Information Security Management Principles Bcs

IT Capability Maturity FrameworkTM (IT-CMFTM) 2nd edition
Managing Technology for Business Value
Information Security Management Principles: Information security principles; 2. Information risk; 3. Information security framework; 4. Procedural and people security controls; 5. Technical security controls; 6. Software development and life cycle; 7. Physical and environmental security; 8. Disaster recovery and business continuity management; 9. Other technical aspects
Cyber Security Management
Information Security Management Principles
Once more unto the Breach
GDPR and Cyber Security for Business Information Systems
Which One Is Nettie?
Safety and Security of Cyber-Physical Systems
IT Governance
ITIL® 4 Foundation Courseware - Deutsch
Information Security and Employee Behaviour
The Secure Online Business Handbook
Cyber Security
Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications
Delivering Superior Health and Wellness Management with IoT and Analytics
ECCWS 2023 22nd European Conference on Cyber Warfare and Security
IT Capability Maturity Framework™ (IT-CMF™) 2nd edition
The World Beyond Digital Rights Management
Critical Information Infrastructure Protection and Resilience in the ICT Sector
Cyber Security
Business Information Systems
Navigating Through the Crisis: Business, Technological and Ethical Considerations
Practical Information Security Management
Information Risk Management
Information Security Management Principles
Fourth International Congress on Information and Communication Technology
Essential Information Security
Cyber Security Practitioner's Guide
Information Security Handbook
DIGITAL FINANCE
Strategic Cyber Security Management
Information Security Management Principles
Securing Information and Communications Systems
International Standards for Design and Manufacturing
Cybersecurity Education for Awareness and Compliance
Handbook of Information Security Management

HEATH COLLINS

IT Capability Maturity FrameworkTM (IT-CMFTM) 2nd edition BCS, The Chartered Institute
This one-stop reference gives you the latest expertise on everything from access control and network security, to smart cards and privacy. Representing a total blueprint to security design and operations, this book brings all modern considerations into focus. It maps out user authentication methods that feature the latest biometric techniques, followed by authorization and access controls including DAC, MAC, and ABAC and how these controls are best applied in todayOCOs relational and multilevel secure database systems."
Managing Technology for Business Value IGI Global
Cyber Security Management: A Governance, Risk and Compliance Framework by Peter Trim and Yang-Im Lee has been written for a wide audience. Derived from research, it places security management in a holistic context and outlines how the strategic marketing approach can be used to underpin cyber security in partnership arrangements. The book is unique because it integrates material that is of a highly specialized nature but which can be interpreted by those with a non-specialist background in the area. Indeed, those with a limited knowledge of cyber security will be able to develop a comprehensive understanding of the subject and will be guided into devising and implementing relevant policy, systems and procedures that make the organization better able to withstand the increasingly sophisticated forms of cyber attack. The book includes a sequence-of-events model; an organizational governance framework; a business continuity management planning framework; a multi-cultural communication model; a cyber security management model and strategic management framework; an integrated governance mechanism; an integrated resilience management model; an integrated management model and system; a communication risk management strategy; and recommendations for counteracting a range of cyber threats. Cyber Security Management: A Governance, Risk and Compliance Framework simplifies complex material and provides a multi-disciplinary perspective and an explanation and interpretation of how managers can manage cyber threats in a pro-active manner and work towards counteracting cyber threats both now and in the future.
Information Security Management Principles: Information security principles; 2. Information risk; 3. Information security framework; 4. Procedural and people security controls; 5. Technical security controls; 6. Software development and life cycle; 7. Physical and environmental security; 8. Disaster recovery and business continuity management; 9. Other technical aspects Springer Nature
This handbook provides a comprehensive collection of knowledge for emerging multidisciplinary research areas such as cybersecurity, IoT, Blockchain, Machine Learning, Data Science, and AI. This book brings together, in one resource, information security across multiple domains. Information Security Handbook addresses the knowledge for emerging multidisciplinary research. It explores basic and high-level concepts and serves as a manual for industry while also helping beginners to understand both basic and advanced aspects in security-related issues. The handbook explores security and privacy issues through the IoT ecosystem and implications to the real world and, at the same time, explains the concepts of IoT-related technologies, trends, and future directions. University graduates and postgraduates, as well as research scholars, developers, and end-users, will find this handbook very useful.
Cyber Security Management Cambridge Scholars Publishing
Through the rise of big data and the internet of things, terrorist organizations have been freed from geographic and logistical confines and now have more power than ever before to strike the average citizen directly at home. This, coupled with the inherently asymmetrical nature of cyberwarfare, which grants great advantage to the attacker, has created an unprecedented national security risk that both governments and their citizens are woefully ill-prepared to face. Examining cyber warfare and terrorism through a critical and academic perspective can lead to a better understanding of its foundations and implications. Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications is an essential reference for the latest research on the utilization of online tools by terrorist organizations to communicate with and recruit potential extremists and examines effective countermeasures employed by law enforcement agencies to defend against such threats. Highlighting a range of topics such as cyber threats, digital intelligence, and counterterrorism, this multi-volume book is ideally designed for law enforcement, government officials, lawmakers, security analysts, IT specialists, software developers, intelligence and security practitioners, students, educators, and researchers.
Information Security Management Principles Academic Conferences and publishing limited
The role of the information security manager has changed. Have you? The challenges you face as an information security manager (ISM) have increased enormously since the first edition of Once more unto the breach was published. What seemed exceptional in 2011 is the norm in 2015: vulnerabilities have been experienced across all operating systems, millions of individuals have been affected by data breaches, and countless well-known companies have fallen victim to cyber attacks. It’s your duty to ensure that your organisation isn’t next. The ISM’s information security responsibilities now cover all aspects of the organisation and its operations, and relate to the security of information in all forms, locations and transactions across the organisation – and beyond. Topics covered include: Project managementPhysical securityPassword managementConsumerisation (BYOD)Audit log managementVulnerability managementCloud computingIncident reportingPenetration testingLinking information security with records managementPrivacy impact assessmentsInternal auditing In this revised edition of Once more unto the breach, Andrea C Simmons uses her extensive experience to provide an important insight into the changing role and responsibilities of the ISM, walking you through a typical ISM’s year and highlighting the challenges and pitfalls of an information security programme. One of the key failures of security change management is that it is perceived as a project instead of a programme ,

and is therefore mistakenly assumed to have an end. Once more unto the breachexplains why information security is an ongoing process, using the role of project manager on a programme of change to highlight the various incidents and issues that arise on an almost daily basis – and often go unnoticed. A major challenge for the ISM is achieving all-important buy-in from their colleagues. Once more unto the breach explains how to express the importance of the tasks you are undertaking in language that executive management will understand. You'll also discover the importance of having a camera with you at all times. For too long, security has been seen as more of an inhibitor than an enabler. Once more unto the breach is an invaluable resource that will help you improve this perception, and achieve better overall information protection results as a result. About the author Andrea C Simmons is an information governance specialist with extensive experience in the private and public sectors. She has made significant contributions to the development of standards and industry research, and is currently working on a PhD in information assurance. She writes articles and blogs, and presents at conferences, seminars and workshops. Andrea is a member of many professional bodies and has just been awarded Senior Member status by the Information Systems Security Association (ISSA). Buy this book and understand the latest challenges information security managers face.

Once more unto the Breach Pearson Education

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

GDPR and Cyber Security for Business Information Systems BCS, The Chartered Institute for IT

Research suggests that between 60-75% of all information security incidents are the result of a lack of knowledge and/or understanding amongst an organization's own staff. And yet the great majority of money spent protecting systems is focused on creating technical defences against external threats. Angus McIlwraith's book explains how corporate culture affects perceptions of risk and information security, and how this in turn affects employee behaviour. He then provides a pragmatic approach for educating and training employees in information security and explains how different metrics can be used to assess awareness and behaviour. Information security awareness will always be an ongoing struggle against complacency, problems associated with new systems and technology, and the challenge of other more glamorous and often short term priorities. Information Security and Employee Behaviour will help you develop the capability and culture that will enable your organization to avoid or reduce the impact of unwanted security breaches.

Which One Is Nettie? Apress

With the progression of technological breakthroughs creating dependencies on telecommunications, the internet, and social networks connecting our society, CIIP (Critical Information Infrastructure Protection) has gained significant focus in order to avoid cyber attacks, cyber hazards, and a general breakdown of services. Critical Information Infrastructure Protection and Resilience in the ICT Sector brings together a variety of empirical research on the resilience in the ICT sector and critical information infrastructure protection in the context of uncertainty and lack of data about potential threats and hazards. This book presents a variety of perspectives on computer science, economy, risk analysis, and social sciences; beneficial to academia, governments, and other organisations engaged or interested in CIIP, Resilience and Emergency Preparedness in the ICT sector.

Safety and Security of Cyber-Physical Systems CRC Press

Content owners and commercial stakeholders face a constant battle to protect their intellectual property and commercial rights. Umeh outlines the issues behind this battle, current solutions to the problem, and looks to a future beyond digital rights management.

IT Governance IGI Global

A lot of companies have fallen prey to data breaches involving customers' credit and debit accounts. Private businesses also are affected and are victims of cybercrime. All sectors including governments, healthcare, finance, enforcement, academia etc. need information security professionals who can safeguard their data and knowledge. But the current state is that there's a critical shortage of qualified cyber security and knowledge security professionals. That is why we created this book to offer all of you a summary of the growing field of cyber and information security along with the various opportunities which will be available to you with professional cyber security degrees. This book may be a quick read; crammed with plenty of information about industry trends, career paths and certifications to advance your career. We all hope you'll find this book helpful as you begin your career and develop new skills in the cyber security field. "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the nation's critical infrastructure in the face of such threats." -Presidential Executive Order, 2013 (Improving Critical Infrastructure Cybersecurity)

ITIL® 4 Foundation Courseware - Deutsch Kogan Page Publishers

In an era of unprecedented volatile political and economic environments across the world, computer-

based cyber security systems face ever growing challenges. While the internet has created a global platform for the exchange of ideas, goods and services, it has also created boundless opportunities for cyber crime. The debate over how to plan for the cyber security of the future has focused the minds of developers and scientists alike. This book aims to provide a reference on current and emerging issues on systems security from the lens of autonomy, artificial intelligence and ethics as the race to fight and prevent cyber crime becomes increasingly pressing.

Information Security and Employee Behaviour Cendikia Mulia Mandiri

This textbook places cyber security management within an organizational and strategic framework, enabling students to develop their knowledge and skills for a future career. The reader will learn to: • evaluate different types of cyber risk • carry out a threat analysis and place cyber threats in order of severity • formulate appropriate cyber security management policy • establish an organization-specific intelligence framework and security culture • devise and implement a cyber security awareness programme • integrate cyber security within an organization's operating system Learning objectives, chapter summaries and further reading in each chapter provide structure and routes to further in-depth research. Firm theoretical grounding is coupled with short problem-based case studies reflecting a range of organizations and perspectives, illustrating how the theory translates to practice, with each case study followed by a set of questions to encourage understanding and analysis. Non-technical and comprehensive, this textbook shows final year undergraduate students and postgraduate students of Cyber Security Management, as well as reflective practitioners, how to adopt a pro-active approach to the management of cyber security. Online resources include PowerPoint slides, an instructor's manual and a test bank of questions.

The Secure Online Business Handbook IGI Global

This proceedings volume provides a multifaceted perspective on the unprecedented crises generated by the global COVID-19 pandemic, and its ramifications for individuals, businesses, organizations, governments and systems in developing countries. Featuring selected papers from the 2020 Annual Griffiths School of Management and IT Conference (GSMAC), held in Oradea, Romania, this volume focuses on business, technological and ethical considerations in the process of navigating through a global crisis. It analyzes the effectiveness of different measures taken at individual, organizational and country level and outlines potential scenarios and solutions for the new post-crisis reality. Finally, the book provides diagnosis and recommendations for managerial practice in various industries impacted.

Van Haren

Mempelajari digital finance memberi kesempatan untuk menggabungkan pengetahuan keuangan dengan teknologi modern. Ini akan memberi keunggulan kompetitif dalam dunia keuangan yang terus berkembang. Digital finance telah mengubah cara bisnis beroperasi dan berinteraksi dengan pelanggan serta mitra bisnis. Dengan memahami dan menerapkan prinsip-prinsip digital finance, bisnis dapat mengoptimalkan efisiensi, meningkatkan aksesibilitas keuangan, dan meraih keunggulan kompetitif dalam lingkungan bisnis yang semakin digital.

Cyber Security IGI Global

Information Security Management PrinciplesBCS, The Chartered Institute for IT

Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications Van Haren

This book provides a first introduction into the field of Information security. Information security is about preserving your data, keeping private data private, making sure only the people who are authorized have access to the data, making sure your data is always there, always the way you left it, keeping your secrets secret, making sure you trust your sources, and comply with government and industry regulations and standards. It is about managing your risks and keeping the business going when it all goes south. Every new security practitioner should start with this book, which covers the most relevant topics like cloud security, mobile device security and network security and provides a comprehensive overview of what is important in information security. Processes, training strategy, policies, contingency plans, risk management and effectiveness of tools are all extensively discussed.

Delivering Superior Health and Wellness Management with IoT and Analytics Bloomsbury Publishing USA

Extensive advertising and review coverage in the leading business and IT media, and direct mail campaigns targeting IT professionals, libraries, corporate customers and approximately 70,000 BCS members.

ECCWS 2023 22nd European Conference on Cyber Warfare and Security BCS, The Chartered Institute for IT

Besides the ITIL® 4 Foundation Courseware - English (ISBN: 978 94 018 0394 6) publication you are advised to obtain the publication ITIL® 4 - A Pocket Guide (ISBN: 978 94 018 0439 4). The course is designed as an introduction to ITIL 4 and enables you to understand a new way to look at IT Service Management through a Service Value System (SVS). ITIL 4 provides an end-to-end picture of what means to contribute to business value, and also integrates concepts from models such as Lean IT, Agile and DevOps. This course is for those who are involved in the delivery of IT services and need an understanding of best practice in IT Service Management. Student must pass a 60 minute, 40 question closed book multiple choice, examination with a passing score of 65% in order to receive this certification. You can write the exam at any time and at any place after the course. The test is done via your own computer proctored via webcam. Candidates wishing to be trained and pass the exam for this qualification would be recommended to have a general awareness of IT and appreciation of their own business environment. You'll learn: Understand the key concepts of service management Understand how the ITIL guiding principles can help an organization adopt and adapt service management Understand the four dimensions of service management Understand the purpose and components of the ITIL service value system Understand the activities of the service value chain, and how they interconnect Know the purpose and key terms of 18 ITIL practices Understand 7 ITIL practices

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

International standards ensure that organisations operate the right processes to support their objectives. International Standards for Design and Manufacturing is an accessible guide for manufacturing and production managers and students. It guides readers through the standards needed to build operating systems which are robust, integrated and used to drive the continuous improvement of business performance. International Standards for Design and Manufacturing is

based on many years of research collaboration between Swansea University and leading manufacturing and production practitioners from key companies from around the world. Each chapter includes an introduction to the standards being discussed, definitions, examples of using the standards in practice, why these standards are important, conclusions, seminar topics and mock exam questions to allow the reader to test their knowledge and understanding.

The World Beyond Digital Rights Management CRC Press

This book constitutes the refereed post-conference proceedings of the Second International Workshop on Information & Operational Technology (IT & OT) security systems, IOSec 2019 , the First International Workshop on Model-driven Simulation and Training Environments, MSTEC 2019, and the First International Workshop on Security for Financial Critical Infrastructures and Services, FINSEC 2019, held in Luxembourg City, Luxembourg, in September 2019, in conjunction with the 24th European Symposium on Research in Computer Security, ESORICS 2019. The IOSec Workshop received 17 submissions from which 7 full papers were selected for presentation. They cover topics related to security architectures and frameworks for enterprises, SMEs, public administration or critical infrastructures, threat models for IT & OT systems and communication networks, cyber-threat detection, classification and pro ling, incident management, security training and awareness, risk assessment safety and security, hardware security, cryptographic engineering, secure software development, malicious code analysis as well as security testing platforms. From the MSTEC Workshop 7 full papers out of 15 submissions are included. The selected papers deal focus on the verification and validation (V&V) process, which provides the operational community with confidence in knowing that cyber models represent the real world, and discuss how defense training may benefit from cyber models. The FINSEC Workshop received 8 submissions from which 3 full papers and 1 short paper were accepted for publication. The papers reflect the objective to rethink cyber-security in the light of latest technology developments (e.g., FinTech, cloud computing, blockchain, BigData, AI, Internet-of-Things (IoT), mobile-first services, mobile payments).