

Iso 27004

Information Security Management, Measurement (ISO/IEC 27004:2009)
 PN-ISO/IEC 27004
 An International Guide to Data Security and ISO27001/ISO27002
 IT Governance based on CobiT® 4.1 - A Management Guide
 Network Security and Cyber Defence (CNSS)
 It Governance
 First International Conference, CIIT 2011, Pune, India, November 7-8, 2011. Proceedings
 Encyclopedia of Organizational Knowledge, Administration, and Technology
 Cyberterrorism, Information Warfare, and Internet Immobilization
 Web Commerce Security
 Engineering-Based Establishment of Security Standards
 Encyclopedia of Information Assurance - 4 Volume Set (Print)
 Building a Practical Information Security Program
 Advances in Communications, Computing, Networks and Security Volume 10
 Banking, Finance, and Accounting: Concepts, Methodologies, Tools, and Applications
 4th International Conference, ICGeS 2008, London, UK, June 23-25, 2008, Proceedings
 10th International Conference, TrustBus 2013, Prague, Czech Republic, August 28-29, 2013. Proceedings
 Computer Networks and Information Technologies
 The CSSLP Prep Guide
 Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization
 Design and Development
 Information Security Governance
 Trust, Privacy, and Security in Digital Business
 Developing Cybersecurity Programs and Policies
 Second International Conference on Advances in Communication, Network, and Computing, CNC 2011, Bangalore, India, March 10-11, 2011. Proceedings
 Confederated International Conferences: CoopIS, C&TC, and ODBASE 2017, Rhodes, Greece, October 23-27, 2017, Proceedings, Part I
 Information Technology - Security Techniques - Information Security Management - Measurement
 Information Security based on ISO 27001/ISO 27002
 A Systems Approach
 International Standard ISO/IEC 27004
 On the Move to Meaningful Internet Systems. OTM 2017 Conferences
 Pattern and Security Requirements
 Creating an Information Security Program from Scratch
 Software Quality Assurance
 Information technology - security techniques - information security management - measurement
 Principles and Practices
 ISO/IEC 27004
 Information Technology, Security Techniques

Iso 27004

Downloaded from ecobankpayservices.ecobank.com by guest

RODRIGO RODGERS

Information Security Management, Measurement (ISO/IEC 27004:2009) CRC Press

IT Governance: Policies and Procedures, 2022 Edition

PN-ISO/IEC 27004 Pearson Education

IT governance seems to be one of the best strategies to optimize IT assets in an economic context dominated by information, innovation, and the race for performance. The multiplication of internal and external data and increased digital management, collaboration, and sharing platforms exposes organizations to ever-growing risks. Understanding the threats, assessing the risks, adapting the organization, selecting and implementing the appropriate controls, and implementing a management system are the activities required to establish proactive security governance that will provide management and customers the assurance of an effective mechanism to manage risks. IT Governance and Information Security: Guides, Standards, and Frameworks is a fundamental resource to discover IT governance and information security. This book focuses on the guides, standards, and maturity frameworks for adopting an efficient IT governance and information

security strategy in the organization. It describes numerous case studies from an international perspective and brings together industry standards and research from scientific databases. In this way, this book clearly illustrates the issues, problems, and trends related to the topic while promoting the international perspectives of readers. This book offers comprehensive coverage of the essential topics, including: IT governance guides and practices; IT service management as a key pillar for IT governance; Cloud computing as a key pillar for Agile IT governance; Information security governance and maturity frameworks. In this new book, the authors share their experience to help you navigate today's dangerous information security terrain and take proactive steps to measure your company's IT governance and information security maturity and prepare your organization to survive, thrive, and keep your data safe. It aspires to provide a relevant reference for executive managers, CISOs, cybersecurity professionals, engineers, and researchers interested in exploring and implementing efficient IT governance and information security strategies.

An International Guide to Data Security and ISO27001/ISO27002 Syngress

Performance Management for the Oil, Gas, and Process Industries: A Systems Approach is a practical guide on the business cycle and techniques to undertake step, episodic, and

breakthrough improvement in performance to optimize operating costs. Like many industries, the oil, gas, and process industries are coming under increasing pressure to cut costs due to ongoing construction of larger, more integrated units, as well as the application of increasingly stringent environmental policies. Focusing on the 'value adder' or 'revenue generator' core system and the company direction statement, this book describes a systems approach which assures significant sustainable improvements in the business and operational performance specific to the oil, gas, and process industries. The book will enable the reader to: utilize best practice principles of good governance for long term performance enhancement; identify the most significant performance indicators for overall business improvement; apply strategies to ensure that targets are met in agreed upon time frames. Describes a systems approach which assures significant sustainable improvements in the business and operational performance specific to the oil, gas, and process industries Helps readers set appropriate and realistic short-term/ long-term targets with a pre-built facility health checker Elucidates the relationship between PSM, OHS, and Asset Integrity with an increased emphasis on behavior-based safety Discusses specific oil and gas industry issues and examples such as refinery and gas plant performance initiatives and hydrocarbon accounting [IT Governance based on CobiT® 4.1 - A Management Guide](#) John Wiley & Sons

Charged with ensuring the confidentiality, integrity, availability, and delivery of all forms of an entity's information, Information Assurance (IA) professionals require a fundamental understanding of a wide range of specializations, including digital forensics, fraud examination, systems engineering, security risk management, privacy, and compliance. Establishing this understanding and keeping it up to date requires a resource with coverage as diverse as the field it covers. Filling this need, the Encyclopedia of Information Assurance presents an up-to-date collection of peer-reviewed articles and references written by authorities in their fields. From risk management and privacy to auditing and compliance, the encyclopedia's four volumes provide comprehensive coverage of the key topics related to information assurance. This complete IA resource: Supplies the understanding needed to help prevent the misuse of sensitive information Explains how to maintain the integrity of critical systems Details effective tools, techniques, and methods for protecting personal and corporate data against the latest threats Provides valuable examples, case studies, and discussions on how to address common and emerging IA challenges Placing the wisdom of leading researchers and practitioners at your fingertips, this authoritative reference provides the knowledge and insight needed to avoid common pitfalls and stay one step ahead of evolving threats. Also Available Online This Taylor & Francis encyclopedia is also available through online subscription, offering a variety of extra benefits for researchers, students, and librarians, including: □ Citation tracking and alerts □ Active reference linking □ Saved searches and marked lists □ HTML and PDF format options Contact Taylor and Francis for more information or to inquire about subscription options and print/online combination packages. US: (Tel) 1.888.318.2367; (E-mail) e-reference@taylorandfrancis.com International: (Tel) +44 (0) 20 7017 6062; (E-mail) online.sales@tandf.co.uk

Network Security and Cyber Defence (CNSS) CRC Press

How will the ISO 27004 data be captured? Is any ISO 27004 documentation required? Are you using a design thinking approach and integrating Innovation, ISO 27004 Experience, and Brand Value? Who do we want your customers to become? Do you combine technical expertise with business knowledge and ISO 27004 Key topics include lifecycles, development approaches, requirements and how to make a business case? Defining, designing, creating, and implementing a process to solve a challenge or meet an objective is the most valuable role... In EVERY group, company, organization and department. Unless you are talking a one-time, single-use project, there should be a process. Whether that process is managed and implemented by humans, AI, or a combination of the two, it needs to be designed by someone with a complex enough perspective to ask the right questions. Someone capable of asking the right questions and step back and say, 'What are we really trying to accomplish here? And is there a different way to look at it?' This Self-Assessment empowers people to do just that - whether their title is entrepreneur, manager, consultant, (Vice-)President, CxO etc... - they are the people who rule the future. They are the person who asks the right questions to make ISO 27004 investments work better. This ISO 27004 All-Inclusive Self-Assessment enables You to be that person. All the tools you need to an in-depth ISO 27004 Self-Assessment. Featuring 943 new and updated case-based questions, organized into seven core areas of process design, this Self-Assessment will help you identify areas in which ISO 27004 improvements can be made. In using the questions you will be better able to: - diagnose ISO 27004 projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices - implement evidence-based best practice strategies aligned with overall goals - integrate recent advances in ISO 27004 and process design strategies into practice according to best practice guidelines Using a Self-Assessment tool known as the ISO 27004 Scorecard, you will develop a clear picture of which ISO 27004 areas need attention. Your purchase includes access details to the ISO 27004 self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows your organization exactly what to do next. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation - In-depth and specific ISO 27004 Checklists - Project management checklists and templates to assist with implementation INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.

It Governance CRC Press

Spanning the multi-disciplinary scope of information technology, the Encyclopedia of Information Systems and Technology draws together comprehensive coverage of the inter-related aspects of information systems and technology. The topics covered in this encyclopedia encompass internationally recognized bodies of knowledge, including those of The IT BOK, the Chartered Information Technology Professionals Program, the International IT Professional Practice Program (British Computer Society), the Core Body of Knowledge for IT Professionals (Australian Computer Society), the International Computer Driving License Foundation (European Computer Driving License Foundation), and the Guide to the Software Engineering Body of Knowledge. Using the universally recognized definitions of IT and information systems from these recognized bodies of knowledge, the encyclopedia brings together the information that students, practicing professionals, researchers, and academicians need to keep their knowledge up to date. Also Available Online This Taylor & Francis encyclopedia is also available through online subscription, offering a variety of extra benefits for researchers, students, and librarians, including: □ Citation tracking and alerts □ Active reference linking □ Saved searches and marked lists □ HTML and PDF format options Contact Taylor and Francis for more information or to inquire about subscription options and print/online combination packages. US: (Tel) 1.888.318.2367; (E-mail) e-reference@taylorandfrancis.com International: (Tel) +44 (0) 20 7017 6062; (E-mail) online.sales@tandf.co.uk

First International Conference, CIIT 2011, Pune, India, November 7-8, 2011. Proceedings IGI Global

The first test prep guide for the new ISC2 Certified Secure Software Lifecycle Professional exam The CSSLP (Certified Secure Software Lifecycle Professional) is a new certification that incorporates government standards and best practices for secure software development. It emphasizes the application of secure software methodologies during the software development cycle. If you're an IT professional, security professional, software developer, project manager, software assurance tester, executive manager or employee of a government agency in a related field, your career may benefit from this certification. Written by experts in computer systems and security, The CSSLP Prep Guide thoroughly covers all aspects of the CSSLP certification exam, with hundreds of sample test questions and answers available on the accompanying CD. The Certified Secure Software Lifecycle Professional (CSSLP) is an international certification incorporating new government, commercial, and university derived secure software development methods; it is a natural complement to the CISSP credential The study guide covers the seven domains of the CSSLP Common Body of Knowledge (CBK), namely Secure Software Concepts, Secure Software Requirements, Secure Software Design, and Secure Software Implementation/Coding and Testing, Secure Software Testing, Software Acceptance, and Software Deployment, Operations, Maintenance and Disposal Provides in-depth exploration and explanation of the seven CSSLP domains Includes a CD with hundreds of practice exam questions and answers The CSSLP Prep Guide prepares you for the certification exam and career advancement.

Encyclopedia of Organizational Knowledge, Administration, and Technology John Wiley & Sons

How to manage the cybersecurity of industrial systems is a crucial question. To implement relevant solutions, the industrial manager must have a clear understanding of IT systems, of communication networks and of control-command systems. They must also have some knowledge of the methods used by attackers, of the standards and regulations involved and of the available security solutions. Cybersecurity of Industrial Systems presents these different subjects in order to give an in-depth overview and to help the reader manage the cybersecurity of their installation. The book addresses these issues for both classic SCADA architecture systems and Industrial Internet of Things (IIoT) systems.

Cyberterrorism, Information Warfare, and Internet Immobilization ISO 27004 A Complete Guide - 2020 Edition

"This book provides relevant frameworks and best practices as well as current empirical research findings for professionals who want to improve their understanding of the impact of cyber-attacks on critical infrastructures and other information systems essential to the smooth running of society, how such attacks are carried out, what measures should be taken to mitigate their impact"--Provided by publisher.

Web Commerce Security IGI Global

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 Springer Science & Business Media

With the global economy still in recovery, it is more important than ever for individuals and organizations to be aware of their money and its potential for both depreciation and growth. Banking, Finance, and Accounting: Concepts, Methodologies, Tools, and Applications investigates recent advances and undertakings in the financial industry to better equip all members of the world economy with the tools and insights needed to weather any shift in the economic climate. With chapters on topics ranging from investment portfolios to credit unions, this multi-volume reference source will serve as a crucial resource for managers, investors, brokers, and all others within the banking industry.

Engineering-Based Establishment of Security Standards Wolters Kluwer Law & Business

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.

Encyclopedia of Information Assurance - 4 Volume Set (Print) Springer Science & Business Media

This book aims to provide the latest research developments and results in the domain of AI techniques for smart cyber ecosystems. It presents a holistic insight into AI-enabled theoretic approaches and methodology in IoT networking, security analytics using AI tools and network automation, which ultimately enable intelligent cyber space. This book will be a valuable resource for students, researchers, engineers and policy makers working in various areas related to cybersecurity and privacy for Smart Cities. This book includes chapters titled "An Overview of the Artificial Intelligence Evolution and Its Fundamental Concepts, and Their Relationship with IoT Security", "Smart City: Evolution and Fundamental Concepts", "Advances in AI-Based Security for Internet of Things in Wireless Virtualization Environment", "A Conceptual Model for Optimal

Resource Sharing of Networked Microgrids Focusing Uncertainty: Paving Path to Eco-friendly Smart Cities", "A Novel Framework for a Cyber Secure Smart City", "Contemplating Security Challenges and Threats for Smart Cities", "Self-Monitoring Obfuscated IoT Network", "Introduction to Side Channel Attacks and Investigation of Power Analysis and Fault Injection Attack Techniques", "Collaborative Digital Forensic Investigations Model for Law Enforcement: Oman as a Case Study", "Understanding Security Requirements and Challenges in the Industrial Internet of Things: A Review", "5G Security and the Internet of Things", "The Problem of Deepfake Videos and How to Counteract Them in Smart Cities", "The Rise of Ransomware Aided by Vulnerable IoT Devices", "Security Issues in Self-Driving Cars within Smart Cities", and "Trust-Aware Crowd Associated Network-Based Approach for Optimal Waste Management in Smart Cities". This book provides state-of-the-art research results and discusses current issues, challenges, solutions and recent trends related to security and organization within IoT and Smart Cities. We expect this book to be of significant importance not only to researchers and practitioners in academia, government agencies and industries, but also for policy makers and system managers. We anticipate this book to be a valuable resource for all those working in this new and exciting area, and a "must have" for all university libraries.

Building a Practical Information Security Program CRC Press

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.

Advances in Communications, Computing, Networks and Security Volume 10 John Wiley & Sons Everything you need to know about information security programs and policies, in one book Clearly explains all facets of InfoSec program and policy planning, development, deployment, and management Thoroughly updated for today's challenges, laws, regulations, and best practices The perfect resource for anyone pursuing an information security management career In today's dangerous world, failures in information security can be catastrophic. Organizations must protect themselves. Protection begins with comprehensive, realistic policies. This up-to-date guide will help you create, deploy, and manage them. Complete and easy to understand, it explains key concepts and techniques through real-life examples. You'll master modern information security regulations and frameworks, and learn specific best-practice policies for key industry sectors, including finance, healthcare, online commerce, and small business. If you understand basic

information security, you're ready to succeed with this book. You'll find projects, questions, exercises, examples, links to valuable easy-to-adapt information security policies...everything you need to implement a successful information security program. Sari Stern Greene, CISSP, CRISC, CISM, NSA/IAM, is an information security practitioner, author, and entrepreneur. She is passionate about the importance of protecting information and critical infrastructure. Sari founded Sage Data Security in 2002 and has amassed thousands of hours in the field working with a spectrum of technical, operational, and management personnel, as well as boards of directors, regulators, and service providers. Her first text was Tools and Techniques for Securing Microsoft Networks, commissioned by Microsoft to train its partner channel, which was soon followed by the first edition of Security Policies and Procedures: Principles and Practices. She is actively involved in the security community, and speaks regularly at security conferences and workshops. She has been quoted in The New York Times, Wall Street Journal, and on CNN, and CNBC. Since 2010, Sari has served as the chair of the annual Cybercrime Symposium. Learn how to

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

Banking, Finance, and Accounting: Concepts, Methodologies, Tools, and Applications Kogan Page Publishers

In today's society, where technology is ubiquitous, protecting ourselves with firewalls is as important as defending ourselves with firepower. New technology is providing criminals with a world of opportunity, while law enforcement agencies all over the world are struggling to cope. E-security is an issue of global importance. In many ways, cybercrime is no different to more traditional types of crime - both involve identifying targets, using surveillance and psychological profiling of potential victims. The major difference is that the perpetrators of cybercrime are increasingly remote to the scene of their crime and that in some cases their victims may not even realize that a crime is taking place. Knowledge of the techniques being used by criminals and the technology and training available to combat them is essential in fighting cybercrime. Establishing dialogue between crime-fighting agencies, the security industry, researchers and experts can provide a platform from which e-security can be examined from several global perspectives.

4th International Conference, ICGeS 2008, London, UK, June 23-25, 2008, Proceedings John Wiley & Sons

The most comprehensive General, Organic, and Biochemistry book available, Introduction to General, Organic, and Biochemistry, 11th Edition continues its tradition of a solid development of problem-solving skills, numerous examples and practice problems, along with coverage of current applications. Written by an experienced author team, they skillfully anticipate areas of difficulty and pace the book accordingly. Readers will find the right mix of general chemistry compared to the discussions on organic and biochemistry. Introduction to General, Organic, and Biochemistry, 11th Edition has clear & logical explanations of chemical concepts and great depth of coverage as well as a clear, consistent writing style which provides great readability. An emphasis on Real-World aspects of chemistry makes the reader comfortable in seeing how the chemistry will apply to their career.

10th International Conference, TrustBus 2013, Prague, Czech Republic, August 28-29, 2013, Proceedings Van Haren

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.

Computer Networks and Information Technologies Springer

It provides a holistic view of modern network security including operating system hardening, Firewalls, intrusion-detection systems, VPNs and Encryption. Physical Security, Standards, System Security and Security Policies are also included. Before diving into how to protect a network, exploring what networks are, would probably be a good idea. For many readers this section will be a review, but for some it might be new material. Whether this is a review for you, or new information, having a thorough understanding of basic networking before attempting to study network security is critical. Also, be aware this is just a brief introduction of basic network concepts.

The CSSLP Prep Guide Gulf Professional Publishing

Provides information on designing effective security mechanisms for e-commerce sites, covering such topics as cryptography, authentication, information classification, threats and attacks, and certification.

Related with Iso 27004:

[© Iso 27004 Ap French Exam Score Calculator](#)

[© Iso 27004 Ap English Literature And Composition Practice Exam](#)

[© Iso 27004 Ap Gov Ultimate Review Packet Answer Key](#)