Iso27001 Iso27002 Guida Tascabile

Questa indispensabile guida tascabile fornisce un'utile panoramica di due importanti norme sulla sicurezza delle informazioni Cosi ricco di consigli pratici per l'attuazione di un sistema di gestione della sicurezza delle informazioni che vi chiederete come avete potuto farne a meno prima d'ora. Acquista la tua copia oggi stesso.

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.

Thrive under the GDPR (General Data Protection Regulation) wherever you are in the world. This pocket guide will help you understand the Regulation, the broader principles of data protection, and what the GDPR means for businesses in Europe and beyond.

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.

Proteja la información de su organización con la ISO27001:2013 La información es uno de los recursos más importantes de su organización y mantener esa información segura es vital para su negocio. Esta guía de bolsillo útil es una visión de conjunto esencial sobre las dos normas de la seguridad de la información clave que cubren los requisitos formales (ISO27001:2013) para crear un Sistema de Gestión de la Seguridad de la Información (SGSI) y las recomendaciones de mejores prácticas (ISO27002:2013) para aquellos responsables de iniciar, implementar o mantenerlo. Un SGSI basado en la ISO27001/ISO27002 ofrece un sinfín de beneficios: Eficacia mejorada implantando procedimientos y sistemas de seguridad de la información, que le permiten concentrarse en su actividad empresarial principal.Protege sus activos de información de un amplio abanico de ciberamenazas, actividad criminal, compromiso de información privilegiada y fallo del sistema.Gestione sus riesgos sistemáticamente y establezca planes para eliminar o reducir las ciberamenazas.Permite la detección temprana de amenazas o errores de procesamiento y una solicuón más rápida¿Siguiente paso para la certificación? Puede organizar una auditoría independiente de su SGSI frente a las especificaciones de la ISO27001 y, si su SGSI se ajusta, finalmente logra la certificación acreditada. Publicamos una variedad de libros y herramientas de documentación del SGSI (como Nueve pasos para el éxito) para ayudarle a lograr esto. ÍndiceLa familia de normas de la seguridad de la información ISO-/IEC 27000;Historia de las Normas;Especificación frente al Código de Prácticas;Proceso de certificación;El SGSI y la ISO27001;Visión de conjunto de la ISO/IEC 27001:2013;Visión de conjunto de la ISO/IEC 27002:2013;Documentación y registros;Responsabilidad de la gestión;Enfoque del proceso y el ciclo PDCA;Contexto, política y alcance;Evaluación del riesgo;La declaración de aplicabilidad (SoA);Implementación; 15. Verificar y actuar;Revisión gerencial;ISO27001; Anexo A

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.

30 achievable ways in which Agile business analysts can increase the relevance, quality, and overall business value of your Agile projects.

Information technology plays a fundamental role in the operations of any modern business. While the confidentiality and integrity of your organisation's information have to be protected, a business still needs to have this information readily available in order to be able to function from day to day. If you are an information security practitioner, you need to be able to sell complex and often technical solutions to boards and management teams. Persuading the board to invest in information security measures requires sales skills. As an information security professional, you are a scientific and technical specialist; and yet you need to get your message across to people whose primary interests lie elsewhere, in turnover and overall performance. In other words, you need to develop sales and marketing skills. This pocket guide will help you with the essential sales skills that persuade company directors to commit money and resources to your information security initiatives.

Now in its fourth edition, this bestselling guide is the ideal companion for anyone carrying out a GDPR (General Data Protection Regulation) compliance project. It provides comprehensive guidance and practical advice on complying with the Regulation.

This pocket guide is a primer for any OES (operators of essential services) that needs to comply with the NIS Regulations, and explores who they are, and why the NIS Regulations are different for them. An introduction to the new NIS Regulations 2018 that bring the EU's NIS Directive and Implementing Regulation into UK law. This guide outlines the requirements for operators of essential services based on the Cyber Assessment Framework established by the National Cyber Security Centre (NCSC), including an explanation of the objectives, principles and indicators of good practice, and offers implementation guidance. This guide will help you: Understand how to comply with NIS Regulations, and avoid penalties associated with non-compliance Unravel the key definitions, authorities and points of contact Learn the benefits of a good Cyber Resilience plan Interpret and ensure compliance with the Cyber Assessment Framework Establish the NCSC's cyber security objectives, principles and indicators of good practice Your essential guide to understanding the NIS Regulations - buy this book today and get the help and guidance you need.

Cyber Security – Essential principles to secure your organisation takes you through the fundamentals of cyber security, the principles that underpin it, vulnerabilities and threats, and how to defend against attacks.

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

The emergence of ISO/IEC 38500 OCo the international standard for the corporate governance of information and communication technology OCo puts boards around the world in a position from which they can take effective action to apply core governance principles to their information and communication technology."

This new book sets out for managers, executives and IT professionals the practical steps necessary to meet today's corporate and IT governance requirements. It provides practical guidance on how board executives and IT professionals can navigate, integrate and deploy to best corporate and commercial advantage the most widely used frameworks and standards.

A clear, concise primer on the EU GDPR The EU General Data Protection Regulation (GDPR) is a key piece of legislation that provides a single, harmonised privacy law for the European Union, improving the promotion and regulation of data privacy. With the Regulation now formally approved by the European Parliament, all companies that operate in Europe have until 26 April 2018 to comply with the new law, or potentially face fines of up to 4% of annual turnover or 20 million. This pocket guide is the perfect introduction for organisations that need to get to grips with the key principles of data privacy and the EU General Data Protection Regulation.

This newdownloadable pocket guidein the Practical IT Governance series, is designed to provide the reader with a basic understanding of how an organization's Information Technology supports and enables the achievement of its strategies and objectives.

This pocket guide is an introduction to the EU's NIS Directive (Directive on security of network and information systems). It outlines the key requirements, details which digital service providers are within scope, and explains how the security objectives from ENISA's Technical Guidelines and international standards can help DSPs achieve compliance. This pocket guide is a primer for any DSP that needs to comply with the NIS Directive. The pocket guide helps DSPs: Gain insight into the NIS Directive and who is regulating it; Identify if they are within the scope of the Directive; Understand the key requirements; and Understand how guidance from international standards and ENISA can help them comply. Your essential guide to understanding the EU's NIS Directive - buy this book today and get the help and guidance you need.

This important new book - 'IT Governance: Guidelines for Directors' provides directors, executives, managers and professional advisers with clear,pragmatic guidelines for ensuring that IT and the business work together for thesamestrategic objectives.

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.

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

This book is apocket guide to the ISO27001 risk assessment, and designed to assist asset owners and others who are working within an ISO27001/ISO17799 framework to deliver a qualitative risk assessment. It conforms with the guidance provided in BS7799-3:2006 and NIST SP 800-30.

This book was written with two objectives. First, as a guide to a number of the detailed areas that are important for practitioners to think through when creating an IT governance framework, and second, to provide a detailed companion to "IT Governance: Guidelines for Directors."

ISO27001/ISO27002: Guida tascabileIT Governance Ltd

Aligned with the latest iteration of the Standard – ISO 27001:2013 – this new edition of the original no-nonsense guide to successful ISO

27001 certification is ideal for anyone tackling ISO 27001 for the first time, and covers each element of the ISO 27001 project in simple, non-technical language

This pocket guide serves as an introduction to the National Institute of Standards and Technology (NIST) and to its Cybersecurity Framework (CSF). This is a US focused product. Now more than ever, organizations need to have a strong and flexible cybersecurity strategy in place in order to both protect themselves and be able to continue business in the event of a successful attack. The NIST CSF is a framework for organizations to manage and mitigate cybersecurity risk based on existing standards, guidelines, and practices. With this pocket guide you can: Adapt the CSF for organizations of any size to implementEstablish an entirely new cybersecurity program, improve an existing one, or simply provide an opportunity to review your cybersecurity practicesBreak down the CSF and understand how other frameworks, such as ISO 27001 and ISO 22301, can integrate into your cybersecurity framework By implementing the CSF in accordance with their needs, organizations can manage cybersecurity risks in the most cost-effective way possible, maximizing the return on investment in the organization’s security. This pocket guide also aims to help you take a structured, sensible, risk-based approach to cybersecurity.

A Guide to Effective Internal Management System Audits provides a model for the management and implementation of internal audits that moves beyond simple compliance to ISO requirements and turns the internal audit into a transformational tool that the organization can use to assist with the management of risk, and implement improvements to management systems.

This book helps you to bring the information security of your organization to the right level by using the ISO/IEC 27001 standard. An organization often provides services or products for years before the decision is taken to obtain an ISO/IEC 27001 certificate. Usually, a lot has already been done in the field of information security, but after reading the requirements of the standard, it seems that something more needs to be done: an 'information security management system' must be set up. A what? This handbook is intended to help small and medium-sized businesses establish, implement, maintain and continually improve an information security management system in accordance with the requirements of the international standard ISO/IEC 27001. At the same time, this handbook is also intended to provide information to auditors who must investigate whether an information security management system meets all requirements and has been effectively implemented. This handbook assumes that you ultimately want your information security management system to be certified by an accredited certification body. The moment you invite a certification body to perform a certification audit, you must be ready to demonstrate that your management system meets all the requirements of the Standard. In this book, you will find detailed explanations, more than a hundred examples, and sixty-one common pitfalls. It also contains information about the rules of the game and the course of a certification audit. Cees van der Wens (1965) studied industrial automation in the Netherlands. In his role as Lead Auditor, the author has carried out dozens of ISO/IEC 27001 certification audits at a wide range of organizations. As a consultant, he has also helped many organizations obtain the ISO/IEC 27001 certificate. The author feels very connected to the standard because of the social importance of information security and the power of a management system to get better results.

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.

This book provides an accessible overview of the changes you need to make in your organization to comply with the new law. --

Presents the compelling business case for implementing ISO27001:2013 to protect your information assets. Perfect for supporting an ISO27001 project proposal.

In this book, users will get to know about the ISO 27001 and how to implement the required policies and procedures to acquire this certification. Real policies and procedures have been used as examples with step by step explanations about the process which includes implementing group polices in windows server. And lastly, the book also includes details about how to conduct an Internal Audit and proceed to the Final Audit

Understand the basics of business continuity and ISO 22301:2019 with this concise pocket guide, which will help you ensure your organisation can continue to operate in the event of a disruption.

The most complete, up to date guide to risk management in finance Risk Management and Financial Institutions explains all aspects of financial risk and financial institution regulation, helping readers better understand the financial markets and potential dangers. This new fourth edition has been updated to reflect the major developments in the industry, including the finalization of Basel III, the fundamental review of the trading book, SEFs, CCPs, and the new rules affecting derivatives markets. There are new chapters on enterprise risk management and scenario analysis. Readers learn the different types of risk, how and where they appear in different types of institutions, and how the regulatory structure of each institution affects risk management practices. Comprehensive ancillary materials include software, practice questions, and all necessary teaching supplements, facilitating more complete understanding and providing an ultimate learning resource. All financial professionals need a thorough background in risk and the interlacing connections between financial institutions to better understand the market, defend against systemic dangers, and perform their jobs. This book provides a complete picture of the risk management industry and practice, with the most up to date information. Understand how risk affects different types of financial institutions Learn the different types of risk and how they are managed Study the most current regulatory issues that deal with risk Risk management is paramount with the dangers inherent in the financial system, and a deep understanding is essential for anyone working in the finance industry; today, risk management is part of everyone's job. For complete information and comprehensive coverage of the latest industry issues and practices, Risk Management and Financial Institutions is an informative, authoritative guide.

Work-life balance is one of the most important issues facing employers and managers today. Employees at all levels are no longer willing to trade their quality of life in order to get a decent standard of living. Managers can no longer afford to ignore the costs that the long-hours culture imposes on their organisation. Overwork causes stress-related absenteeism, poor retention levels, low creativity, appalling customer service and unethical employee behaviour. Combine that with the risks of being sued by a stressed employee or a parent who wanted to work

flexibly, and the business case for paying real attention to work-life issues has never been stronger. This text sets out the roadmap for moving your organisation towards a positive work-life culture. With clear and practical advice for HR and line managers alike, Managing Work-Life Balance shows you how to engage employers, managers and employees in the process of controlling the inherent conflicts between the worlds of work and home.

This pocket guide is a primer for any DSPs (digital service providers) that needs to comply with the NIS Regulations, and explores who they are, and why the NIS Regulations are different for them.

"Cyber Essentials certification will provide numerous benefits, including the opportunity to tender for business where certification to the scheme may be a prerequisite, reducing insurance premiums, and helping to improve investor and customer confidence. This pocket guide explains how to achieve certification to Cyber Essentials in a fast, effective and cost-effective manner."--

In this book, the following subjects are included: information security, the risk assessment and treatment processes (with practical examples), the information security controls. The text is based on the ISO/IEC 27001 standard and on the discussions held during the editing meetings, attended by the author. Appendixes include short presentations and check lists. CESARE GALLOTTI has been working since 1999 in the information security and IT process management fields and has been leading many projects for companies of various sizes and market sectors. He has been leading projects as consultant or auditor for the compliance with standards and regulations and has been designing and delivering ISO/IEC 27001, privacy and ITIL training courses. Some of his certifications are: Lead Auditor ISO/IEC 27001, Lead Auditor 9001, CISA, ITIL Expert and CBCI, CIPP/e. Since 2010, he has been Italian delegate for the the editing group for the ISO/IEC 27000 standard family. Web: www.cesaregallotti.it.

Information is widely regarded as the lifeblood of modern business, but organizations are facing a flood of threats to such “intellectual capital” from hackers, viruses, and online fraud. Directors must respond to increasingly complex and competing demands regarding data protection, privacy regulations, computer misuse, and investigatory regulations. IT Governance will be valuable to board members, executives, owners and managers of any business or organization that depends on information. Covering the Sarbanes-Oxley Act (in the US) and the Turnbull Report and the Combined Code (in the UK), the book examines standards of best practice for compliance and data security. Written for companies looking to protect and enhance their information security management systems, it allows them to ensure that their IT security strategies are coordinated, coherent, comprehensive and cost effective.

Essential summary of the PCI DSS v3.0, ideal for quick reference or staff awareness.

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.