ISO27001/ISO27002 A Pocket Guide Second Edition: 2013

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

The issues, opportunities and challenges of aligning information technology more closely with an organization and effectively governing an organization's Information Technology (IT) investments, resources, major initiatives and superior uninterrupted service is becoming a major concern of the Board and executive management in enterprises on a global basis. An integrated and comprehensive approach to the alignment, planning, execution and governance of IT and its resources has become critical to more effectively align, integrate, invest, measure, deploy, service and sustain the strategic and tactical direction and value proposition of IT in support of organizations. Much has been written and documented about the individual components of IT Governance such as strategic planning, demand (portfolio investment) management, program and project management, IT service management and delivery, strategic sourcing and outsourcing, performance management and metrics, like the balanced scorecard, compliance and others. Much less has been written about a comprehensive and integrated IT/Business Alignment, Planning, Execution and Governance approach. This new title fills that need in the marketplace and gives readers a structured and practical solutions using the best of the best principles available today. The book is divided into nine chapters, which cover the three critical pillars necessary to develop, execute and sustain a robust and effective IT governance environment - leadership and proactive people and change agents, flexible and scalable processes and enabling technology. Each of the chapters also covers one or more of the following action oriented topics: demand management and alignment (the why and what of IT – strategic planning, portfolio investment management, decision authority, etc.); execution management (includes the how - Program/Project Management, IT Service Management with IT Infrastructure Library (ITIL) and Strategic Sourcing and outsourcing); performance, risk and contingency management (e.g. includes COBIT, the balanced scorecard and other metrics and controls); and leadership, teams and people skills.

Information risk management (IRM) is about identifying, assessing and prioritising risks to keep information secure and available. This accessible book is a practical guide to understanding the principles of IRM and developing a strategic approach to an IRM programme. It also includes a chapter on applying IRM in the public sector. It is the only textbook for the BCS Practitioner Certificate in Information Risk Management.

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.

IT Governance

An Example of Applied Compliance Management

The Cyber Security Handbook – Prepare for, respond to and recover from cyber attacks

ISO27001 / ISO27002

EU GDPR

Building an Information Security Risk Management Program from the Ground Up

This helpful, handy ISO27001/ISO27002 pocket guide gives a useful overview of these two important information security standards.

You may regard cloud computing as an ideal way for your company to control IT costs, but do you know how private and secure this service really is? Not many people do. With Cloud Security and Privacy, you'll

learn what's at stake when you trust your data to the cloud, and what you can do to keep your virtual infrastructure and web applications secure. Ideal for IT staffers, information security and privacy practitioners, business managers, service providers, and investors alike, this book offers you sound advice from three well-known authorities in the tech security world. You'll learn detailed information on cloud computing security that-until now-has been sorely lacking. Review the current state of data security and storage in the cloud, including confidentiality, integrity, and availability Learn about the identity and access management (IAM) practice for authentication, authorization, and auditing of the users accessing cloud services Discover which security management frameworks and standards are relevant for the cloud Understand the privacy aspects you need to consider in the cloud, including how they compare with traditional computing models Learn the importance of audit and compliance functions within the cloud, and the various standards and frameworks to consider Examine security delivered as a service-a different facet of cloud security

In todayOCOs technology-driven environment, there is an ever-increasing demand for information delivery. A compromise has to be struck between security and availability. This book is a pragmatic guide to information assurance for both business professionals and technical experts. This second edition includes the security of cloud-based resources."

Implement an effective and compliant information security management system using IT governance best practice

Cloud Security and Privacy

GDPR - Fix it Fast

A Guide to Understanding, Detecting, and Defending Against the Enemy from Within

A Pocket Guide, Second Edition

ISO 27001 controls – A guide to implementing and auditing

Implementing IT Governance - A Practical Guide to Global Best Practices in IT Management

EU GDPR – A Pocket Guide, second edition provides an accessible overview of the changes you need to make in your organisation to comply with the new law. The EU General Data Protection Regulation unifies data protection across the EU. It applies to every organisation in the world that does business with EU residents. The Regulation introduces a number of key changes for organisations – and the change from DPA compliance to GDPR compliance is a complex one. New for the second edition: Updated to take into account the latest guidance from WP29 and ICO.Improved guidance around related laws such as the NIS Directive and the future ePrivacy Regulation. This pocket guide also sets out: A brief history of data protection and national

data protection laws in the EU (such as the UK DPA, German BDSG and French LIL).The terms and definitions used in the GDPR, including explanations.The key requirements of the GDPRHow to comply with the RegulationA full index of the Regulation, enabling you to find relevant Articles quickly and easily. This guide is the ideal resource for anyone wanting a clear, concise primer on the EU GDPR.

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.

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. For trainers free additional material of this book is available. This can be found under the "Training Material" tab. Log in with your trainer account to access the material.The increasing complexity of the IT value chain and the rise of multi-vendor supplier ecosystems has led to the rise of Service Integration and Management (SIAM) as a new approach. Service Integration is the set of principles and practices, which facilitate the collaborative working relationships between service providers required to maximize the benefit of multi-sourcing. Service integration facilitates the linkage of services, the technology of which they are comprised and the delivery organizations and processes used to operate them, into a single operating model.SIAM is a relatively new and fast evolving concept. SIAM teams are being established in many organizations and in many different sectors, as part of a strategy for (out)sourcing IT services and other types of service.This is the first book that describes the concepts of SIAM. It is intended for: ITSM professionals working in integrated multi-sourced environments; Service customer managers, with a responsibility to secure the business supply of IT services in a multi-sourced environment; Service provider delivery managers with a responsibility to integrate multiple services to meet the demands of the customers business and users; Service provider managers with responsibilities to manage integrated services, participating in a multi-sourced environment.

An International Guide to Data Security and ISO27001/ISO27002

Implementing the ISO/IEC 27001:2013 ISMS Standard

An Introduction to Information Security and ISO27001:2013

Insider Threat

How to Measure Anything in Cybersecurity Risk

An Enterprise Perspective on Risks and Compliance

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

This pocket guide summarises the key principles and standards of ISO/IEC 20000 on best practice in IT service management (which was derived from the British Standard BS 15000). It is aimed at a broad range of practitioners, trainers and students who work in the IT sector as well as in other environments. Sections cover: background information to the standard; core and supporting material; overall management issues including planning and implementation; the self-assessment workbook; and information on service delivery, relationship, resolution, control and release processes.

Quickly understand the principles of information security.
Iso27001/Iso27002 a Pocket GuideIt Governance Limited
Iso27001/Iso27002 a Pocket Guide
Do-it-yourself and Get-certified
An ISO27001:2013 Implementation Overview, Third edition
Information Security Management Based on Iso 27001 2013
Information Security Risk Management for ISO 27001/ISO 27002, third edition

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.

This book is a comprehensive cyber security implementation manual which gives practical guidance on the individual activities identified in the IT Governance Cyber Resilience Framework (CRF) that can help organisations become cyber resilient and combat the cyber threat landscape. Start your cyber security journey and buy this book today!

GDPR - Fix it Fast! Apply GDPR to Your Company in 10 Simple Steps is a plain-language guide to implementing the European General Data Protection Regulation's requirements to your organization. This isn't a legal book, it's a road map to compliance. Fix it Fast will help you to implement the key requirements of GDPR. It contains templates, outlines, examples and plain-English explanations to help you: Complete your data inventory Start and finish your data map Draft and institute a Privacy Impact Assessment process Plan how you'll deal with a Data Breach Implement Data Privacy Policies and Privacy Notifications And much more This book's 10 Simple Steps will take you from beginning to end of your GDPR readiness and implementation project. This isn't a legal book - it's a practical, no-nonsense guide to getting the job done fast. This book helps is built for compliance officers, lawyers, information technology and information security professionals, and anyone else tasked with GDPR compliance to complete the critical tasks.

Management systems and procedural controls are essential components of any really secure information system and, to be effective, need careful planning and attention to detail. This book provides the specification for an information security management system.

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

Information Security Management Principles

Security Risk Management

It Governance

ISO27001

A Manager's Guide to Data Security and ISO 27001/ISO 27002

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 an 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.

Information is widely regarded as the lifeblood of modern business, but organizations are facing a flood of threats to such “intellectual capita 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 managers of any business or organization that depends on information. Covering the Sarbanes-Oxley Act (in the US) and the Turnbull Rep 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.

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

A ground shaking exposé on the failure of popular cyber risk management methods How to Measure Anything in Cybersecurity Risk expos the shortcomings of current "risk management" practices, and offers a series of improvement techniques that help you fill the holes and ram up security. In his bestselling book How to Measure Anything, author Douglas W. Hubbard opened the business world's eyes to the critical need for better measurement. This book expands upon that premise and draws from The Failure of Risk Management to sound the alarm i cybersecurity realm. Some of the field's premier risk management approaches actually create more risk than they mitigate, and questionab methods have been duplicated across industries and embedded in the products accepted as gospel. This book sheds light on these blatant and provides alternate techniques that can help improve your current situation. You'll also learn which approaches are too risky to save, an are actually more damaging than a total lack of any security. Dangerous risk management methods abound; there is no industry more critic in need of solutions than cybersecurity. This book provides solutions where they exist, and advises when to change tracks entirely. Discove shortcomings of cybersecurity's "best practices" Learn which risk management approaches actually create risk Improve your current practic with practical alterations Learn which methods are beyond saving, and worse than doing nothing Insightful and enlightening, this book will inspire a closer examination of your company's own risk management practices in the context of cybersecurity. The end goal is airtight data protection, so finding cracks in the vault is a positive thing—as long as you get there before the bad guys do. How to Measure Anything in Cybersecurity Risk is your guide to more robust protection through better quantitative processes, approaches, and techniques.

Implementing and Auditing an Information Security Management System in Small and Medium-Sized Businesses

ISO27001/ISO27002 A Pocket Guide, 2nd edition

Information security: risk assessment, management systems, the ISO/IEC 27001 standard

Information Security Risk Management for ISO27001/ISO27002

ISO/IEC 20000

Implementing Information Security based on ISO 27001/ISO 27002

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. 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.

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 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.

Nine Steps to Success

Information Security Policy Development for Compliance

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

Apply GDPR to Your Company in 10 Simple Steps

How to Achieve 27001 Certification

SIAM: Principles and Practices for Service Integration and Management

Providing a comprehensive framework for a sustainable governance model, and how to leverage it in competing global markets, Governance, Risk, and Compliance Handbook presents a readable overview to the political, regulatory, technical, process, and people considerations in complying with an ever more demanding regulatory environment and achievement of good corporate governance. Offering an international overview, this book features contributions from sixty-four industry experts from fifteen countries.

Every type of organization is vulnerable to insider abuse, errors, and malicious attacks: Grant anyone access to a system and you automatically introduce a vulnerability. Insiders can be current or former employees, contractors, or other business partners who have been granted authorized access to networks, systems, or data, and all of them can bypass security measures through legitimate means. Insider Threat – A Guide to Understanding, Detecting, and Defending Against the Enemy from Within shows how a security culture based on international best practice can help mitigate the insider threat, providing short-term quick fixes and long-term solutions that can be applied as part of an effective insider threat program. Read this book to learn the seven organizational characteristics common to insider threat victims; the ten stages of a malicious attack; the ten steps of a successful insider threat program; and the construction of a three-tier security culture, encompassing artefacts, values, and shared assumptions. Perhaps most importantly, it also sets out what not to do, listing a set of worst practices that should be avoided. About the author Dr Julie Mehan is the founder and president of JEMStone Strategies and a principal in a strategic consulting firm in Virginia. She has delivered cybersecurity and related privacy services to senior commercial, Department of Defense, and federal government clients. Dr Mehan is also an associate professor at the University of Maryland University College, specializing in courses in cybersecurity, cyberterror, IT in organizations, and ethics in an Internet society Security Risk Management is the definitive guide for building or running an information security risk management program. This book teaches practical techniques that will be used on a daily basis, while also explaining the fundamentals so students understand the rationale behind these practices. It explains how to perform risk assessments for new IT projects, how to efficiently manage daily risk activities, and how to qualify the current risk level for presentation to executive level management. While other books focus entirely on risk analysis methods, this is the first comprehensive text for managing security risks. This book will help you to break free from the so-called best practices argument by articulating risk exposures in business terms. It includes case studies to provide hands-on experience using risk assessment tools to calculate the costs and benefits of any security investment. It explores each phase of the risk management lifecycle, focusing on policies and assessment processes that should be used to properly assess and mitigate risk. It also presents a roadmap for designing and implementing a security risk management program. This book will be a valuable resource for CISOs, security managers, IT managers, security consultants, IT auditors, security analysts, and students enrolled in information security/assurance college programs. Named a 2011 Best Governance and ISMS Book by InfoSec Reviews Includes case studies to provide hands-on experience using risk assessment tools to calculate the costs and benefits of any security investment Explores each phase of the risk management lifecycle, focusing on policies and assessment processes that should be used to

properly assess and mitigate risk Presents a roadmap for designing and implementing a security risk management program

Business organizations, both public and private, are constantly challenged to innovate and generate real value. CIOs are uniquely well-positioned to seize this opportunity and adopt the role of business transformation partner, helping their organizations to grow and prosper with innovative, IT-enabled products, services and processes. To succeed in this, however, the IT function needs to manage an array of inter-related and inter-dependent disciplines focused on the generation of business value. In response to this need, the Innovation Value Institute, a cross-industry international consortium, developed the IT Capability Maturity Framework™ (IT-CMF™). This second edition of the IT Capability Maturity Framework™ (IT-CMF™) is a comprehensive suite of tried and tested practices, organizational assessment approaches, and improvement roadmaps covering key IT capabilities needed to optimize value and innovation in the IT function and the wider organization. It enables organizations to devise more robust strategies, make better-informed decisions, and perform more effectively, efficiently and consistently. IT-CMF is: An integrated management toolkit covering 36 key capability management disciplines, with organizational maturity profiles, assessment methods, and improvement roadmaps for each. A coherent set of concepts and principles, expressed in business language, that can be used to guide discussions on setting goals and evaluating performance. A unifying (or umbrella) framework that complements other, domain-specific frameworks already in use in the organization, helping to resolve conflicts between them, and filling gaps in their coverage. Industry/sector and vendor independent. IT-CMF can be used in any organizational context to guide performance improvement. A rigorously developed approach, underpinned by the principles of Open Innovation and guided by the Design Science Research methodology, synthesizing leading academic research with industry practitioner expertise

ISO 27001 Handbook

Information Security based on ISO 27001/ISO 27002

IT Capability Maturity Framework™ (IT-CMF™) 2nd edition

EU GDPR A Pocket Guide second edition

A Pocket Guide

A Practitioner's Guide

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

The security criteria of the International Standards Organization (ISO) provides an excellent foundation for identifying and addressing business risks through a disciplined security management process. Using security standards ISO 17799 and ISO 27001 as a basis, How to Achieve 27001 Certification: An Example of Applied Compliance Management helps an organization align its security and organizational goals so it can generate effective security, compliance, and management programs. The authors offer insight from their own experiences, providing questions and answers to determine an organization's information security strengths and weaknesses with respect to the standard. They also present step-by-step information to help an organization plan an implementation, as well as prepare for certification and audit. Security is no longer a luxury for an organization, it is a legislative mandate. A formal methodology that helps an organization define and execute an ISMS is essential in order to perform and prove due diligence in upholding stakeholder interests and legislative compliance. Providing a good starting point for novices, as well as finely tuned nuances for seasoned security professionals, this book is an invaluable resource for anyone involved with meeting an organization's security, certification, and compliance needs.

Although compliance standards can be helpful guides to writing comprehensive security policies, many of the standards state the same requirements in slightly different ways. Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0 provides a simplified way to write policies th

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.

ISO 21500 Guidance on project management - A Pocket Guide

Governance, Risk, and Compliance Handbook

Information Risk Management

Technology, Finance, Environmental, and International Guidance and Best Practices

ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0

NIST Cybersecurity Framework: A pocket guide

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.
We constructing "Do-It-Yourself and Get Certified: Information Security Management Based on ISO 27001:2013" book to provide direction and illustration for organizations who need a workable framework and person who is interested to learn on how to implement information security management effectively in accordance with ISO/IEC 27001:2013 standard. This book is organized to provide step-by-step, comprehensive guidance and many examples for an organization who wants to adopt and implement the information security and wish to obtain certification of ISO/IEC 27001:2013. By providing all materials required in this book, we expect that you can DO IT YOURSELF the implementation of ISO/IEC 27001:2013 standard and GET CERTIFIED. Information security management implementation presented in this book is using Plan-Do-Check-Act (PDCA) cycle, which is a standard continuous improvement process model used by ISO.
This pocket guide explains the content and the practical use of ISO 21500 - Guidance on project management, the latest international standard for project management, and the first of a family of ISO standards for project, portfolio and program management. ISO 21500 is meant for senior managers and project sponsors to better understand project management and to properly support projects, for project managers and their team members to have a reference for comparing their projects to others and it can be used as a basis for the development of national standards.This pocket guide provides a quick introduction as well as a structured overview of this guidance and deals with the key issues within project management: Roles and responsibilities Balancing the project constraints Competencies of project personnelAll ISO 21500 subject groups (themes) are explained: Integration, Stakeholder, Scope, Resource, Time, Cost, Risk, Quality, Procurement and Communication.A separate chapter explains the comparison between, ISO 21500 and PMBOK® Guide PRINCE2, Agile, Lean, Six Sigma and other methods, practices and models.Finally, it provides a high level description of how ISO 21500 can be applied in practice using a generic project life cycle.Proper application of this new globally accepted project management guideline will support organizations and individuals in growing their project management maturity consistently to a professional level.