Get Free Iso 27002 Compliance Guide Rapid7 Read Pdf Free

EU General Data Protection Regulation (GDPR) – An implementation and compliance guide, fourth edition Executive's Guide to IT Governance ISO27001 / ISO27002 Information Security based on ISO 27001/ISO 27002 Risk Management: The Open Group Guide Information Security Risk Management for ISO 27001/ISO 27002, third edition The Manager's Guide to Cybersecurity Law IT Governance Iso/Iec 27002 Foundation Complete Certification Kit Implementing Information Security based on ISO 27001/ISO 27002 AWS Certified Solutions Architect Official Study Guide Network and Information Systems (NIS) Regulations - A pocket guide for operators of essential services A concise introduction to the NIS Directive - A pocket guide for digital service providers ISO/Iec 27002 Foundation Complete Certification Kit - Study Guide Book and Online Course - Second Edition AWS Certified Solutions Architect - Professional Complete Study Guide: Network and Information Systems (NIS) Regulations - A pocket guide for digital service providers Enterprise Cybersecurity in Digital Business CompTIA Security+ Review Guide PCI DSS: A Pocket Guide, fifth edition CompTIA Security+ Study Guide Information Security Risk Management for ISO27001/ISO27002 CompTIA Security+ Deluxe Study Guide with Online Labs ISO 27001 Controls Official (ISC)2 Guide to the CISSP-ISSMP CBK CISM Certified Information Security Manager Study Guide HCISPP Study Guide Iso27001/Iso27002 a Pocket Guide US National Cyber Security Strategy and Programs Handbook Volume 1 Strategic Information and Developments Information Assurance Architecture Implementing the ISO/IEC 27001:2013 ISMS Standard Official (ISC)2® Guide to the ISSMP® CBK® CASP+ CompTIA Advanced Security Practitioner Study Guide Guide to Security Assurance for Cloud Computing AWS Certified Security Study Guide The CSSLP Prep Guide CISSP Study Guide IT Governance Security Program and Policies Developing Cybersecurity Programs and Policies SSCP (ISC)2 Systems Security Certified Practitioner Official Study Guide

Enterprise Cybersecurity in Digital Business Oct 05 2021 Cyber risk is the highest perceived business risk according to risk managers and corporate insurance experts. Cybersecurity typically is viewed as the boogeyman: it strikes fear into the hearts of non-technical employees. Enterprise Cybersecurity in Digital Business: Building a Cyber Resilient Organization provides a clear guide for companies to understand cyber from a business perspective rather than a technical perspective, and to build resilience for their business. Written by a world-renowned expert in the field, the book is based on three years of research with the Fortune 1000 and cyber insurance industry carriers, reinsurers, and brokers. It acts as a roadmap to understand cybersecurity maturity, set goals to increase resiliency, create new roles to fill business gaps related to cybersecurity, and make cyber inclusive for everyone in the business. It is unique since it provides strategies and learnings that have shown to lower risk and demystify cyber for each person. With a clear structure covering the key areas of the Evolution of Cybersecurity, Cybersecurity Basics, Cybersecurity Tools, Cybersecurity Regulation, Cybersecurity Incident Response, Forensics and Audit, GDPR, Cybersecurity Insurance, Cybersecurity Risk Management, Cybersecurity Risk Management Strategy, and Vendor Risk Management Strategy, the book provides a guide for professionals as well as a key text for students studying this field. The book is essential reading for CEOs,

Chief Information Security Officers, Data Protection Officers, Compliance Managers, and other cyber stakeholders, who are looking to get up to speed with the issues surrounding cybersecurity and how they can respond. It is also a strong textbook for postgraduate and executive education students in cybersecurity as it relates to business.

CISM Certified Information Security Manager Study Guide Jan 28 2021 Sharpen your information security skills and grab an invaluable new credential with this unbeatable study guide As cybersecurity becomes an increasingly mission-critical issue, more and more employers and professionals are turning to ISACA's trusted and recognized Certified Information Security Manager qualification as a tried-and-true indicator of information security management expertise. In Wiley's Certified Information Security Manager (CISM) Study Guide, you'll get the information you need to succeed on the demanding CISM exam. You'll also develop the IT security skills and confidence you need to prove yourself where it really counts: on the job. Chapters are organized intuitively and by exam objective so you can easily keep track of what you've covered and what you still need to study. You'll also get access to a pre-assessment, so you can find out where you stand before you take your studies further. Sharpen your skills with Exam Essentials and chapter review questions with detailed explanations in all four of the CISM exam domains: Information Security Governance, Information Security Risk Management, Information Security Program, and Incident Management. In this essential resource, you'll also: Grab a head start to an in-demand certification used across the information security industry Expand your career opportunities to include rewarding and challenging new roles only accessible to those with a CISM credential Access the Sybex online learning center, with chapter review questions, full-length practice exams, hundreds of electronic flashcards, and a glossary of key terms Perfect for anyone prepping for the challenging CISM exam or looking for a new role in the information security field, the Certified Information Security Manager (CISM) Study Guide is an indispensable resource that will put you on the fast track to success on the test and in your next job.

CompTIA Security+ Study Guide Jul 02 2021 Learn the key objectives and most crucial concepts covered by the Security+ Exam SY0-601 with this comprehensive and practical study guide! An online test bank offers 650 practice questions and flashcards! The Eighth Edition of the CompTIA Security+ Study Guide Exam SY0-601 efficiently and comprehensively prepares you for the SY0-601 Exam. Accomplished authors and security experts Mike Chapple and David Seidl walk you through the fundamentals of crucial security topics, including the five domains covered by the SY0-601 Exam: Attacks, Threats, and Vulnerabilities Architecture and Design Implementation Operations and Incident Response Governance, Risk, and Compliance The study guide comes with the Sybex online, interactive learning environment offering 650 practice questions! Includes a pre-assessment test, hundreds of review questions, practice exams, flashcards, and a glossary of key terms. The book is written in a practical and straightforward manner, ensuring you can easily learn and retain the material. Perfect for everyone planning to take the SY0-601 Exam—as well as those who hope to secure a high-level certification like the CASP+, CISSP, or CISA—the study guide also belongs on the bookshelves of everyone who has ever wondered if the field of IT security is right for them. It’s a must-have reference!

Risk Management: The Open Group Guide Oct 17 2022 This book brings together The Open Group s set of publications addressing risk management, which have been developed and approved by The Open Group. It is presented in three parts:The Technical Standard for Risk TaxonomyTechnical Guide to the Requirements for Risk Assessment MethodologiesTechnical Guide: FAIR ISO/IEC 27005 CookbookPart 1: Technical Standard for Risk Taxonomy This Part provides a standard definition and taxonomy for information security risk, as well as information regarding

how to use the taxonomy. The intended audience for this Part includes anyone who needs to understand and/or analyze a risk condition. This includes, but is not limited to:Information security and risk management professionalsAuditors and regulatorsTechnology professionalsManagementThis taxonomy is not limited to application in the information security space. It can, in fact, be applied to any risk scenario. This means the taxonomy to be used as a foundation for normalizing the results of risk analyses across varied risk domains.Part 2: Technical Guide: Requirements for Risk Assessment MethodologiesThis Part identifies and describes the key characteristics that make up any effective risk assessment methodology, thus providing a common set of criteria for evaluating any given risk assessment methodology against a clearly defined common set of essential requirements. In this way, it explains what features to look for when evaluating the capabilities of any given methodology, and the value those features represent.Part 3: Technical Guide: FAIR ISO/IEC 27005 CookbookThis Part describes in detail how to apply the FAIR (Factor Analysis for Information Risk) methodology to any selected risk management framework. It uses ISO/IEC 27005 as the example risk assessment framework. FAIR is complementary to all other risk assessment models/frameworks, including COSO, ITIL, ISO/IEC 27002, COBIT, OCTAVE, etc. It provides an engine that can be used in other risk models to improve the quality of the risk assessment results. The Cookbook enables risk technology practitioners to follow by example how to apply FAIR to other risk assessment models/frameworks of their choice.

Information Security Risk Management for ISO 27001/ISO 27002, third edition Sep 16 2022 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.

AWS Certified Solutions Architect - Professional Complete Study Guide: Dec 07 2021 The AWS Certified Solutions Architect Professional exam validates advanced technical skills and experience in designing distributed applications and systems on the AWS platform. Example concepts you should understand for this exam include: - Designing and deploying dynamically scalable, highly available, fault-tolerant, and reliable applications on AWS - Selecting appropriate AWS services to design and deploy an application based on given requirements - Migrating complex, multi-tier applications on AWS - Designing and deploying enterprise-wide scalable operations on AWS - Implementing cost-control strategies - Recommended AWS Knowledge This book contains Free Resources. Preview the book & see what's inside.

Developing Cybersecurity Programs and Policies Nov 13 2019 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

Information Assurance Architecture Sep 23 2020 Now that information has become the lifeblood of your organization, you must be especially vigilant about assuring it. The hacker, spy, or cyber-thief of today can breach any barrier if it remains unchanged long enough or has even the tiniest leak. In Information Assurance Architecture, Keith D. Willett draws on his over 25 years of technical, security, and business experience to provide a framework for organizations to align information assurance with the enterprise and their overall mission. The Tools to Protect Your Secrets from Exposure This work provides the security industry with the know-how to create a formal information assurance architecture that complements an enterprise architecture, systems engineering, and the enterprise life cycle management (ELCM). Information Assurance Architecture consists of a framework, a process, and many supporting tools, templates and methodologies. The framework provides a reference model for the consideration of security in many contexts and from various perspectives; the process provides direction on how to apply that framework. Mr. Willett teaches readers how to identify and use the right tools for the right job. Furthermore, he demonstrates a disciplined approach in thinking about, planning, implementing and managing security, emphasizing that solid solutions can be made impenetrable when they are seamlessly integrated with the whole of an enterprise. Understand the Enterprise Context This book covers many information assurance subjects, including disaster recovery and firewalls. The objective is to present security services and security mechanisms in the context of information assurance architecture, and in an enterprise context of managing business risk. Anyone who utilizes the concepts taught in these pages will find them to be a valuable weapon in the arsenal of information protection.

Official (ISC)2 Guide to the CISSP-ISSMP CBK Feb 26 2021 The Certified Information Systems Security Professional-Information Systems Security Management Professional (CISSP-ISSMP) certification was developed for CISSPs who are seeking to further their careers and validate their expertise in information systems security management. Candidates for the ISSMP need to demonstrate a thorough understanding of t

Implementing Information Security based on ISO 27001/ISO 27002 May 12 2022 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

Security Program and Policies Dec 15 2019 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. ¿ 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 ¿

Implementing the ISO/IEC 27001:2013 ISMS Standard Aug 23 2020 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.

The CSSLP Prep Guide Mar 18 2020 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.

ISO27001 / ISO27002 Dec 19 2022 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.

Iso/Iec 27002 Foundation Complete Certification Kit Jun 13 2022 Information security is more important than ever before. Globalization of the economy leads to a growing exchange of information between organizations (their employees, customers and suppliers) and a growing use of networks, such as the internal company network, connection with the networks of other companies and the Internet. Furthermore, activities of many companies now rely on IT, and information has become a valuable asset. Protection of information is crucial for the continuity and proper functioning of the organization: information must be reliable. The international standard, the Code of Practice for Information Security ISO/IEC 27002:2005 structures the organization of information security and tests organizational and managerial aspects of information security. The target audience is people who are professionally involved with the implementation and evaluation of information security and this program is also suitable for small independent businesses for whom some basic knowledge of information security is necessary. In addition this foundation level provides a good starting point for new information security professionals. This certification kit contains both the study guide and access to our online program including presentations, exam preparation modules, the sample exam and forum to interact, that together provides everything you need to prepare for the ISO/IEC 27002 Foundation certification exam. ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains best practices of control objectives and controls in the following areas of information security management: - security policy; - organization of information security; - asset management; - human resources security; - physical and environmental security; - communications and operations management; - access control; - information systems acquisition, development and maintenance; - information security incident management; - business continuity management; - compliance. The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to

meet the requirements identified by a risk assessment. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

IT Governance Jul 14 2022 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.

AWS Certified Solutions Architect Official Study Guide Apr 11 2022 Validate your AWS skills. This is your opportunity to take the next step in your career by expanding and validating your skills on the AWS cloud. AWS has been the frontrunner in cloud computing products and services, and the AWS Certified Solutions Architect Official Study Guide for the Associate exam will get you fully prepared through expert content, and real-world knowledge, key exam essentials, chapter review questions, access to Sybex's interactive online learning environment, and much more. This official study guide, written by AWS experts, covers exam concepts, and provides key review on exam topics, including: Mapping Multi-Tier Architectures to AWS Services, such as web/app servers, firewalls, caches and load balancers Understanding managed RDBMS through AWS RDS (MySQL, Oracle, SQL Server, Postgres, Aurora) Understanding Loose Coupling and Stateless Systems Comparing Different Consistency Models in AWS Services Understanding how AWS CloudFront can make your application more cost efficient, faster and secure Implementing Route tables, Access Control Lists, Firewalls, NAT, and DNS Applying AWS Security Features along with traditional Information and Application Security Using Compute, Networking, Storage, and Database AWS services Architecting Large Scale Distributed Systems Understanding of Elasticity and Scalability Concepts Understanding of Network Technologies Relating to AWS Deploying and Managing Services with tools such as CloudFormation, OpsWorks and Elastic Beanstalk. Learn from the AWS subject-matter experts, review with proven study tools, and apply real-world scenarios. If you are looking to take the AWS Certified Solutions Architect Associate exam, this guide is what you need for comprehensive content and robust study tools that will help you gain the edge on exam day and throughout your career.

The Manager's Guide to Cybersecurity Law Aug 15 2022 In today's litigious business world, cyber-related matters could land you in court. As a computer security professional, you are protecting your data, but are you protecting your company? While you know industry standards and regulations, you may not be a legal expert. Fortunately, in a few hours of reading, rather than months of classroom study, Tari Schreider's The Manager's Guide to Cybersecurity Law: Essentials for Today's Business, lets you integrate legal issues into your security

program. Tari Schreider, a board-certified information security practitioner with a criminal justice administration background, has written a much-needed book that bridges the gap between cybersecurity programs and cybersecurity law. He says, “My nearly 40 years in the fields of cybersecurity, risk management, and disaster recovery have taught me some immutable truths. One of these truths is that failure to consider the law when developing a cybersecurity program results in a protective façade or false sense of security.” In a friendly style, offering real-world business examples from his own experience supported by a wealth of court cases, Schreider covers the range of practical information you will need as you explore – and prepare to apply – cybersecurity law. His practical, easy-to-understand explanations help you to: Understand your legal duty to act reasonably and responsibly to protect assets and information. Identify which cybersecurity laws have the potential to impact your cybersecurity program. Upgrade cybersecurity policies to comply with state, federal, and regulatory statutes. Communicate effectively about cybersecurity law with corporate legal department and counsel. Understand the implications of emerging legislation for your cybersecurity program. Know how to avoid losing a cybersecurity court case on procedure – and develop strategies to handle a dispute out of court. Develop an international view of cybersecurity and data privacy – and international legal frameworks. Schreider takes you beyond security standards and regulatory controls to ensure that your current or future cybersecurity program complies with all laws and legal jurisdictions. Hundreds of citations and references allow you to dig deeper as you explore specific topics relevant to your organization or your studies. This book needs to be required reading before your next discussion with your corporate legal department.

ISO/Iec 27002 Foundation Complete Certification Kit - Study Guide Book and Online Course - Second Edition Jan 08 2022 The first edition of this book and its accompanying eLearning course is regarded as a classic in its field. Now, in an expanded and updated version of The Art of Service's book, the authors once again present a step-by-step guide to getting your ISO/IEC 27002 Foundation Certificate. Information security is more important than ever before. Globalization of the economy leads to a growing exchange of information between organizations (their employees, customers and suppliers) and a growing use of networks, such as the internal company network, connection with the networks of other companies and the Internet. Furthermore, activities of many companies now rely on IT, and information has become a valuable asset. Protection of information is crucial for the continuity and proper functioning of the organization: information must be reliable. The international standard, the Code of Practice for Information Security ISO/IEC 27002:2005 structures the organization of information security and tests organizational and managerial aspects of information security. The target audience is people who are professionally involved with the implementation and evaluation of information security and this program is also suitable for small independent businesses for whom some basic knowledge of information security is necessary. In addition this foundation level provides a good starting point for new information security professionals. This certification kit contains both the study guide and access to our online program including presentations, exam preparation modules, the sample exam and forum to interact, that together provides everything you need to prepare for the ISO/IEC 27002 Foundation certification exam. ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains best practices of control objectives and controls in the following areas of information security management: - security policy; - organisation of information security; - asset management; -

human resources security; - physical and environmental security; - communications and operations management; - access control; - information systems acquisition, development and maintenance; - information security incident management; - business continuity management; - compliance. The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities. Considering the increasing number of IT Professionals and their Organizations who want to be actively involved in Identity and Access Management, this book, which leads to ISO/IEC 27002 Foundation, should do at least as well as the first edition, which is a bestseller.

Information Security Risk Management for ISO27001/ISO27002 Jun 01 2021 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.

CompTIA Security+ Deluxe Study Guide with Online Labs Apr 30 2021 Learn the key objectives and most crucial concepts covered by the Security+ Exam SY0-601 with this comprehensive and practical Deluxe Study Guide Covers 100% of exam objectives including threats, attacks, and vulnerabilities; technologies and tools; architecture and design; identity and access management; risk management; cryptography and PKI, and much more... Includes interactive online learning environment and study tools with: 4 custom practice exams 100 Electronic Flashcards Searchable key term glossary Plus 33 Online Security+ Practice Lab Modules Expert Security+ SY0-601 exam preparation--Now with 33 Online Lab Modules The Fifth edition of CompTIA Security+ Deluxe Study Guide offers invaluable preparation for Exam SY0-601. Written by expert authors, Mike Chapple and David Seidl, the book covers 100% of the exam objectives with clear and concise explanations. Discover how to handle threats, attacks, and vulnerabilities using industry-standard tools and technologies, while gaining and understanding the role of architecture and design. Spanning topics from everyday tasks like identity and access management to complex subjects such as risk management and cryptography, this study guide helps you consolidate your knowledge base in preparation for the Security+ exam. Illustrative examples show how these processes play out in real-world scenarios, allowing you to immediately translate essential concepts to on-the-job application. Coverage of 100% of all exam objectives in this Study Guide means you'll be ready for: Attacks, Threats, and Vulnerabilities Architecture and Design Implementation Operations and Incident Response Governance, Risk, and Compliance Interactive learning environment Take your exam prep to the next level with Sybex's superior interactive online study tools. To access our learning environment, simply visit www.wiley.com/go/sybextestprep, register your book to receive your unique PIN, and instantly gain one year of FREE access after activation to: Interactive test bank with 4 bonus exams. Practice questions help you identify areas where further review is needed. 100 Electronic Flashcards to reinforce learning and last-minute prep before the exam. Comprehensive glossary in PDF format gives you instant access to the key terms so you are fully prepared. ABOUT THE PRACTICE LABS SECURITY+ LABS So you can practice with hands-on learning in a real environment, Sybex has bundled Practice Labs virtual labs that run from your browser. The registration code is included with the book and gives you 6 months unlimited access to Practice Labs CompTIA Security+ Exam SY0-601 Labs with 33 unique lab modules to practice your

skills. If you are unable to register your lab PIN code, please contact Wiley customer support for a replacement PIN code.

Executive's Guide to IT Governance Jan 20 2023 Create strong IT governance processes In the current business climate where a tremendous amount of importance is being given to governance, risk, and compliance (GRC), the concept of IT governance is becoming an increasingly strong component. Executive's Guide to IT Governance explains IT governance, why it is important to general, financial, and IT managers, along with tips for creating a strong governance, risk, and compliance IT systems process. Written by Robert Moeller, an authority in auditing and IT governance Practical, no-nonsense framework for identifying, planning, delivering, and supporting IT services to your business Helps you identify current strengths and weaknesses of your enterprise IT governance processes Explores how to introduce effective IT governance principles with other enterprise GRC initiatives Other titles by Robert Moeller: IT Audit, Control, and Security and Brink's Modern Internal Auditing: A Common Body of Knowledge There is strong pressure on corporations to have a good understanding of their IT systems and the controls that need to be in place to avoid such things as fraud and security violations. Executive's Guide to IT Governance gives you the tools you need to improve systems processes through IT service management, COBIT, and ITIL.

AWS Certified Security Study Guide Apr 18 2020 Get prepared for the AWS Certified Security Specialty certification with this excellent resource By earning the AWS Certified Security Specialty certification, IT professionals can gain valuable recognition as cloud security experts. The AWS Certified Security Study Guide: Specialty (SCS-C01) Exam helps cloud security practitioners prepare for success on the certification exam. It’s also an excellent reference for professionals, covering security best practices and the implementation of security features for clients or employers. Architects and engineers with knowledge of cloud computing architectures will find significant value in this book, which offers guidance on primary security threats and defense principles. Amazon Web Services security controls and tools are explained through real-world scenarios. These examples demonstrate how professionals can design, build, and operate secure cloud environments that run modern applications. The study guide serves as a primary source for those who are ready to apply their skills and seek certification. It addresses how cybersecurity can be improved using the AWS cloud and its native security services. Readers will benefit from detailed coverage of AWS Certified Security Specialty Exam topics. Covers all AWS Certified Security Specialty exam topics Explains AWS cybersecurity techniques and incident response Covers logging and monitoring using the Amazon cloud Examines infrastructure security Describes access management and data protection With a single study resource, you can learn how to enhance security through the automation, troubleshooting, and development integration capabilities available with cloud computing. You will also discover services and tools to develop security plans that work in sync with cloud adoption.

IT Governance Jan 16 2020 Faced with the compliance requirements of increasingly punitive information and privacy-related regulation, as well as the proliferation of complex threats to information security, there is an urgent need for organizations to adopt IT governance best practice. IT Governance is a key international resource for managers in organizations of all sizes and across industries, and deals with the strategic and operational aspects of information security. Now in its seventh edition, the bestselling IT Governance provides guidance for companies looking to protect and enhance their information security management systems (ISMS) and protect themselves against cyber threats. The new edition covers changes in global regulation, particularly GDPR, and updates to standards in the ISO/IEC 27000 family, BS 7799-3:2017 (information security risk management) plus the latest standards on

auditing. It also includes advice on the development and implementation of an ISMS that will meet the ISO 27001 specification and how sector-specific standards can and should be factored in. With information on risk assessments, compliance, equipment and operations security, controls against malware and asset management, IT Governance is the definitive guide to implementing an effective information security management and governance system.

SSCP (ISC)2 Systems Security Certified Practitioner Official Study Guide Oct 13 2019 Fully updated Study Guide for the SSCP This guide prepares you for the SSCP, Systems Security Certified Practitioner certification examination by focusing on the Common Body of Knowledge (CBK) as determined by ISC2 in seven high level topics. This Sybex Study Guide covers 100% of all exam objectives. You'll prepare for the exam smarter and faster with Sybex thanks to expert content, real-world practice, access to the Sybex online interactive learning environment and much more. Reinforce what you've learned with key topic exam essentials and chapter review questions. Along with the book you also get access to Sybex's superior online interactive learning environment that includes: 125 question practice exam to help you identify where you need to study more. Get more than 90 percent of the answers correct, you're ready to take the certification exam. More than 100 Electronic Flashcards to reinforce your learning and give you last minute test prep before the exam A searchable glossary in PDF to give you instant access to the key terms you need to know for the exam Appendix of charts, tables, typical applications, and programs Coverage of all of the exam topics in the book means you'll be ready for: Access Controls Security Operations and Administration Risk Identification, Monitoring and Analysis Incident Response and Recovery Cryptography Network and Communications Security Systems and Application Security

EU General Data Protection Regulation (GDPR) – An implementation and compliance guide, fourth edition Feb 21 2023 Now in its fourth edition, this bestselling guide is the ideal companion for anyone carrying out a GDPR (General Data Protection Regulation) compliance project. It provides comprehensive guidance and practical advice on complying with the Regulation.

Guide to Security Assurance for Cloud Computing May 20 2020 This practical and didactic text/reference discusses the leading edge of secure cloud computing, exploring the essential concepts and principles, tools, techniques and deployment models in this field. Enlightening perspectives are presented by an international collection of pre-eminent authorities in cloud security assurance from both academia and industry. Topics and features: · Describes the important general concepts and principles of security assurance in cloud-based environments · Presents applications and approaches to cloud security that illustrate the current state of the art · Reviews pertinent issues in relation to challenges that prevent organizations moving to cloud architectures · Provides relevant theoretical frameworks and the latest empirical research findings · Discusses real-world vulnerabilities of cloud-based software in order to address the challenges of securing distributed software · Highlights the practicalities of cloud security, and how applications can assure and comply with legislation · Includes review questions at the end of each chapter This Guide to Security Assurance for Cloud Computing will be of great benefit to a broad audience covering enterprise architects, business analysts and leaders, IT infrastructure managers, cloud security engineers and consultants, and application developers involved in system design and implementation. The work is also suitable as a textbook for university instructors, with the outline for a possible course structure suggested in the preface. The editors are all members of the Computing and Mathematics Department at the University of Derby, UK, where Dr. Shao Ying Zhu serves as a Senior Lecturer in Computing, Dr. Richard Hill as a Professor and Head of the Computing and Mathematics Department, and Dr. Marcello Trovati as a Senior Lecturer in

Mathematics. The other publications of the editors include the Springer titles Big-Data Analytics and Cloud Computing, Guide to Cloud Computing and Cloud Computing for Enterprise Architectures.

HCISPP Study Guide Dec 27 2020 The HCISPP certification is a globally-recognized, vendor-neutral exam for healthcare information security and privacy professionals, created and administered by ISC2. The new HCISPP certification, focused on health care information security and privacy, is similar to the CISSP, but has only six domains and is narrowly targeted to the special demands of health care information security. Tim Virtue and Justin Rainey have created the HCISPP Study Guide to walk you through all the material covered in the exam's Common Body of Knowledge. The six domains are covered completely and as concisely as possible with an eye to acing the exam. Each of the six domains has its own chapter that includes material to aid the test-taker in passing the exam, as well as a chapter devoted entirely to test-taking skills, sample exam questions, and everything you need to schedule a test and get certified. Put yourself on the forefront of health care information privacy and security with the HCISPP Study Guide and this valuable certification. Provides the most complete and effective study guide to prepare you for passing the HCISPP exam - contains only what you need to pass the test, and no fluff! Completely aligned with the six Common Body of Knowledge domains on the exam, walking you step by step through understanding each domain and successfully answering the exam questions. Optimize your study guide with this straightforward approach - understand the key objectives and the way test questions are structured.

CASP+ CompTIA Advanced Security Practitioner Study Guide Jun 20 2020 Prepare to succeed in your new cybersecurity career with the challenging and sought-after CASP+ credential In the newly updated Fourth Edition of CASP+ CompTIA Advanced Security Practitioner Study Guide Exam CAS-004, risk management and compliance expert Jeff Parker walks you through critical security topics and hands-on labs designed to prepare you for the new CompTIA Advanced Security Professional exam and a career in cybersecurity implementation. Content and chapter structure of this Fourth edition was developed and restructured to represent the CAS-004 Exam Objectives. From operations and architecture concepts, techniques and requirements to risk analysis, mobile and small-form factor device security, secure cloud integration, and cryptography, you'll learn the cybersecurity technical skills you'll need to succeed on the new CAS-004 exam, impress interviewers during your job search, and excel in your new career in cybersecurity implementation. This comprehensive book offers: Efficient preparation for a challenging and rewarding career in implementing specific solutions within cybersecurity policies and frameworks A robust grounding in the technical skills you'll need to impress during cybersecurity interviews Content delivered through scenarios, a strong focus of the CAS-004 Exam Access to an interactive online test bank and study tools, including bonus practice exam questions, electronic flashcards, and a searchable glossary of key terms Perfect for anyone preparing for the CASP+ (CAS-004) exam and a new career in cybersecurity, CASP+ CompTIA Advanced Security Practitioner Study Guide Exam CAS-004 is also an ideal resource for current IT professionals wanting to promote their cybersecurity skills or prepare for a career transition into enterprise cybersecurity.

CompTIA Security+ Review Guide Sep 04 2021 Learn the ins and outs of the IT security field and efficiently prepare for the CompTIA Security+ Exam SY0-601 with one easy-to-follow resource CompTIA Security+ Review Guide: Exam SY0-601, Fifth Edition helps you to efficiently review for the leading IT security certification—CompTIA Security+ SY0-601. Accomplished author and security expert James Michael Stewart covers each domain in a straightforward and practical way, ensuring that you grasp and understand the objectives as quickly as possible. Whether you're refreshing your knowledge or doing a last-

minute review right before taking the exam, this guide includes access to a companion online test bank that offers hundreds of practice questions, flashcards, and glossary terms. Covering all five domains tested by Exam SY0-601, this guide reviews: Attacks, Threats, and Vulnerabilities Architecture and Design Implementation Operations and Incident Response Governance, Risk, and Compliance This newly updated Fifth Edition of CompTIA Security+ Review Guide: Exam SY0-601 is not just perfect for anyone hoping to take the SY0-601 Exam, but it is also an excellent resource for those wondering about entering the IT security field.

PCI DSS: A Pocket Guide, fifth edition Aug 03 2021 An ideal introduction and a quick reference to PCI DSS version 3.2 All businesses that accept payment cards are prey for hackers and criminal gangs trying to steal financial information and commit identity fraud. The PCI DSS (Payment Card Industry Data Security Standard) exists to ensure that businesses process credit and debit card orders in a way that effectively protects cardholder data. All organisations that accept, store, transmit or process cardholder data must comply with the Standard; failure to do so can have serious consequences for their ability to process card payments. Product overview Co-written by a PCI QSA (Qualified Security Assessor) and updated to cover PCI DSS version 3.2, this handy pocket guide provides all the information you need to consider as you approach the PCI DSS. It is also an ideal training resource for anyone in your organisation involved with payment card processing. Coverage includes: An overview of PCI DSS v3.2.A PCI self-assessment questionnaire (SAQ).Procedures and qualifications.An overview of the Payment Application Data Security Standard (PA-DSS).About the authors Alan Calder is the founder and executive chairman of IT Governance Ltd, an information, advice and consultancy firm that helps company boards tackle IT governance, risk management, compliance and information security issues. He has many years of senior management experience in the private and public sectors. Geraint Williams is a knowledgeable and experienced senior information security consultant and PCI QSA, with a strong technical background and experience of the PCI DSS and security testing. He leads the IT Governance CISSP Accelerated Training Programme, as well as the PCI Foundation and Implementer training courses. He has broad technical knowledge of security and IT infrastructure, including high performance computing and Cloud computing. His certifications include CISSP, PCI QSA, CREST Registered Tester, CEH and CHFI.

Network and Information Systems (NIS) Regulations - A pocket guide for operators of essential services Mar 10 2022 This pocket guide is a primer for any OES (operators of essential services) that needs to comply with the NIS Regulations, and explores who they are, and why the NIS Regulations are different for them.

Information Security based on ISO 27001/ISO 27002 Nov 18 2022 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.

Iso27001/Iso27002 a Pocket Guide Nov 25 2020 This helpful, handy ISO27001/ISO27002 pocket guide gives a useful overview

of these two important information security standards.
Official (ISC)2® Guide to the ISSMP® CBK® Jul 22 2020 As the recognized leader in the field of information security education and certification, the (ISC)2 promotes the development of information security professionals around the world. The Certified Information Systems Security Professional-Information Systems Security Management Professional (CISSP-ISSMP) examination assesses individuals understa
Network and Information Systems (NIS) Regulations - A pocket guide for digital service providers Nov 06 2021 This pocket guide is a primer for any DSPs (digital service providers) that needs to comply with the NIS Regulations, and explores who they are, and why the NIS Regulations are different for them.
CISSP Study Guide Feb 15 2020 The CISSP certification is the most prestigious, globally-recognized, vendor neutral exam for information security professionals. The newest edition of this acclaimed study guide is aligned to cover all of the material included in the newest version of the exam's Common Body of Knowledge. The ten domains are covered completely and as concisely as possible with an eye to acing the exam. Each of the ten domains has its own chapter that includes specially designed pedagogy to aid the test-taker in passing the exam, including: Clearly stated exam objectives; Unique terms/Definitions; Exam Warnings; Learning by Example; Hands-On Exercises; Chapter ending questions. Furthermore, special features include: Two practice exams; Tiered chapter ending questions that allow for a gradual learning curve; and a self-test appendix Provides the most complete and effective study guide to prepare you for passing the CISSP exam—contains only what you need to pass the test, with no fluff! Eric Conrad has prepared hundreds of professionals for passing the CISSP exam through SANS, a popular and well-known organization for information security professionals Covers all of the new information in the Common Body of Knowledge updated in January 2012, and also provides two practice exams, tiered end-of-chapter questions for a gradual learning curve, and a complete self-test appendix
A concise introduction to the NIS Directive - A pocket guide for digital service providers Feb 09 2022 This pocket guide is an introduction to the EU's NIS Directive (Directive on security of network and information systems). It outlines the key requirements, details which digital service providers are within scope, and explains how the security objectives from ENISA's Technical Guidelines and international standards can help DSPs achieve compliance.
ISO 27001 Controls Mar 30 2021 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.
US National Cyber Security Strategy and Programs Handbook Volume 1 Strategic Information and Developments Oct 25 2020 US National Cyber Security Strategy and Programs Handbook - Strategic Information and Developments