

The Iso27k Standards Iso 27001 Security

Getting the books **The Iso27k Standards Iso 27001 Security** now is not type of inspiring means. You could not forlorn going later than ebook buildup or library or borrowing from your links to right of entry them. This is an completely simple means to specifically acquire guide by on-line. This online publication The Iso27k Standards Iso 27001 Security can be one of the options to accompany you as soon as having other time.

It will not waste your time. say yes me, the e-book will unquestionably proclaim you further matter to read. Just invest little epoch to right of entry this on-line pronouncement **The Iso27k Standards Iso 27001 Security** as well as evaluation them wherever you are now.

Learn Social Engineering - Dr. Erdal Ozkaya
2018-04-30

Improve information security by learning Social Engineering. Key Features Learn to implement information security using social engineering Get hands-on experience of using different tools such as Kali Linux, the Social Engineering toolkit

and so on Practical approach towards learning social engineering, for IT security Book Description This book will provide you with a holistic understanding of social engineering. It will help you to avoid and combat social engineering attacks by giving you a detailed insight into how a social engineer operates.

Learn Social Engineering starts by giving you a grounding in the different types of social engineering attacks, and the damages they cause. It then sets up the lab environment to use different tools and then perform social engineering steps such as information gathering. The book covers topics from baiting, phishing, and spear phishing, to pretexting and scareware. By the end of the book, you will be in a position to protect yourself and your systems from social engineering threats and attacks. All in all, the book covers social engineering from A to Z, along with excerpts from many world wide known security experts. What you will learn

- Learn to implement information security using social engineering
- Learn social engineering for IT security
- Understand the role of social media in social engineering
- Get acquainted with Practical Human hacking skills
- Learn to think like a social engineer
- Learn to beat a social engineer

Who this book is for This book targets security professionals, security analysts,

penetration testers, or any stakeholder working with information security who wants to learn how to use social engineering techniques. Prior knowledge of Kali Linux is an added advantage

Information Security Management Based on Iso 27001 2013 - Anis Radianis 2015-09-15

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.

Computer Security - Sokratis Katsikas
2020-02-21

This book constitutes the refereed post-conference proceedings of the 5th International Workshop on Security of Industrial Control Systems and Cyber-Physical Systems, CyberICPS 2019, the Third International Workshop on Security and Privacy Requirements Engineering, SECPRE 2019, the First International Workshop on Security, Privacy, Organizations, and Systems Engineering, SPOSE 2019, and the Second International Workshop on Attacks and Defenses for Internet-of-Things, ADIoT 2019, held in Luxembourg City, Luxembourg, in September 2019, in conjunction with the 24th European Symposium on Research in Computer Security, ESORICS 2019. The CyberICPS Workshop

received 13 submissions from which 5 full papers and 2 short papers were selected for presentation. They cover topics related to threats, vulnerabilities and risks that cyber-physical systems and industrial control systems face; cyber attacks that may be launched against such systems; and ways of detecting and responding to such attacks. From the SECPRE Workshop 9 full papers out of 14 submissions are included. The selected papers deal with aspects of security and privacy requirements assurance and evaluation; and security requirements elicitation and modelling and to GDPR compliance. The SPOSE Workshop received 7 submissions from which 3 full papers and 1 demo paper were accepted for publication. They demonstrate the possible spectrum for fruitful research at the intersection of security, privacy, organizational science, and systems engineering. From the ADIoT Workshop 5 full papers and 2 short papers out of 16 submissions are included. The papers focus on IoT attacks

and defenses and discuss either practical or theoretical solutions to identify IoT vulnerabilities and IoT security mechanisms.

IT Governance - Alan Calder 2008

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.

ISO27001 in a Windows Environment - Brian Honan 2014-07-29

Most ISO27001 implementations will involve a Windows® environment at some level. The two approaches to security, however, mean that there is often a knowledge gap between those trying to implement ISO27001 and the IT specialists trying to put the necessary best practice controls in place while using Microsoft®’s technical controls. ISO27001 in a Windows® Environment bridges the gap and gives essential guidance to everyone involved in a Windows®-based ISO27001 project.

Information Security Risk Management - Edward Humphreys 2010

Data processing, Computers, Management, Data security, Data storage protection, Risk assessment, Risk analysis, Data management, Information exchange, Business continuity, Anti-burglar measures, Documents, IT and

Information Management: Information Security
**Foundations of Information Security Based
on ISO27001 and ISO27002** - Hans Baars
1970-01-01

Note: Also available for this book: 3rd revised edition (2015) 9789401800129; available in two languages: Dutch, English. 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. Information security issues impact all organizations; however measures used to implement effective measures are often viewed as a businesses barrier costing a great deal of money. This practical title clearly explains the approaches that most organizations can consider and implement which helps turn Information Security management into an approachable, effective and well-understood tool. It covers: The quality requirements an organization may have for information; The risks associated with these quality requirements; The countermeasures that

are necessary to mitigate these risks; Ensuring business continuity in the event of a disaster; When and whether to report incidents outside the organization. All information security concepts in this book are based on the ISO/IEC 27001 and ISO/IEC 27002 standards. But the text also refers to the other relevant international standards for information security. The text is 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 book also contains many Case Studies which usefully demonstrate how theory translates into an operating environment. This book is primarily developed as a study book for anyone who wants to pass the ISFS (Information Security Foundation) exam of

EXIN. In an appendix an ISFS model exam is given, with feedback to all multiple choice options, so that it can be used as a training for the real ISFS exam.

An Introduction to ISO/IEC 27001:2013 - British Standards Institute Staff 2013

Data processing, Computers, Management, Data security, Data storage protection, Anti-burglar measures, Information systems, Documents, Records (documents), Classification systems, Computer technology, Computer networks, Technical documents, Maintenance, Information exchange

Information Security Risk Management for ISO27001/ISO27002 - Alan Calder 2010-04-27

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.

Foundations of Information Security Based on ISO27001 and ISO27002 - Hans Baars
2010-04-09

Information security issues impact all organizations; however measures used to implement effective measures are often viewed as a businesses barrier costing a great deal of money. This practical title clearly explains the approaches that most organizations can consider and implement which helps turn Information Security management into an approachable, effective and well-understood tool. It covers: The quality requirements an organization may have for information; The risks associated with these quality requirements; The countermeasures that are necessary to mitigate these risks; Ensuring business continuity in the event of a disaster; When and whether to report incidents outside the organization. All information security concepts in this book are based on the ISO/IEC

27001 and ISO/IEC 27002 standards. But the text also refers to the other relevant international standards for information security. The text is 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 book also contains many Case Studies which usefully demonstrate how theory translates into an operating environment This book is primarily developed as a study book for anyone who wants to pass the ISFS (Information Security Foundation) exam of EXIN. In an appendix an ISFS model exam is given, with feedback to all multiple choice options, so that it can be used as a training for the 'real' ISFS exam. *Information Systems Security and Privacy -*

Paolo Mori 2019-07-04

This book constitutes the revised selected papers of the 4th International Conference on Information Systems Security and Privacy, ICISSP 2018, held in Funchal - Madeira, Portugal, in January 2018. The 15 full papers presented were carefully reviewed and selected from a total of 71 submissions. They are dealing with topics such as data and software security; privacy and confidentiality; mobile systems security; biometric authentication; information systems security and privacy; authentication, privacy and security models; data mining and knowledge discovery; phishing; security architecture and design analysis; security testing; vulnerability analysis and countermeasures; web applications and services. *Application security in the ISO27001:2013 Environment - Vinod Vasudevan 2015-10-15* Application Security in the ISO 27001:2013 Environment explains how organisations can implement and maintain effective security

practices to protect their web applications - and the servers on which they reside - as part of a wider information security management system by following the guidance set out in the international standard for information security management, ISO 27001. The book describes the methods used by criminal hackers to attack organisations via their web applications and provides a detailed explanation of how you can combat such attacks by employing the guidance and controls set out in ISO 27001. Product overview
Second edition, updated to reflect ISO 27001:2013 as well as best practices relating to cryptography, including the PCI SSC's denigration of SSL in favour of TLS. Provides a full introduction to ISO 27001 and information security management systems, including implementation guidance. Describes risk assessment, management and treatment approaches. Examines common types of web app security attack, including injection attacks, cross-site scripting, and attacks on

authentication and session management, explaining how each can compromise ISO 27001 control objectives and showing how to test for each attack type. Discusses the ISO 27001 controls relevant to application security. Lists useful web app security metrics and their relevance to ISO 27001 controls. Provides a four-step approach to threat profiling, and describes application security review and testing approaches. Sets out guidelines and the ISO 27001 controls relevant to them, covering: input validation authentication authorisation sensitive data handling and the use of TLS rather than SSL session management error handling and logging Describes the importance of security as part of the web app development process
The Case for the Iso27001 - It Governance 2013-11

This guide, updated to reflect ISO27001:2013, presents the compelling business case for implementing ISO27001 in order to protect your information assets. Ideal reading for anyone

unfamiliar with the many benefits of the Standard, this is a clear and concise introduction and perfect supporting text for an ISO27001 project proposal.

Governance, Risk, and Compliance Handbook -

Anthony Tarantino 2008-03-11

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.

Enterprise Security Architecture - Rassoul Ghaznavi-Zadeh 2015-06-28

This book is a complete guide for those who would like to become an Enterprise Security

Architect. In this book you will learn all the necessary security requirement and considerations in Enterprise organizations. You will need to be in security industry to get the most out of this book but it has been designed in a way to cover all the requirements for beginners up to professionals. After reading this book, you should be able to use these techniques and procedures in any enterprise company with any field. Becoming a Security Architect is not obviously happening over a night and lots of effort and practice is required. However; if you keep reviewing the methods and concepts in this book, you will soon become a great Security Architect with extensive knowledge about business. You will learn how to use security practices to enable business to achieve its goals.

ISO 27001 Handbook - Cees Wens 2019-12-24

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.

Implementing the ISO/IEC 27001:2013 ISMS Standard - Edward Humphreys 2016-03-01
Authored by an internationally recognized

expert in the field, this expanded, timely second edition addresses all the critical information security management issues needed to help businesses protect their valuable assets. Professionals learn how to manage business risks, governance and compliance. This updated resource provides a clear guide to ISO/IEC 27000 security standards and their implementation, focusing on the recent ISO/IEC 27001. Moreover, readers are presented with practical and logical information on standard accreditation and certification. From information security management system (ISMS) business context, operations, and risk, to leadership and support, this invaluable book is your one-stop resource on the ISO/IEC 27000 series of standards.

Information Security Management Systems -
Heru Susanto 2018-06-14

This new volume, *Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with*

Information Security Standard, looks at information security management system standards, risk management associated with information security, and information security awareness within an organization. The authors aim to improve the overall ability of organizations to participate, forecast, and actively assess their information security circumstances. It is important to note that securing and keeping information from parties who do not have authorization to access such information is an extremely important issue. To address this issue, it is essential for an organization to implement an ISMS standard such as ISO 27001 to address the issue comprehensively. The authors of this new volume have constructed a novel security framework (ISF) and subsequently used this framework to develop software called Integrated Solution Modeling (ISM), a semi-automated system that will greatly help organizations comply with ISO 27001 faster and cheaper than

other existing methods. In addition, ISM does not only help organizations to assess their information security compliance with ISO 27001, but it can also be used as a monitoring tool, helping organizations monitor the security statuses of their information resources as well as monitor potential threats. ISM is developed to provide solutions to solve obstacles, difficulties, and expected challenges associated with literacy and governance of ISO 27001. It also functions to assess the RISC level of organizations towards compliance with ISO 27001. The information provide here will act as blueprints for managing information security within business organizations. It will allow users to compare and benchmark their own processes and practices against these results shown and come up with new, critical insights to aid them in information security standard (ISO 27001) adoption.

IT Governance - Alan Calder 2012-04-03

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 fully updated to take account of the latest regulatory and technological developments, including the creation of the International Board for IT Governance Qualifications. IT Governance also includes new material on key international markets - including the UK and the US, Australia and South Africa.

Implementing an Information Security Management System - Abhishek Chopra
2019-12-09

Discover the simple steps to implementing information security standards using ISO 27001, the most popular information security standard across the world. You'll see how it offers best practices to be followed, including the roles of all the stakeholders at the time of security framework implementation, post-implementation, and during monitoring of the implemented controls. Implementing an Information Security Management System

provides implementation guidelines for ISO 27001:2013 to protect your information assets and ensure a safer enterprise environment. This book is a step-by-step guide on implementing secure ISMS for your organization. It will change the way you interpret and implement information security in your work area or organization. What You Will Learn Discover information safeguard methods Implement end-to-end information security Manage risk associated with information security Prepare for audit with associated roles and responsibilities Identify your information risk Protect your information assets Who This Book Is For Security professionals who implement and manage a security framework or security controls within their organization. This book can also be used by developers with a basic knowledge of security concepts to gain a strong understanding of security standards for an enterprise.

Implementing Information Security based on ISO

27001/ISO 27002 - Alan Calder 2011-09-09

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 *Information Security Risk Management for ISO 27001/ISO 27002, third edition* - Alan Calder 2019-08-29

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.

Cybersecurity - Ishaani Priyadarshini 2022-03-10
This book is the first of its kind to introduce the integration of ethics, laws, risks, and policies in cyberspace. The book provides understanding of the ethical and legal aspects of cyberspace along with the risks involved. It also addresses current and proposed cyber policies, serving as a

summary of the state of the art cyber laws in the United States. It also, importantly, incorporates various risk management and security strategies from a number of organizations. Using easy-to-understand language and incorporating case studies, the authors begin with the consideration of ethics and law in cybersecurity and then go on to take into account risks and security policies. The section on risk covers identification, analysis, assessment, management, and remediation. The very important topic of cyber insurance is covered as well—its benefits, types, coverage, etc. The section on cybersecurity policy acquaints readers with the role of policies in cybersecurity and how they are being implemented by means of frameworks. The authors provide a policy overview followed by discussions of several popular cybersecurity frameworks, such as NIST, COBIT, PCI/DSS, ISO series, etc.

Implementing the ISO/IEC 27001 Information Security Management System

Standard - Edward Humphreys 2007
Authored by an internationally recognized expert in the field, this timely book provides you with an authoritative and clear guide to the ISO/IEC 27000 security standards and their implementation. The book addresses all the critical information security management issues that you need to understand to help protect your business's valuable assets, including dealing with business risks and governance and compliance. Moreover, you find practical information on standard accreditation and certification. From information security management system (ISMS) design and deployment, to system monitoring, reviewing and updating, this invaluable book is your one-stop resource on the ISO/IEC 27000 series of standards.

Foundations of Information Security Based on ISO27001 and ISO27002 - 3rd revised edition - Hans Baars 2015-04-01

This book is intended for everyone in an

organization who wishes to have a basic understanding of information security. Knowledge about information security is important to all employees. It makes no difference if you work in a profit- or non-profit organization because the risks that organizations face are similar for all organizations. It clearly explains the approaches that most organizations can consider and implement which helps turn Information Security management into an approachable, effective and well-understood tool. It covers: The quality requirements an organization may have for information; The risks associated with these quality requirements; The countermeasures that are necessary to mitigate these risks; Ensuring business continuity in the event of a disaster; When and whether to report incidents outside the organization. The information security concepts in this revised edition are based on the ISO/IEC27001:2013 and ISO/IEC27002:2013 standards. But the text also refers to the other

relevant international standards for information security. The text is structured as follows: Fundamental Principles of Security and Information security and Risk management. Architecture, processes and information, needed for basic understanding of what information security is about. Business Assets are discussed. Measures that can be taken to protect information assets. (Physical measures, technical measures and finally the organizational measures.) The primary objective of this book is to achieve awareness by students who want to apply for a basic information security examination. It is a source of information for the lecturer who wants to question information security students about their knowledge. Each chapter ends with a case study. In order to help with the understanding and coherence of each subject, these case studies include questions relating to the areas covered in the relevant chapters. Examples of recent events that illustrate the vulnerability of information are

also included. This book is primarily developed as a study book for anyone who wants to pass the ISFS (Information Security Foundation) exam of EXIN. In an appendix an ISFS model exam is given, with feedback to all multiple choice options, so that it can be used as a training for the real ISFS exam.

Information Security Policies, Procedures, and Standards - Douglas J. Landoll 2017-03-27

Information Security Policies, Procedures, and Standards: A Practitioner's Reference gives you a blueprint on how to develop effective information security policies and procedures. It uses standards such as NIST 800-53, ISO 27001, and COBIT, and regulations such as HIPAA and PCI DSS as the foundation for the content. Highlighting key terminology, policy development concepts and methods, and suggested document structures, it includes examples, checklists, sample policies and procedures, guidelines, and a synopsis of the applicable standards. The author explains how

and why procedures are developed and implemented rather than simply provide information and examples. This is an important distinction because no two organizations are exactly alike; therefore, no two sets of policies and procedures are going to be exactly alike. This approach provides the foundation and understanding you need to write effective policies, procedures, and standards clearly and concisely. Developing policies and procedures may seem to be an overwhelming task. However, by relying on the material presented in this book, adopting the policy development techniques, and examining the examples, the task will not seem so daunting. You can use the discussion material to help sell the concepts, which may be the most difficult aspect of the process. Once you have completed a policy or two, you will have the courage to take on even more tasks. Additionally, the skills you acquire will assist you in other areas of your professional and private life, such as expressing an idea

clearly and concisely or creating a project plan.

An Introduction to Information Security and

ISO27001:2013 - Steve G. Watkins 2013

The perfect introduction to the principles of information security management and ISO27001:2013

Transforming Cybersecurity: Using COBIT 5 - ISACA 2013-06-18

The cost and frequency of cybersecurity incidents are on the rise, is your enterprise keeping pace? The numbers of threats, risk scenarios and vulnerabilities have grown exponentially. Cybersecurity has evolved as a new field of interest, gaining political and societal attention. Given this magnitude, the future tasks and responsibilities associated with cybersecurity will be essential to organizational survival and profitability. This publication applies the COBIT 5 framework and its component publications to transforming cybersecurity in a systemic way. First, the impacts of cybercrime and cyberwarfare on

business and society are illustrated and put in context. This section shows the rise in cost and frequency of security incidents, including APT attacks and other threats with a critical impact and high intensity. Second, the transformation addresses security governance, security management and security assurance. In accordance with the lens concept within COBIT 5, these sections cover all elements of the systemic transformation and cybersecurity improvements.

CyberWar, CyberTerror, CyberCrime and CyberActivism - Julie Mehan 2014-05-08

This book encourages cybersecurity professionals to take a wider view of what cybersecurity means, and to exploit international standards and best practice to create a culture of cybersecurity awareness within their organization that supplements technology-based defenses.

ISO27001 / ISO27002 - Alan Calder 2013-10-03
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.

IT Governance - Alan Calder 2019-10-03

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

ISO 27001 controls - A guide to implementing and auditing - Bridget Kenyon 2019-09-16

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.

An Introduction to Information Security and ISO27001:2013 - Steve Watkins 2013-10-03

Quickly understand the principles of information security.

Security Controls Evaluation, Testing, and Assessment Handbook - Leighton Johnson 2019-11-21

Security Controls Evaluation, Testing, and Assessment Handbook, Second Edition, provides a current and well-developed approach to evaluate and test IT security controls to prove they are functioning correctly. This handbook discusses the world of threats and potential breach actions surrounding all industries and systems. Sections cover how to take FISMA, NIST Guidance, and DOD actions, while also providing a detailed, hands-on guide to performing assessment events for information security professionals in US federal agencies. This handbook uses the DOD Knowledge Service and the NIST Families assessment guides as the basis for needs assessment, requirements and

evaluation efforts. Provides direction on how to use SP800-53A, SP800-115, DOD Knowledge Service, and the NIST Families assessment guides to implement thorough evaluation efforts Shows readers how to implement proper evaluation, testing, assessment procedures and methodologies, with step-by-step walkthroughs of all key concepts Presents assessment techniques for each type of control, provides evidence of assessment, and includes proper reporting techniques

Nine Steps to Success - Alan Calder 2017-10-03
Step-by-step guidance on a successful ISO 27001 implementation from an industry leader
Resilience to cyber attacks requires an organization to defend itself across all of its attack surface: people, processes, and technology. ISO 27001 is the international standard that sets out the requirements of an information security management system (ISMS) - a holistic approach to information security that encompasses people, processes, and technology.

Accredited certification to the Standard is recognized worldwide as the hallmark of best-practice information security management. Achieving and maintaining accredited certification to ISO 27001 can be complicated, especially for those who are new to the Standard. Author of *Nine Steps to Success - An ISO 27001 Implementation Overview*, Alan Calder is the founder and executive chairman of IT Governance. He led the world's first implementation of a management system certified to BS 7799, the forerunner to ISO 27001, and has been working with the Standard ever since. Hundreds of organizations around the world have achieved accredited certification to ISO 27001 with IT Governance's guidance, which is distilled in this book.

Securing the Smart Grid - Tony Flick 2010-11-03
Securing the Smart Grid discusses the features of the smart grid, particularly its strengths and weaknesses, to better understand threats and attacks, and to prevent insecure deployments of

smart grid technologies. A smart grid is a modernized electric grid that uses information and communications technology to be able to process information, such as the behaviors of suppliers and consumers. The book discusses different infrastructures in a smart grid, such as the automatic metering infrastructure (AMI). It also discusses the controls that consumers, device manufacturers, and utility companies can use to minimize the risk associated with the smart grid. It explains the smart grid components in detail so readers can understand how the confidentiality, integrity, and availability of these components can be secured or compromised. This book will be a valuable reference for readers who secure the networks of smart grid deployments, as well as consumers who use smart grid devices. Details how old and new hacking techniques can be used against the grid and how to defend against them Discusses current security initiatives and how they fall short of what is needed Find out how hackers

can use the new infrastructure against itself

Nine Steps to Success - Alan Calder

2016-05-17

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

ISO27001/ISO27002 - Alan Calder 2013-10

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.

Cyber Security - Xiaochun Yun 2019-01-01

This open access book constitutes the refereed proceedings of the 15th International Annual Conference on Cyber Security, CNCERT 2018, held in Beijing, China, in August 2018. The 14 full papers presented were carefully reviewed and selected from 53 submissions. The papers cover the following topics: emergency response, mobile internet security, IoT security, cloud security, threat intelligence analysis, vulnerability, artificial intelligence security, IPv6 risk research, cybersecurity policy and

regulation research, big data analysis and industrial security.

Information Technology Risk Management in Enterprise Environments - Jake Kouns
2011-10-04

Discusses all types of corporate risks and practical means of defending against them. Security is currently identified as a critical area of Information Technology management by a majority of government, commercial, and industrial organizations. Offers an effective risk management program, which is the most critical function of an information security program.