Cybersecurity Capability Maturity Model White Paper

Thank you enormously much for downloading **Cybersecurity Capability Maturity Model White Paper**.Maybe you have knowledge that, people have look numerous time for their favorite books subsequent to this Cybersecurity Capability Maturity Model White Paper, but stop up in harmful downloads.

Rather than enjoying a good book taking into account a mug of coffee in the afternoon, then again they juggled like some harmful virus inside their computer. **Cybersecurity Capability Maturity Model White Paper** is user-friendly in our digital library an online access to it is set as public for that reason you can download it instantly. Our digital library saves in compound countries, allowing you to get the most less latency era to download any of our books with this one. Merely said, the Cybersecurity Capability Maturity Model White Paper is universally compatible behind any devices to read.

Developing Cybersecurity Capacity Springer Nature

The second publication in the Create, Protect, and Deliver Digital Business value series provides practitioners with detailed guidance on creating a NIST Cybersecurity Framework risk management program using NIST Special Publication 800-53, the DVMS Institute ' s CPD Model, and existing digital business systems

Cybersecurity Maturity Model Certification (CMMC): Levels 1-3 Manual IGI Global

This book covers the following main topics: A) information and knowledge management; B) organizational models and information systems; C) software and systems modeling; D) software systems, architectures, applications and tools; E) multimedia systems and applications; F) computer networks, mobility and pervasive systems; G) intelligent and decision support systems; H) big data analytics and applications; I) human–computer interaction; J) ethics, computers and security; K) health informatics; L) information technologies in education; M) information technologies in radio communications; N) technologies for biomedical applications. This book is composed by a selection of articles from The 2022 World Conference on Information Systems and Technologies (WorldCIST'22), held between April 12 and 14, in Budva, Montenegro. WorldCIST is a global forum for researchers and practitioners to present and discuss recent results and innovations, current trends, professional experiences, and challenges of modern information systems and technologies research, together with their technological development and applications.

Enterprise Cybersecurity Springer

This book focuses on the vulnerabilities of state and local services to cyber-threats and suggests possible protective action that might be taken against such threats. Cyber-threats to U.S. critical infrastructure are of growing concern to policymakers, managers and consumers. Information and communications technology (ICT) is ubiquitous and many ICT devices and other components are interdependent; therefore, disruption of one component may have a negative, cascading effect on others. Cyber-attacks might include denial of service, theft or manipulation of data. Damage to critical infrastructure through a cyber-based attack could have a significant impact on the national security, the economy, and the livelihood and safety of many individual citizens. Traditionally cyber security has generally been viewed as being focused on higher level threats such as those against the internet or the Federal government. Little attention has been paid to cyber-security at the state and local level. However, these governmental units play a critical role in providing services to local residents and consequently are highly vulnerable to cyber-threats. The failure of these services, such as waste water collection and water supply, transportation, public safety, utility services, and communication services, would pose a great threat to the public. Featuring contributions from leading experts in the field, this volume is intended for state and local government officials and managers, state and Federal officials, academics, and public policy specialists.

CERT Resilience Management Model (CERT-RMM) Independently Published

A Systems Approach to Managing the Complexities of Process Industries discusses the principles of system engineering, system thinking, complexity thinking and how these apply to the process industry, including benefits and implementation in process safety management systems. The book focuses on the ways system engineering skills, PLM, and IIoT can radically improve effectiveness of implementation of the process safety management system. Covering lifecycle, megaproject system engineering, and project management issues, this book reviews available tools and software and presents the practical web-based approach of Analysis & Dynamic Evaluation of Project Processes (ADEPP) for system engineering of the process manufacturing development and operation phases. Key solutions proposed include adding complexity management steps in the risk assessment framework of ISO 31000 and utilization of Installation Lifecycle Management. This study of this end-to-end process will help users improve operational excellence and navigate the complexities of managing a chemical or processing plant. Presents a review of Operational Excellence and Process Safety Management Methods, along with solutions to complexity assessment and management Provides a comparison of the process manufacturing industry with discrete manufacturing, identifying similarities and areas of customization for process manufacturing Discusses key solutions for managing the complexities of process manufacturing development and operational phases

The Rules of Project Risk Management Routledge

CERT® Resilience Management Model (CERT-RMM) is an innovative and transformative way to manage operational resilience in complex, risk-evolving environments. CERT-RMM distills years of research into best practices for managing the security and survivability of people, information, technology, and facilities. It integrates these best practices into a unified, capability-focused maturity model that encompasses security, business continuity, and IT operations. By using CERT-RMM, organizations can escape silo-driven approaches to managing operational risk and align to achieve strategic resili.

The Cybersecurity Maturity Model Certification (CMMC) Apress

The Rules of Project Risk Management, 2nd Edition, provides practical experience-based guidance to support the delivery of effective project risk management. While the discipline is recognised as a major contributor to the successful outcome of projects, its implementation is far from straightforward. Successful delivery requires an in-depth understanding of the "ingredients" of effective risk management practices which impact project performance. The book's value is derived from the description of these ingredients in a manner which will support their practical implementation. The author describes a series of guidelines (labelled "rules") to support the practical application of project risk management to positively influence project outcomes. The rules are supported by mini case studies of both successful and unsuccessful projects to bring to life the ramifications of effective and poor risk management respectively, and are assembled under seven headings of environment, external stakeholders, organisation and culture, leadership and governance, internal stakeholders, risk resources and system. This second edition contains a new glossary of terms and an overview of the risk management process to enable those new to the subject to understand the core risk management activities. It also contains six more individual guidelines and ten more case studies to support practitioners, researchers and academics alike to gain an even greater appreciation of the drivers of successful project risk management. Enabling the reader to "get inside" risk management to gain an appreciation of the individual components and "how the engine works", this book is essential reading for project and risk management professionals. While the guidelines are described individually so specific subjects can be examined in detail, they must be considered together, for like a car, specialist carburettors, fuel injection or high-octane fuel on their own do not support improved performance. The guidelines can be considered as the elements that should be taken into account when compiling a risk maturity model to drive incremental improvement in risk management practices.

Medical Device Cybersecurity for Engineers and Manufacturers John Wiley & Sons

Past events have shed light on the vulnerability of mission-critical computer systems at highly sensitive levels. It has been demonstrated that common hackers can use tools and techniques downloaded from the Internet to attack government and commercial information systems. Although threats may come from mischief makers and pranksters, they are more

Software Process Improvement and Capability Determination CRC Press

Book 1: Cybersecurity Capability Maturity Model White Paper - Cybersecurity is a leading national security challenge facing this country today. An emerging topic of importance is how organizations track, assess, grow, and shape their workforce. Many organizations have turned to workforce planning as a way to understand their current cybersecurity human capital skills and abilities as well as potential infrastructure needs. The National Initiative for Cybersecurity Education (NICE) evolved from the Comprehensive National Cybersecurity Initiative (CNCI), Initiative 8 - Expand Cyber Education, to develop a technologically-skilled and cyber-savvy workforce with the right knowledge and skills. Towards these ends, Component 3 of NICE is focused on the cybersecurity Workforce Structure - specifically talent management and the role of workforce planning in developing the national cybersecurity workforce. NICE has initiated discussions and issued guidance on workforce planning for cybersecurity best practices. In spring 2012, NICE published a white paper titled: Best Practices for Planning a Cybersecurity Workforce1, which introduces workforce planning methodologies for cybersecurity. This White Paper introduces a qualitative management tool, a Cybersecurity Workforce Planning Capability Maturity Model, to help organizations apply the best practice elements of workforce planning in analyzing their cybersecurity workforce requirements and needs. Contents * EXECUTIVE SUMMARY * THE CYBERSECURITY LANDSCAPE: NOW'S THE TIME TO PLAN * MAKING THE CASE: A NEED FOR CYBER WORKFORCE PLANNING CAPABILITY * The Practice of Workforce Planning * The Benefits of Workforce Planning * INTRODUCTION TO THE NICE CMM DEFINING WORKFORCE CMMS * Existing Models * Components of the NICE CMM * Criteria Areas * Maturity Levels * DETAILED OVERVIEW OF THE NICE CMM Process and Analytics * Integrated Governance * Skilled Practitioners and Enabling Technology * ACHIEVING MATURITY * Differing Maturity Goals * Assessing Current Capability * Step One: Gather Data * Step Two: Analyze Data and Determine Current Maturity * Step Three: Progressing in Maturity * BENEFITS OF ACHIEVING CYBERSECURITY WORKFORCE PLANNING MATURITY * CONCLUSION Book 2: Best Practices for Planning a Cybersecurity Workforce White Paper - The Nation's cybersecurity workforce is at the forefront of protecting critical infrastructure and computer networks from attack by foreign nations, criminal groups, hackers, and terrorist organizations. Organizations must have a clear understanding of their cybersecurity human capital skills and abilities as well as potential infrastructure needs to ensure protection against threats to information systems. Today, the cybersecurity community has evolved enough to define a National Cybersecurity Workforce Framework for understanding specialty areas of cybersecurity work and workforce needs. As a result, the field has reached a maturity level that enables organizations to inventory current capabilities. Next, as the nation seeks to build a skilled cybersecurity workforce, it will be necessary for organizations to mature further and begin forecasting future demand for the cybersecurity workforce. B2-A * INTRODUCTION * B2-B * BACKGROUND * B2-C * APPROACH * B2-D * CYBERSECURITY REQUIREMENTS * B2-E * CONCLUSION

Cybersecurity Maturity Model Certification (CMMC) Handbook Packt Publishing Ltd

Your one stop solution to implement a Cyber Defense Intelligence program in to your organisation. Key Features Intelligence processes and procedures for response mechanisms Master F3EAD to drive processes based on intelligence Threat modeling and intelligent frameworks Case studies and how to go about building intelligent teams Book Description Cyber intelligence is the missing link between your cyber defense operation teams, threat intelligence, and IT operations to provide your organization with a full spectrum of defensive capabilities. This book kicks off with the need for cyber intelligence and why it is required in terms of a defensive framework. Moving forward, the book provides a practical explanation of the F3EAD protocol with the help of examples. Furthermore, we learn how to go about threat models and intelligence products/frameworks and apply them to real-life scenarios. Based on the discussion with the prospective author I would also love to explore the induction of a tool to enhance the marketing feature and functionality of the book. By the end of this book, you will be able to boot up an intelligence program in your organization based on the operation and tactical/strategic spheres of Cyber defense intelligence. What you will learn Learn about the Observe-Orient-Decide-Act (OODA) loop and it's applicability to security Understand tactical view of Active defense concepts and their application in today's threat landscape Get acquainted with an operational view of the F3EAD process to drive decision making within an organization Create a Framework and Capability Maturity Model that integrates inputs and outputs from key functions in an information security organization Understand the idea of communicating with the Potential for Exploitability based on cyber intelligence Who this book is for This book targets incident managers, malware analysts, reverse engineers, digital forensics specialists, and intelligence analysts; experience in, or knowledge of, security operations, incident responses or investigations is desirable so you can make the most of the subjects presented.

The Cybersecurity Maturity Model Certification (CMMC) – A pocket guide Addison-Wesley Professional

Data analysis is an important part of modern business administration, as efficient compilation of information allows managers and business leaders to make the best decisions for the financial solvency of their organizations. Understanding the use of analytics, reporting, and data mining in everyday business environments is imperative to the success of modern businesses. Applying Business Intelligence Initiatives in Healthcare and Organizational Settings incorporates emerging concepts, methods, models, and relevant applications of business intelligence systems within problem contexts of healthcare and other organizational boundaries. Featuring coverage on a broad range of topics such as rise of embedded analytics, competitive advantage, and strategic capability, this book is ideally designed for business analysts, investors, corporate managers, and entrepreneurs seeking to advance their understanding and practice of business intelligence.

CyberWar, CyberTerror, CyberCrime and CyberActivism IGI Global

Organizations face increasing cybersecurity attacks that threaten their sensitive data, systems, and existence; but there are solutions. Experts recommend cybersecurity training and general awareness learning experiences as strategic necessities; however, organizations lack cybersecurity training planning, implementation, and optimization guidance. Cybersecurity Training: A Pathway to Readiness addresses the demand to provide cybersecurity training aligned with the normal flow of IT project delivery and technology operations. Cybersecurity Training combines best practices found in standards and frameworks like ITIL technology management, NIST Cybersecurity Framework, ISO risk, quality and information security management systems, and the Guide to the Project Management Body of Knowledge. Trainers will appreciate the approach that builds on the ADDIE model of instructional design, Bloom’s Taxonomy of Cognitive Thought, and Kirkpatrick’s Model of Evaluation, a trilogy of training best practices. Readers learn to apply this proven project-oriented training approach to improve the probability of successful cybersecurity awareness and role-based training experiences. The reader is guided to initiate, plan, design, develop, pilot, implement and evaluate training and learning, followed by continual improvement sprints and projects. Cybersecurity Training prepares trainers, project managers, and IT security professionals to deliver and optimize cybersecurity training so that organizations and its people are ready to prevent and mitigate cybersecurity threats leading to more resilient organizations.

Information Systems and Technologies Artech House

The demand for cybersecurity expertise is growing phenomenally; enhancing cybersecurity project skills will boost technology professionals’ careers and improve organizational cybersecurity readiness. Shields Up: Cybersecurity Project Management provides an end-to-end framework tuned for cybersecurity projects. More experienced cybersecurity professionals will appreciate the innovative and lean elements of this approach. The reader is guided through the delivery, management, and optimization approach that increases the probability of cybersecurity project success. Cybersecurity project management in Shields Up brings together international frameworks such as the Guide to the Project Management Body of Knowledge, the National Institute of Standards and Technology Cybersecurity Framework, ITIL 4 Service Management, the ISO 27001 Information Security Management, ISO 31000 Risk Management, and ISO 9000 Quality Management. A key benefit of this book is the reader can quickly apply the hybrid project management approach since it combines global frameworks already followed by cybersecurity professionals leading to successful projects. Never before has cybersecurity project management been so important.

Applying Business Intelligence Initiatives in Healthcare and Organizational Settings Academic Press

This book provides a comprehensive overview of smart ports and remote technologies in the maritime industry. It demonstrates how modern advances in artificial intelligence and robotics have transformed the shipping industry, and assesses the impact of this technology from a law and governance standpoint. The book covers a range of topics including port autonomous operations systems, cybersecurity, big data analytics, digitalization and blockchain to throw light on the opportunities and benefits of these new technologies in improving security and safety. It also considers the challenges and threats of their application. It concludes by examining the trajectory of national and international regulatory developments. The book will appeal to scholars and students of maritime technology, law and governance, as well as practitioners and policymakers. Chapters 8, 19 and 20 are available open access under a Creative Commons Attribution 4.0 International License via link.springer.com.

A Systems Approach to Managing the Complexities of Process Industries Springer

In today’s digital transformation environments, a rigorous cybersecurity approach to effective risk management — including contingency planning, outlining immediate actions, preparing post-breach responses — is central to defending organizations’ interconnected computer systems, networks, and infrastructure resources from malicious cyber-attacks. Specifically, cybersecurity technologies, processes, and practices need to be generalized and applied to intrusion detection and prevention measures. This entails analyzing profiles of cyber-attackers and building cyber-attack models for behavior simulation that can effectively counter such attacks. This comprehensive volume aims to cover all essential aspects of cybersecurity in digital transformation and to provide a framework for considering the many objectives and requirements involved. In addition to introducing theoretical foundations, the work also offers practical techniques for defending against malicious cybercriminals. Topics and features: Explores cybersecurity’s impact on the dynamics of interconnected, complex cyber- and physical systems, infrastructure resources, and networks Provides numerous examples of applications and best practices Considers methods that organizations can use to assess their cybersecurity awareness and/or strategy Describes anomaly intrusion detection, a key tool in thwarting both malware and theft (whether by insiders or external parties) of corporate data Addresses cyber-attacker profiles, cyber-attack models and simulation, cybersecurity ontology, access-control mechanisms, and policies for handling ransomware attacks Discusses the NIST Cybersecurity Framework, MITRE Adversarial Tactics, Techniques and Common Knowledge, CIS Critical Security Controls, and the ISA/IEC 62442 Cybersecurity Standard Gathering all the relevant information, this practical guide is eminently suitable as a self-study resource for engineers, scientists, computer scientists, and chief information officers. Further, with its many examples of best practices, it can serve as an excellent text for graduate-level courses and research into cybersecurity. Dietmar P. F. Möller, a retired full professor, is affiliated with the Institute for Mathematics at Clausthal University of Technology, Germany. He was an author of several other Springer titles, including Guide to Automotive Connectivity and Cybersecurity.

Smart Ports and Robotic Systems Business Expert Press

This book constitutes the refereed proceedings of the 17th International Conference on Software Process Improvement and Capability Determination, SPICE 2017, held in Palma de Mallorca, Spain, in October 2017. The 34 full papers presented together with 4 short papers were carefully reviewed and selected from 65 submissions. The papers are organized in the following topical sections: SPI in agile approaches; SPI in small settings; SPI and assessment; SPI and models; SPI and functional safety; SPI in various settings; SPI and gamification; SPI case studies; strategic and knowledge issues in SPI; education issues in SPI.

Cybercrime and Cybersecurity in the Global South TSO

Proactively plan and manage innovation in your business while keeping operations safe and secure. This book provides a framework and practices to help you safeguard customer information, prevent unauthorized access, and protect your brand and assets. Securing company operations is a board-level discussion. Across all industries, companies are pouring millions of dollars into taming cybercrime and other related security crime. Achieving and Sustaining Secured Business Operations presents a holistic approach looking top down, bottom up, and sideways. The end goal is to achieve and sustain a safe environment to conduct secured business operations while continuously innovating for competitive advantage. What You’ll Learn Discover why security, specifically secured business operations, needs to be part of business planning and oversight by design and not left to technologists to make the business case Determine what you can do in your role and in your organization to drive and implement integration and improvements in planning and managing secured business operations in conjunction with other business planning and management activities Choose ways in which progress toward achieving and sustaining secured business operations can be measured Understand best practices for organizing, planning, architecting, governing, monitoring, and managing secured business operations Create a framework, including methods and tools for operationalizing assessment, planning, and ongoing management of secured business operations Use cases and potential case studies for various industries and business models Who This Book Is For Chief executive officers and their leadership team; chief operations officers; chief information officers and their leadership team; chief information security officers; business functional middle managers; and enterprise, solution, and information technology architects

Cybersecurity Training Springer Nature

VERSION 2 ~ PROVIDES CMMC DEVELOPMENTS AND UPDATES.This is a companion guidebook to Cybersecurity Maturity Model Certification (CMMC) Controlled Unclassified Information (CUI) marking and storage requirements under CMMC. It has the latest information for any company or agency needing to understand their requirements to safeguard and protect sensitive US information and data. This guide answers CMMC Controls CMMC-C005/P1035 (Identify, categorize, and label CUI data), and CMMC-C005/P1036 (Define procedures for the handling of CUI Data). Written by Mark A. Russo the former Senior Information Security Engineer within the Department of Defense's (DOD) F-35 Joint Strike Fighter program. He has an extensive background in cybersecurity and is an expert in the Risk Management Framework (RMF) and DOD Instruction 8510, which implements RMF throughout the DOD and the federal government. He holds both a Certified Information Systems Security Professional (CISSP) certification and a CISSP in information security architecture (ISSAP). He holds a 2017 certification as a Chief Information Security Officer (CISO) from the National Defense University, Washington, DC. He retired from the US Army in 2012 as the Senior Intelligence Officer.

Achieving and Sustaining Secured Business Operations Routledge

Cybersecurity is vital for all businesses, regardless of sector. With constant threats and potential online dangers, businesses must remain aware of the current research and information available to them in order to protect themselves and their employees. Maintaining tight cybersecurity can be difficult for businesses as there are so many moving parts to contend with, but remaining vigilant and having protective measures and training in place is essential for a successful company. The Research Anthology on Business Aspects of Cybersecurity considers all emerging aspects of cybersecurity in the business sector including frameworks, models, best practices, and emerging areas of interest. This comprehensive reference source is split into three sections with the first discussing audits and risk assessments that businesses can conduct to ensure the security of their systems. The second section covers training and awareness initiatives for staff that promotes a security culture. The final section discusses software and systems that can be used to secure and manage cybersecurity threats. Covering topics such as audit models, security behavior, and insider threats, it is ideal for businesses, business professionals, managers, security analysts, IT specialists, executives, academicians, researchers, computer engineers, graduate students, and practitioners.

Shields Up CRC Press

Actionable guidance and expert perspective for real-world cybersecurity The Cyber Risk Handbook is the practitioner's guide to implementing, measuring and improving the counter-cyber capabilities of the modern enterprise. The first resource of its kind, this book provides authoritative guidance for real-world situations, and cross-functional solutions for enterprise-wide improvement. Beginning with an overview of counter-cyber evolution, the discussion quickly turns practical with design and implementation guidance for the range of capabilities expected of a robust cyber risk management system that is integrated with the enterprise risk management (ERM) system. Expert contributors from around the globe weigh in on specialized topics with tools and techniques to help any type or size of organization create a robust system tailored to its needs. Chapter summaries of required capabilities are aggregated to provide a new cyber risk maturity model used to benchmark capabilities and to road-map gap-improvement. Cyber risk is a fast-growing enterprise risk, not just an IT risk. Yet seldom is guidance provided as to what this means. This book is the first to tackle in detail those enterprise-wide capabilities expected by Board, CEO and Internal Audit, of the diverse executive management functions that need to team up with the Information Security function in order to provide integrated solutions. Learn how cyber risk management can be integrated to better protect your enterprise Design and benchmark new and improved practical counter-cyber capabilities Examine planning and implementation approaches, models, methods, and more Adopt a new cyber risk maturity model tailored to your enterprise needs The need to manage cyber risk across the enterprise—inclusive of the IT operations—is a growing concern as massive data breaches make the news on an alarmingly frequent basis. With a cyber risk management system now a business-necessary requirement, practitioners need to assess the effectiveness of their current system, and measure its gap-improvement over time in response to a dynamic and fast-moving threat landscape. The Cyber Risk Handbook brings the world's best thinking to bear on aligning that system to the enterprise and vice-a-versa. Every functional head of any organization must have a copy at-hand to understand their role in achieving that alignment.

Guide to Cybersecurity in Digital Transformation IT Governance Publishing

This is an updated version incorporating the major changes released by the DOD January 31, 2020 Changes include: 1) The latest FAQs and expectations for 2020 and beyond CMMC implementation efforts, 2) alignment of security controls with the most recent CMMC version 1.0 release, and 3) addition of sample control write-ups for inclusion in company Systems Security Plans and Cybersecurity policies.This manual is created to help the small and big business owner in meeting the newest in cybersecurity contracting requirements to conduct business with the Department of Defense (DOD). The CMMC is a wide-ranging certification process with security controls most aligned with federal National Institute of Standards and Technology (NIST) cybersecurity guidance. The gravest weakness of these security controls is that the tell you what to do, but not how to do them. That is the purpose of this book. It provides the how-to best approach and answer the security control or at least where to proceed for how to fully implement the stated cybersecurity measure. The requirement to protect information and data is not just limited to the financial services, insurance, and health care sectors. It is difficult to identify a federal or industrial sector that escapes some responsibility to protect its electronic data. Indeed, some areas deal with more sensitive information, so it is not a surprise that the DOD recently took steps to have its contractors provide "adequate security" for "Controlled Unclassified Information (CUI). CMMC is in its early throes of its roll out. This is a first edition where the author's over 20 years in cybersecurity controls and security engineering is intended to help. Don't expect DOD to be ready for a while. This book will help you and your IT staff start the challenge of CMMC.