steps to Success

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

ISO27001/ISO27002: Guida tascabile

"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. ""

Information Security based on ISO 27001/ISO 27002

Proven and emerging strategies for addressing document and records management risk within the framework of information governance principles and best practices Information Governance (IG) is a rapidly emerging "super discipline" and is now being applied to electronic document and records management, email, social media, cloud computing, mobile computing, and, in fact, the management and output of information organization-wide. IG leverages information technologies to enforce policies, procedures and controls to manage information risk in compliance with legal and litigation demands, external regulatory requirements, and internal governance objectives. Information Governance: Concepts, Strategies, and Best Practices reveals how, and why, to utilize IG and leverage information technologies to control, monitor, and enforce information access and security policies. Written by one of the most recognized and published experts on information governance, including specialization in e-document security and electronic records management Provides big picture guidance on the imperative for information governance and best practice guidance on electronic document and records management Crucial advice and insights for compliance and risk managers, operations managers, corporate counsel, corporate records managers, legal administrators, information technology managers, archivists, knowledge managers, and information governance professionals IG sets the policies that control and manage the use of organizational information, including social media, mobile computing, cloud computing, email, instant messaging, and the use of e-documents and records. This extends to e-discovery planning and preparation. Information Governance: Concepts, Strategies, and Best Practices provides step-by-step guidance for developing information governance strategies and practices to manage risk in the use of electronic business documents and records.

□□□□□□□□□□□□□ISO27001 2013□□□□□□□□□□□□□

This book constitutes the refereed post-conference proceedings of the 5th International Workshop on Security of Industrial Control Systems and Cyber-Physical Systems, CyberICPS 2019, the Third International Workshop on Security and Privacy Requirements Engineering, SECPRE 2019, the First International Workshop on Security, Privacy, Organizations, and Systems Engineering, SPOSE 2019, and the Second International Workshop on Attacks and Defenses for Internet-of-Things, ADIoT 2019, held in Luxembourg City, Luxembourg, in September 2019, in conjunction with the 24th European Symposium on Research in Computer Security, ESORICS 2019. The CyberICPS Workshop received 13 submissions from which 5 full papers and 2 short papers were selected for presentation. They cover topics related to threats, vulnerabilities and risks that cyber-physical systems and industrial control systems face; cyber attacks that may be launched against such systems; and ways of detecting and responding to such attacks. From the SECPRE Workshop 9 full papers out of 14 submissions are included. The selected papers deal with aspects of security and privacy requirements assurance and evaluation; and security requirements elicitation and modelling and to GDPR compliance. The SPOSE Workshop received 7 submissions from which 3 full papers and 1 demo paper were accepted for publication. They demonstrate the possible spectrum for fruitful research at the intersection of security, privacy, organizational science, and systems engineering. From the ADIoT Workshop 5 full papers and 2 short papers out of 16 submissions are included. The papers focus on IoT attacks and defenses and discuss either practical or theoretical solutions to identify IoT vulnerabilities and IoT security mechanisms.

ISO 27001 controls – A guide to implementing and auditing

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

Information Security Risk Management for ISO 27001/ISO 27002, third edition

Learn to defend crucial ICS/SCADA infrastructure from devastating attacks the tried-and-true Hacking Exposed way This practical guide reveals the powerful weapons and devious methods cyber-terrorists use to compromise the devices, applications, and systems vital to oil and gas pipelines, electrical grids, and nuclear refineries. Written in the battle-tested Hacking Exposed style, the book arms you with the skills and tools necessary to defend against attacks that are debilitating—and potentially deadly. Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions explains vulnerabilities and attack vectors specific to ICS/SCADA protocols, applications, hardware, servers, and workstations. You will learn how hackers and malware, such as the infamous Stuxnet worm, can exploit them and disrupt critical processes, compromise safety, and bring production to a halt. The authors fully explain defense strategies and offer ready-to-deploy countermeasures. Each chapter features a real-world case study as well as notes, tips, and cautions. Features examples, code samples, and screenshots of ICS/SCADA-specific attacks Offers step-by-step vulnerability assessment and penetration test instruction Written by a team of ICS/SCADA security experts and edited by Hacking Exposed veteran Joel Scambray

Enterprise Cybersecurity

Helpful advice and reassurance about what an assessment involves, this guide is the perfect tool to prepare everybody in your organisation to play a positive part in your ISO27001 assessment.

Application security in the ISO27001:2013 Environment

Effective security rules and procedures do not exist for their own sake-they are put in place to protect critical assets, thereby supporting overall business objectives. Recognizing security as a business enabler is the first step in building a successful program. Information Security Fundamentals allows future security professionals to gain a solid understanding of the foundations of the field and the entire range of issues that practitioners must address. This book enables students to understand the key elements that comprise a successful information security program and eventually apply these concepts to their own efforts. The book examines the elements of computer security, employee roles and responsibilities, and common threats. It examines the need for management controls, policies and procedures, and risk analysis, and also presents a comprehensive list of tasks and objectives that make up a typical information protection program. The volume discusses organizationwide policies and their documentation, and legal and business requirements. It explains policy format, focusing on global, topic-specific, and application-specific policies. Following a review of asset classification, the book explores access control, the components of physical security, and the foundations and processes of risk analysis and risk management. Information Security Fundamentals concludes by describing business continuity planning, including preventive controls, recovery strategies, and ways to conduct a business impact analysis.

Industrial Network Security

This book is intended for everyone in an organization who wishes to have a basic understanding of information security. Knowledge about information security is important to all employees. It makes no difference if you work in a profit- or non-profit organization because the risks that organizations face are similar for all organizations.It clearly explains the approaches that most organizations can consider and implement which helps turn Information Security management into an approachable, effective and well-understood tool. It covers: The quality requirements an organization may have for information; The risks associated with these quality requirements; The countermeasures that are necessary to mitigate these risks; Ensuring business continuity in the event of a disaster; When and whether to report incidents outside the organization.The information security concepts in this revised edition are based on the ISO/IEC27001:2013 and ISO/IEC27002:2013 standards. But the text also refers to the other relevant international standards for information security. The text is structured as follows: Fundamental Principles of Security and Information security and Risk management. Architecture, processes and information, needed for basic understanding of what information security is about. Business Assets are discussed. Measures that can be taken to protect information assets. (Physical measures, technical measures and finally the organizational measures.)The primary objective of this book is to achieve awareness by students who want to apply for a basic information security examination. It is a source of information for the lecturer who wants to question information security students about their knowledge. Each chapter ends with a case study. In order to help with the understanding and coherence of each subject, these case studies include questions relating to the areas covered in the relevant chapters. Examples of recent events that illustrate the vulnerability of information are also included.This book is primarily developed as a study book for anyone who wants to pass the ISFS (Information Security Foundation) exam of EXIN. In an appendix an ISFS model exam is given, with feedback to all multiple choice options, so that it can be used as a training for the real ISFS exam.

Information Assurance and Security Education and Training

□□!

ISO27001 / ISO27002

Dit boek is in eerste instantie ontwikkeld als studieboek voor het examen Information Security Foundation based on ISO/IEC27002 van EXIN. De tweede druk is een ingrijpende herziening van de eerste druk (uit 2010), waarbij de inhoud is aangepast aan de nieuwe versie van de standaards: ISO/IEC 27001:2013 en ISO/IEC 27002:2013.Het bevat de basiskennis die onmisbaar is voor iedereen die beroepsmatig betrokken is bij informatiebeveiliging of IT. In al deze gevallen is informatiebeveiliging van belang, al is het maar vanwege de beveiligingsmaatregelen die een organisatie genomen heeft. Deze beveiligingsmaatregelen zijn soms afgedwongen door wet- en regelgeving. De inhoud is afgestemd op de Nederlandse context, zonder de internationale samenhang van informatiebeveiliging uit het oog te verliezen. Informatietechnologie kent immers geen grenzen.Kortom, dit boek is bedoeld voor iedereen die basiskennis van informatiebeveiliging op wil doen: Lijnmanagers die kennis moeten hebben van informatiebeveiliging omdat zij daarvoor binnen hun afdeling verantwoordelijk zijn. Directieleden en zelfstandigen zonder personeel omdat ook zij verantwoordelijk zijn voor het beschermen van de eigendommen en informatie die zij bezitten. Iedereen die thuis met computers werkt; ook dan is een bepaald gevoel van bewustwording belangrijk.

Information Governance

Based on his many years of first-hand experience with ISO27001, Alan Calder covers every single element of the ISO27001 project in simple, non-technical language, including: how to get management and board buy-in; how to get cross-organizational, cross functional buy-in; the gap analysis: how much you really need to do; how to integrate with ISO9001 and other management systems; how to structure and resource your project; whether to use consultants or do it yourself; the timetable and project plan; risk assessment methodologies and tools; the documentation challenges; how to choose a certification body.

Developing Cybersecurity Programs and Policies

Quickly understand the principles of information security.

IT Governance

Information security issues impact all organizations; however measures used to implement effective measures are often viewed as a businesses barrier costing a great deal of money. This practical title 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. All information security concepts in this book are based on the ISO/IEC 27001 and ISO/IEC 27002 standards. But the text also refers to the other relevant international standards for information security. The text is structures 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 book also contains many Case Studies which usefully demonstrate how theory translates into an operating environment This book is primarily developed as a study book for anyone who wants to pass the ISFS (Information Security Foundation) exam of EXIN. In an appendix an ISFS model exam is given, with feedback to all multiple choice options, so that it can be used as a training for the ‘real’ ISFS exam.

IT Governance

Mike Meyers CompTIA Security+ Certification Passport, Sixth Edition (Exam SY0-601)

Throughout the book, we will follow a fictional company, the case study will help you in implementing FIM 2010 R2. All the examples in the book will relate to this fictive company and you will be taken from design, to installation, to configuration of FIM 2010 R2. If you are implementing and managing FIM 2010 R2 in your business, then this book is for you. You will need to have a basic understanding of Microsoft based infrastructure using Active Directory. If you are new to Forefront Identity Management, the case-study approach of this book will help you to understand the concepts and implement them.

Nine Steps to Success

Information is the currency of the information age and in many cases is the most valuable asset possessed by an organisation. Information security management is the discipline that focuses on protecting and securing these assets against the threats of natural disasters, fraud and other criminal activity, user error and system failure. Effective information security can be defined as the ‘preservation of confidentiality, integrity and availability of information.’ This book describes the approach taken by many organisations to realise these objectives. It discusses how information security cannot be achieved through technological means alone, but should include factors such as the organisation’s approach to risk and pragmatic day-to-day business operations. This Management Guide provides an overview of the implementation of an Information Security Management System that conforms to the requirements of ISO/IEC 27001:2005 and which uses controls derived from ISO/IEC 17799:2005. It covers the following: Certification Risk Documentation and Project Management issues Process approach and the PDCA cycle Preparation for an Audit

ISO27001/ISO27002:2013

Proteggi le informazioni della tua organizzazione con ISO27001:2013 Le informazioni costituiscono una delle risorse più importanti della tua organizzazione, e proteggerne la sicurezza è di importanza vitale per la tua attività. Questa pratica guida tascabile costituisce una panoramica essenziale di due norme di sicurezza delle informazioni che prende in esame i requisiti formali (ISO27001:2013) per la creazione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI), e le procedure consigliate (ISO27002:2013) rivolte ai responsabili dell'avvio, dell'attuazione o del mantenimento di tale sistema. Un SGSI basato sulle norme ISO27001/ISO27002 presenta numerosi vantaggi: Una maggiore efficienza derivante dalla messa in atto di sistemi e procedure di sicurezza delle informazioni, consentendoti di concentrarti maggiormente sul tuo core business.Protegge il tuo patrimonio informativo da un gran numero di minacce informatiche, attività criminose, compromissione interna dei dati e errori di sistema.Gestisce i tuoi rischi in modo sistematico e stabilisce piani d'azione per eliminare o ridurre le minacce informatiche.Consente il rilevamento precoce di minacce o errori d'elaborazione e la loro rapida risoluzione.Qualè il passo successivo verso la certificazione? Puoi disporre una verifica indipendente del tuo SGSI per accertarne la conformità alle specifiche dello standard ISO27001 e, in caso di conformità, ottenere quindi la certificazione accreditata. Pubblichiamo una vasta gamma di compendi e libri documentativi sullo standard SGSI (come I Nove Passi Per il Successo) che possono aiutarti a conseguire tale obiettivo. IndiceIl gruppo di norme sulla sicurezza delle informazioni ISO/IEC 27000 ;Il contesto delle norme;Specifica e codice di comportamento a confronto;Il processo di certificazione;Il SGSI e l'ISO27001;Panoramica dell'ISO/IEC 27001:2013;Panoramica dell'ISO/IEC 27002:2013;Documentazione e registrazioni;Responsabilità della direzione;Approccio al processo e ciclo PDCA;Contesto, politica e campo di applicazione;Valutazione dei rischi;La dichiarazione di applicabilità;Attuazione;Check and Act;Riesame della direzione;Allegato A ISO27001

Implementing Information Security based on ISO 27001/ISO 27002

This useful pocket guide is an ideal introduction for those wanting to understand more about ISO 38500. It describes the scope, application and objectives of the Standard and outlines its six core principles.

ECCWS2014-Proceedings of the 13th European Conference on Cyber warefare and Security

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.

The Case for ISO 27001

Faced with constant and fast-evolving threats to information security and with a growing exposure to cyber risk, managers at all levels and in organizations of all sizes need a robust IT governance system. Now in its sixth edition, the bestselling IT Governance provides guidance for companies looking to protect and enhance their information security management systems and protect themselves against cyber threats. This version has been fully updated to take account of current cyber security and advanced persistent threats and reflects the latest regulatory and technical developments, including the 2013 updates to ISO 27001/ISO 27002. Changes for this edition include: updates in line with the revised ISO 27001 standard and accompanying ISO 27002 code of practice for information security controls; full coverage of changes to data-related regulations in different jurisdictions and advice on compliance; guidance on the options for continual improvement models and control frameworks made possible by the new standard; new developments in cyber risk and mitigation practices; guidance on the new information security risk assessment process and treatment requirements. Including coverage of key international markets, IT Governance is the definitive guide to implementing an effective information security management and governance system.

An Introduction to Information Security and ISO27001:2013

Information security means much more than a technology solution, and requires buy-in from senior managers and the collaboration of all staff in the organisation. By looking at ISO27001 and ISO27002 together, this pocket guide gives a wider view of what it means to implement an ISO27001 ISMS.

Mobility in a Globalised World 2013

For many companies, their intellectual property can often be more valuable than their physical assets. Having an effective IT governance strategy in place can protect this intellectual property, reducing the risk of theft and infringement. Data protection, privacy and breach regulations, computer misuse around investigatory powers are part of a complex and often competing range of requirements to which directors must respond. There is increasingly the need for an overarching information security framework that can provide context and coherence to compliance activity worldwide. IT Governance is a key resource for forward-thinking managers and executives at all levels, enabling them to understand how decisions about information technology in the organization should be made and monitored, and, in particular, how information security risks are best dealt with. The development of IT governance - which recognises the convergence between business practice and IT management - makes it essential for managers at all levels, and in organizations of all sizes, to understand how best to deal with information security risk. The new edition has been full updated to take account of the latest regulatory and technological developments, including the creation of the International Board for IT Governance Qualifications. IT Governance also includes new material on key international markets - including the UK and the US, Australia and South Africa.

Implementing the ISO/IEC 27001:2013 ISMS Standard

Este livro prático e de fácil leitura explica de forma clara as abordagens, ou políticas, de gerenciamento de segurança da informação que muitas organizações podem analisar e implementar nos seus negócios. Ele aborda: Os requisitos de qualidade que uma organização pode ter para informações.Os riscos associados com os requisitos de qualidade no uso das informações.As medidas defensivas que são necessárias para mitigar os riscos associados.Como garantir a continuidade do negócio em caso de desastre.Se e quando reportar acidentes para fora da organização. O livro também é útil para aqueles que desejam se preparar para um exame ISFS (Information Security Foundation) do EXIN. Um dos apêndices do livro traz um modelo do exame ISFS, incluindo comentários sobre as opções de resposta para as questões, ou seja, o anexo pode ser usado como treinamento para o exame oficial. Todos os conceitos de segurança da informação apresentados nesta versão do livro estão baseados nas normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013. Além disso, o texto também faz referência a outros padrões internacionais de segurança da informação relevantes, quando apropriado. O livro também traz um estudo de caso real ao longo dos seus capítulos para demonstrar como os controles apresentados nas normas são levados da teoria à prática em um ambiente operacional.

US National Cyber Security Strategy and Programs Handbook Volume 1 Strategic Information and Developments

Enterprise Cybersecurity empowers organizations of all sizes to defend themselves with next-generation cybersecurity programs against the escalating threat of modern targeted cyberattacks. This book presents a comprehensive framework for managing all aspects of an enterprise cybersecurity program. It enables an enterprise to architect, design, implement, and operate a coherent cybersecurity program that is seamlessly coordinated with policy, programmatics, IT life cycle, and assessment. Fail-safe cyberdefense is a pipe dream. Given sufficient time, an intelligent attacker can eventually defeat defensive measures protecting an enterprise’s computer systems and IT networks. To prevail, an enterprise cybersecurity program must manage risk by detecting attacks early enough and delaying them long enough that the defenders have time to respond effectively. Enterprise Cybersecurity shows players at all levels of responsibility how to unify their organization’s people, budgets, technologies, and processes into a cost-efficient cybersecurity program capable of countering advanced cyberattacks and containing damage in the event of a breach. The authors of Enterprise Cybersecurity explain at both strategic and tactical levels how to accomplish the mission of leading, designing, deploying, operating, managing, and supporting cybersecurity capabilities in an enterprise environment. The authors are recognized experts and thought leaders in this rapidly evolving field, drawing on decades of collective experience in cybersecurity and IT. In capacities ranging from executive strategist to systems architect to cybercombatant, Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, and Abdul Aslam have fought on the front lines of cybersecurity against advanced persistent threats to government, military, and business entities.

Foundations of Information Security Based on ISO27001 and ISO27002

Step-by-step guidance on a successful ISO 27001 implementation from an industry leader Resilience to cyber attacks requires an organization to defend itself across all of its attack surface: people, processes, and technology. ISO 27001 is the international standard that sets out the requirements of an information security management system (ISMS) – a holistic approach to information security that encompasses people, processes, and technology. Accredited certification to the Standard is recognized worldwide as the hallmark of best-practice information security management. Achieving and maintaining accredited certification to ISO 27001 can be complicated, especially for those who are new to the Standard. Author of Nine Steps to Success – An ISO 27001 Implementation Overview, Alan Calder is the founder and executive chairman of IT Governance. He led the world’s first implementation of a management system certified to BS 7799, the forerunner to ISO 27001, and has been working with the Standard ever since. Hundreds of organizations around the world have achieved accredited certification to ISO 27001 with IT Governance's guidance, which is distilled in this book.

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

This book constitutes the refereed proceedings of the 8th IFIP WG 11.8 World Conference on Security Education, WISE 8, held in Auckland, New Zealand, in July 2013. It also includes papers from WISE 6, held in Bento Gonçalves, Brazil, in July 2009 and WISE 7, held in Lucerne, Switzerland in June 2011. The 34 revised papers presented were carefully reviewed and selected for inclusion in this volume. They represent a cross section of applicable research as well as case studies in security education.

Computer Security

US National Cyber Security Strategy and Programs Handbook - Strategic Information and Developments

Basiskennis informatiebeveiliging op basis van ISO27001 en ISO27002 - 2de herziene druk

Written in clear English this book explores why so many organizations have already successfully registered to BS7799/ISO27001 and makes a crystal clear case for pursuing the standard that management in any organization anywhere in the world will accept.

Implementing an Information Security Management System

Information Security Fundamentals, Second Edition

Information is the currency of the information age and in many cases is the most valuable asset possessed by an organisation. Information security management is the discipline that focuses on protecting and securing these assets against the threats of natural disasters, fraud and other criminal activity, user error and system failure. This Management Guide provides an overview of the two international information security standards, ISO/IEC 27001 and ISO 27002. These standards provide a basis for implementing information security controls to meet an organisation's own business requirements as well as a set of controls for business relationships with other parties. This Guide provides: An introduction and overview to both the standards The background to the current version of the standards Links to other standards, such as ISO 9001, BS25999 and ISO 20000 Links to frameworks such as CobiT and ITIL Above all, this handy book describes how

ISO 27001 and ISO 27002 interact to guide organizations in the development of best practice information security management systems.

Microsoft Forefront Identity Manager 2010 R2 Handbook

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.