Iso Iec 27034 1 2011 Information Technology Security

Exploring Security in Software Architecture and Design
Global Standards and Publications
Sicherheit von Webanwendungen in der Praxis
Information Security Technology - Controllability Evaluation Index for Security of Information Technology Products - Part 1: General Principles [After payment, write to & get a FREE-of-charge, unprotected true-PDF from: Sales@ChineseStandard.net]
Highlights of the Information Security Solutions Europe 2014 Conference
Trilhas em Segurança da Informação
Surviving Cyberattacks
Robots, Drones, UAVs and UGVs for Operation and Maintenance
Wie sich Unternehmen schützen können – Hintergründe, Maßnahmen, Prüfverfahren und Prozesse
CISSP Cert Guide
Market, Functional and Conceptual View based on SAP S/4HANA
Governance of Enterprise IT based on COBIT 5
Cyber Security Engineering
Compendium on Enterprise Resource Planning
Research Anthology on Privatizing and Securing Data
IT-Sicherheit mit System
Information Technology-Security Techniques-Application Security
Foundations of Information Security Based on ISO27001 and ISO27002 - 3rd revised edition
Zintegrowany system zarządzania unieszkodliwianiem azbestu w ujęciu systemowym
Security at the Source
Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia
Aus- und Weiterbildung zum ISTQB® Advanced Level Specialist – Certified Security Tester
GB/T 36630.1-2018: Translated English of Chinese Standard. (GBT 36630.1-2018, GB/T36630.1-2018, GBT36630.1-2018)
Caminhos e ideias para a proteção de dados
System informatyczny GeoAzbest. Zintegrowany system zarządzania unieszkodliwianiem azbestu w ujęciu systemowym

Principles of Information Security
CISSP Cert Guide, 3/e_c3
18th International Conference, Melbourne, VIC, Australia, July 2-5, 2018, Proceedings, Part II
Practical Technology and Use Cases of Enterprise Blockchain for the Real World
Handbuch für Praktiker und Begleitbuch zum T.I.S.P.
Systems, Software and Services Process Improvement
CompTIA Advanced Secur_o2
ISO 27001 Bilgi Güvenliği Yönetim Sistemi ve ISO 27002 Uygulama Kılavuzu
Blockchain Applied
Who Owns the New Oil?
An International Perspective
Global Standards and Publications
Data Protection and Privacy: (In)visibilities and Infrastructures
Basiswissen Sicherheitstests

DEANDRE BRIGGS

Exploring Security in Software Architecture and Design Springer Nature
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.

Global Standards and Publications Bogdan Wit

Cyber-attacks continue to rise as more individuals rely on storing personal information on networks. Even though these networks are continuously checked and secured, cybercriminals find new strategies to break through these protections. Thus, advanced security systems, rather than simple security patches, need to be designed and developed. Exploring Security in Software Architecture and Design is an essential reference source that discusses the development of security-aware software systems that are built into every phase of the software architecture. Featuring research on topics such as migration techniques, service-based software, and building security, this book is ideally designed for computer and software engineers, ICT specialists, researchers, academicians, and field experts.

Sicherheit von Webanwendungen in der Praxis Springer

With the immense amount of data that is now available online, security concerns have been an issue from the start, and have grown as new technologies are increasingly integrated in data collection, storage, and transmission. Online cyber threats, cyber terrorism, hacking, and other cybercrimes have begun to take advantage of this information that can be easily accessed if not properly handled. New privacy and security measures have been developed to address this cause for concern and have become an essential area of research within the past few years and into the foreseeable future. The ways in which data is secured and privatized should be discussed in terms of the technologies being used, the methods and models for security that have been developed, and the ways in which risks can be detected, analyzed, and mitigated. The Research Anthology on Privatizing and Securing Data reveals the latest tools and technologies for privatizing and securing data across different technologies and industries. It takes a deeper dive into both risk detection and mitigation, including an analysis of cybercrimes and cyber threats, along with a sharper focus on the technologies and methods being actively implemented and utilized to secure data online. Highlighted topics include information governance and privacy, cybersecurity, data protection, challenges in big data, security threats, and more. This book is essential for data analysts, cybersecurity professionals, data scientists, security analysts, IT specialists,

practitioners, researchers, academicians, and students interested in the latest trends and technologies for privatizing and securing data.
Information Security Technology - Controllability Evaluation Index for Security of Information Technology Products - Part 1: General Principles [After payment, write to & get a FREE-of-charge, unprotected true-PDF from: Sales@ChineseStandard.net] CRC Press
Die Effizienz, Existenz und Zukunft eines Unternehmens sind maßgeblich abhängig von der Sicherheit und Kontinuität sowie den Risiken der Informationsverarbeitung. Die dreidimensionale IT-Sicherheitsmanagementpyramide V sowie die innovative und integrative IT-RiSiKo-Managementpyramide V liefern ein durchgängiges, praxisorientiertes und geschäftszentriertes Vorgehensmodell für den Aufbau und die Weiterentwicklung des IT-Sicherheits-, Kontinuitäts- und Risikomanagements. Mit diesem Buch identifizieren Sie Risiken, bauen wegweisendes effizienzförderndes Handlungswissen auf. Sie richten Ihre IT sowie deren Prozesse, Ressourcen und die Organisation systematisch und effektiv auf Sicherheit aus und integrieren Sicherheit in den IT-Lebenszyklus. Der Autor führt Sie von der Politik bis zu Konzepten und Maßnahmen. Beispiele und Checklisten unterstützen Sie. Der Online-Service des Autors bietet Ihnen zusätzliche News, Links und ergänzende Beiträge.
Highlights of the Information Security Solutions Europe 2014 Conference
Pearson IT Certification
Das Grundlagenwerk strukturiert das Basiswissen der Informationssicherheit in 27 aufeinander aufbauenden Kapiteln. - Aktualisierte und erweiterte Auflage Die Neuauflage des Standardwerks wurde um das Kapitel "Sicherheit von mobilen Endgeräten" erweitert. Die Kapitel zu rechtlichen Aspekten, IT-Grundschutz, Sicherheit in mobilen Netzen und zu Malware wurden grundlegend überarbeitet. Alle anderen Themengebiete wurden auf den aktuellen Stand gebracht. - Von Praktikern für Praktiker "Informationssicherheit und Datenschutz" stammt aus der Feder von Praktikern – alle mitwirkenden Autoren sind Security Consultants bei Secorvo in Karlsruhe mit gemeinsam über 280 Jahren Berufserfahrung in der Informationssicherheit und im Datenschutz. - Begleitbuch zum T.I.S.P. Der Band eignet sich auch als Begleitbuch zur T.I.S.P.-Schulung, die mit dem Zertifikat "TeleTrusT Information Security Professional" abgeschlossen werden kann. Er deckt nicht nur alle prüfungsrelevanten Inhalte ab, sondern lehnt sich auch an die Struktur der T.I.S.P.-Schulung an. Autoren André Domnick, Fabian Ebner, Dirk Fox, Stefan Gora, Volker Hammer, Kai Jendrian, Michael Knöppler, Hans-Joachim Knobloch, Michael Knopp, Sarah Niederer, Jannis Pinter, Friederike Schellhas-Mende, Jochen Schlichting, Jörg Völker Inhalt Aufgaben und Ziele Betriebswirtschaftliche Aspekte Rechtliche Aspekte Hackermethoden ISO 27001 und 27002 IT-Grundschutz Sicherheitskonzept Physische Sicherheit Netzwerksicherheit Firewalls Kryptografie Vertrauensmodelle und PKI VPN Sicherheit in mobilen Netzen Authentifizierung und Berechtigungsmanagement Betriebssystemsicherheit Windows-Sicherheit Unix-Sicherheit Sicherheit von mobilen Endgeräten Web Security und Anwendungssicherheit Löschen und Entsorgen Awareness Malware und Content Security Intrusion Detection

Datensicherung Incident-Management und CERT Business-Continuity-Management

Trilhas em Segurança da Informação CRC Press

Monografia dotycząca bezpieczeństwa informacji w urzędach administracji terenowej podsumowująca wyniki badań z lat 2012-2016

Surviving Cyberattacks Springer

This book presents the most interesting talks given at ISSE 2014 – the forum for the inter-disciplinary discussion of how to adequately secure electronic business processes. The reader may expect state-of-the-art: best papers of the Conference ISSE 2014.

Robots, Drones, UAVs and UGVs for Operation and Maintenance Addison-Wesley Professional

Software development continues to be an ever-evolving field as organizations require new and innovative programs that can be implemented to make processes more efficient, productive, and cost-effective. Agile practices particularly have shown great benefits for improving the effectiveness of software development and its maintenance due to their ability to adapt to change. It is integral to remain up to date with the most emerging tactics and techniques involved in the development of new and innovative software. The Research Anthology on Agile Software, Software Development, and Testing is a comprehensive resource on the emerging trends of software development and testing. This text discusses the newest developments in agile software and its usage spanning multiple industries. Featuring a collection of insights from diverse authors, this research anthology offers international perspectives on agile software. Covering topics such as global software engineering, knowledge management, and product development, this comprehensive resource is valuable to software developers, software engineers, computer engineers, IT directors, students, managers, faculty, researchers, and academicians.

Wie sich Unternehmen schützen können – Hintergründe, Maßnahmen, Prüfverfahren und Prozesse

International Standard ISO/IEC 27034-1:2011/Cor.1:2014Information Technology-Security Techniques-Application SecurityBusiness Continuity in a Cyber WorldSurviving Cyberattacks

This volume constitutes the refereed proceedings of the 24th EuroSPI conference, held in Ostrava, Czech Republic, in September 2017.The 56 revised full papers presented were carefully reviewed and selected from 97 submissions. They are organized in topical sections on SPI and VSEs, SPI and process models, SPI and safety, SPI and project management, SPI and implementation, SPI issues, SPI and automotive, selected key notes and workshop papers, GamifySPI, SPI in Industry 4.0, best practices in implementing traceability, good and bad practices in improvement, safety and security, experiences with agile and lean, standards and assessment models, team skills and diversity strategies.

CISSP Cert Guide CRC Press

Cyber Security Engineering is the definitive modern reference and tutorial on the full range of capabilities associated with modern cyber security engineering. Pioneering software assurance experts Dr. Nancy R. Mead and Dr. Carol C. Woody bring together comprehensive best practices for building software systems that exhibit superior operational security,

and for considering security throughout your full system development and acquisition lifecycles. Drawing on their pioneering work at the Software Engineering Institute (SEI) and Carnegie Mellon University, Mead and Woody introduce seven core principles of software assurance, and show how to apply them coherently and systematically. Using these principles, they help you prioritize the wide range of possible security actions available to you, and justify the required investments. Cyber Security Engineering guides you through risk analysis, planning to manage secure software development, building organizational models, identifying required and missing competencies, and defining and structuring metrics. Mead and Woody address important topics, including the use of standards, engineering security requirements for acquiring COTS software, applying DevOps, analyzing malware to anticipate future vulnerabilities, and planning ongoing improvements. This book will be valuable to wide audiences of practitioners and managers with responsibility for systems, software, or quality engineering, reliability, security, acquisition, or operations. Whatever your role, it can help you reduce operational problems, eliminate excessive patching, and deliver software that is more resilient and secure.

Market, Functional and Conceptual View based on SAP S/4HANA

https://www.chinesestandard.net

Die Sicherheit von IT-Systemen ist heute eine der wichtigsten Qualitätseigenschaften. Wie für andere Eigenschaften gilt auch hier das Ziel, fortwährend sicherzustellen, dass ein IT-System den nötigen Sicherheitsanforderungen genügt, dass diese in einem Kontext effektiv sind und etwaige Fehlerzustände in Form von Sicherheitsproblemen bekannt sind.Die Autoren geben einen fundierten, praxisorientierten Überblick über die technischen, organisatorischen, prozessoralen, aber auch menschlichen Aspekte des Sicherheitstestens und vermitteln das notwendige Praxiswissen, um für IT-Anwendungen die Sicherheit zu erreichen, die für eine wirtschaftlich sinnvolle und regulationskonforme Inbetriebnahme von Softwaresystemen notwendig ist.Aus dem Inhalt:- Grundlagen des Testens der Sicherheit- Sicherheitsanforderungen und -risiken- Ziele und Strategien von Sicherheitstests- Sicherheitstestprozesse im Softwarelebenszyklus- Testen von Sicherheitsmechanismen- Auswertung von Sicherheitstests- Auswahl von Werkzeugen und Standards- Menschliche Faktoren, SicherheitstrendsDabei orientiert sich das Buch am Lehrplan "ISTQB® Advanced Level Specialist – Certified Security Tester" und eignet sich mit vielen erläuternden Beispielen und weiterführenden Literaturverweisen und Exkursen gleichermaßen für das Selbststudium wie als Begleitliteratur zur entsprechenden Schulung und folgender Prüfung zum ISTQB® Certified Tester – Sicherheitstester.

Governance of Enterprise IT based on COBIT 5 Springer-Verlag

Master the latest technology and developments from the field with the book specifically oriented to the needs of those learning information systems -- PRINCIPLES OF INFORMATION SECURITY, 6E. Taking a managerial approach, this bestseller emphasizes all aspects of information security, rather than just the technical control perspective. Readers

gain a broad overview of the entire field of information security and related elements with the detail to ensure understanding. The book highlights terms used in the field and a history of the discipline as readers learn how to manage an information security program. This edition highlights the latest practices with fresh examples that explore the impact of emerging technologies, such as the Internet of Things, Cloud Computing, and DevOps. Updates address technical security controls, emerging legislative issues, digital forensics, and ethical issues in IS security, making this the ideal IS resource for business decision makers. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Cyber Security Engineering Bogdan Wit

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 Cybersecurity Law, Standards and Regulations (2nd Edition), 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. This new edition responds to the rapid changes in the cybersecurity industry, threat landscape and providers. It addresses the increasing risk of zero-day attacks, growth of state-sponsored adversaries and consolidation of cybersecurity products

and services in addition to the substantial updates of standards, source links and cybersecurity products.
Compendium on Enterprise Resource Planning European Association for Security
International Standard ISO/IEC 27034-1:2011/Cor.1:2014Information Technology-Security Techniques-Application SecurityBusiness Continuity in a Cyber WorldSurviving CyberattacksBusiness Expert Press
Research Anthology on Privatizing and Securing Data IGI Global
Falar de Segurança da Informação em um mundo em constante transformação é sempre um desafio. De um lado, temos a necessidade de manter os dados protegidos de todas as ameaças que existem e surgem a cada dia. Do outro lado, a preocupação de que essa proteção afete o mínimo possível na usabilidade, performance e experiência do usuário. Apesar de todo o “glamour”, o profissional da área muitas vezes é persona non grata no mundo corporativo. Carrega o estigma de ser o pessimista, aquele que atrapalha o negócio, aquele que anuncia uma tragédia que nunca ocorre e que por esse motivo exige a aplicação de uma série de controles e condições para os dados e sistemas. Esse profissional deve saber justificar suas ações através de argumentos baseados em metodologias sólidas. Deve entender e saber explicar os fundamentos técnicos falando a linguagem do negócio. Este livro é composto de uma série de artigos inéditos escritos por profissionais de destaque na área atuando no Brasil e no exterior e que entendem que Segurança da Informação não pode ser um “trilho” de maneira que imobilize a operação das organizações, mas, sim, uma “trilha”, na medida em que a proteção é dosada por meio da análise dos riscos no percurso. O leitor poderá usar o conteúdo desta obra de forma não linear, como apoio para decidir qual caminho seguir, aproveitando não somente o conteúdo técnico aqui contido, como também a experiência e as lições aprendidas de cada autor. Artigos e seus autores: Procuram-se Hackers – Adriano Mauro Cansian Gestão de Risco – Augusto Paes de Barros Conscientização em Segurança da Informação Como Processo – Anderson Ramos Gestão de Identidades e Acessos – Felipe Silva Introdução à Criptografia Aplicada – Galeno Garbe Melhores Práticas em Segurança de Redes Sem Fio – Luiz Eduardo dos Santos Gestão de Vulnerabilidades e Atualizações de Segurança – Fernando Fonseca Segurança no Desenvolvimento de Software – Wagner Elias O Papel do Usuário – Altieres Rohr Perspectiva, Desafios e Tendências em Auditoria de Tecnologia e Segurança da Informação – Ricardo Castro Estabelecendo a Resiliência Operacional: Definindo e Construindo uma Estratégia para a Continuidade dos Negócios – Eduardo Vianna de Camargo Neves Derivações para o Futuro da Segurança da Informação – Fábio F. Ramo
IT-Sicherheit mit System Springer-Verlag
"Ulf Mattsson leverages his decades of experience as a CTO and security expert to show how companies can achieve data compliance without sacrificing operability." Jim Ambrosini, CISSP, CRISC, Cybersecurity Consultant and Virtual CISO "Ulf Mattsson lays out not just the rationale for accountable data governance, he provides clear strategies and tactics that every business leader should know and put into practice. As individuals, citizens and employees, we should all take heart that following his sound thinking can provide us

all with a better future." Richard Purcell, CEO Corporate Privacy Group and former Microsoft Chief Privacy Officer Many security experts excel at working with traditional technologies but fall apart in utilizing newer data privacy techniques to balance compliance requirements and the business utility of data. This book will help readers grow out of a siloed mentality and into an enterprise risk management approach to regulatory compliance and technical roles, including technical data privacy and security issues. The book uses practical lessons learned in applying real-life concepts and tools to help security leaders and their teams craft and implement strategies. These projects deal with a variety of use cases and data types. A common goal is to find the right balance between compliance, privacy requirements, and the business utility of data. This book reviews how new and old privacy-preserving techniques can provide practical protection for data in transit, use, and rest. It positions techniques like pseudonymization, anonymization, tokenization, homomorphic encryption, dynamic masking, and more. Topics include Trends and Evolution Best Practices, Roadmap, and Vision Zero Trust Architecture Applications, Privacy by Design, and APIs Machine Learning and Analytics Secure Multiparty Computing Blockchain and Data Lineage Hybrid Cloud, CASB, and SASE HSM, TPM, and Trusted Execution Environments Internet of Things Quantum Computing And much more!

Information Technology-Security Techniques-Application Security Van Haren

Van Haren Publishing is the world’s leading publisher in best practice, methods and standards within IT Management, Project Management, Enterprise Architecture and Business Management. We are the official publisher for some of the world’s leading organizations and their frameworks including: The Open Group [TOGAF], IPMA-NL, ITSqc [eSCM Models], GamingWorks [ABC of ICT], ASL BiSL Foundation, IAOP®, IACCM, CRP Henri Tudor and PMI NL. This catalog will provide you with an overview of our most popular and upcoming titles, but also gives you a quality summary on internationally relevant frameworks. Van Haren Publishing is an independent, worldwide recognized publisher, well known for our extensive professional network (authors, reviewers and accreditation bodies of standards), flexibility and years of experience. We make content available in hard copy and digital formats, designed to suit your personal preference (iPad, Kindle and online), available through over 50 distribution partners (Amazon, Google Play, Barnes & Noble, Managementboek and Bol.com, etc.) and over 700 outlets worldwide. Free whitepapers are available in our eKnowledge, with a licence for our eLibrary you can download all our eBooks within your area of expertise and in our eShop you can place your order in your favorite media format: hard copy or eBook.

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

Uluslararası bir standart olarak geliştirilen ISO 27001 Bilgi Güvenliği Yönetim Sistemi, kuruluşların iş süreçlerinde oluşturulan ve işlenen bilgilerin gizlilik, bütünlük ve erişilebilirlik boyutlarında temel şartları belirlemektedir. Çağımızda gittikçe dijitalleşen süreçler üzerindeki tehdit ve

zayıflıkların yarattığı bilgi güvenliği risklerinin bir sistem dahlinde ele alınması, değerlendirilmesi ve işlenmesi bilgi güvenliği kontrolleri için uygulama prensipleri gerekmektedir. Bilgi güvenliğinin bir kurumsal yönetim unsuru olarak insan, teknoloji ve süreçler arasındaki etkileşimlerde kullanılan teknolojilerin güvenliği, fiziksel güvenlik, risk yönetimi, iş sürekliliği ile yasa ve yönetmeliklere uyum gibi unsurlarla yakından ilgili olması, bunların yanısıra çalışanlara, iş ortaklarına, müşterilere ve topluma yönelik çeşitli yükümlülükleri bünyesinde barındırması bu tür bir sistemin kuruluşlar için ne derece önemli olduğunu göstermektedir. Bu kitapçık, ISO 27001 Bilgi güvenliği yönetim sisteminin şartlarıyla ISO 27002 Bilgi güvenliği kontrolleri için uygulama prensipleri dikkate alınarak bu konuda bünyelerinde BGYS kurmak ve bu standarda göre belgelendirilmek isteyen kuruluşlara bir rehber olmak amacıyla hazırlanmıştır.
Zintegrowany system zarządzania unieszkodliwianiem azbestu w ujęciu systemowym Cinius Yayınları
This is the Digital Practitioner Foundation Study Guide for the DPBoK Part 1 Examination. It gives an overview of every learning objective included in the Digital Practitioner Foundation syllabus, and provides in-depth coverage on preparing and taking the DPBoK Part 1 Examination. It is specifically designed to help individuals prepare for certification. This Study Guide is excellent material for: • Senior digital business professionals who need an increased awareness of digital practices • Mid-career IT professionals who need to stay relevant and validate their digital Subject Matter Expert (SME) status in specific domain areas • Entry-level computing and digital business professionals • College-level students and computing and digital business majors It covers the following topics: • An introduction to DPBoK Foundation certification, including the DPBoK Part 1 Examination • Key terminology, key concepts, and the structure of the Body of Knowledge • Basic concepts employed by the Digital Practitioner • The capabilities of digital infrastructure and initial concerns for its effective, efficient, and secure operation • The objectives and activities of application development • Why product management is formalized as a company or team grows, and the differences between product and project management • The key concerns and practices of work management as a team increases in size • The basic concepts and practices of operations management in a digital/IT context • How to coordinate as the organization grows into multiple teams and multiple products • IT investment and portfolio management • Organizational structure, human resources, and cultural factors • Governance, risk, security, and compliance • Information and data management on a large scale • Practices and methods for managing complexity using Enterprise Architecture
Security at the Source Rothstein Publishing
The Digital Practitioner Pocket Guide is designed to be a handy reference guide to selected parts of the Digital Practitioner Body of Knowledge™ Standard. It is designed to help: • Those who require a first introduction and basic understanding of the Digital Practitioner Body of Knowledge Standard • Individuals who wish to create and manage product offerings with an increasing digital component, or lead their organization

through Digital Transformation • IT professionals working within any size organization, from a startup through to a large enterprise, that has adopted digital approaches It covers the following topics: • A brief introduction to the Digital Practitioner Body of Knowledge Standard • An introduction to key terminology, key concepts, and the structure of the Body of Knowledge • Basic concepts employed by the Digital Practitioner • The capabilities of digital infrastructure and initial concerns for its effective, efficient, and secure operation • The objectives and activities of application development • Why product management is formalized as a company or team grows, and the differences between product and project management • The key concerns and practices of work management as a team increases in size • The basic concepts and practices of operations management in a digital/IT context • How to coordinate as the organization grows into multiple teams and multiple products • IT investment and portfolio management • Organizational structure, human resources, and cultural factors • Governance, risk, security, and compliance • Information and data management on a large scale • Practices and methods for managing complexity using Enterprise Architecture