Cybersecurity Capability Maturity Model White Paper

Getting the books **Cybersecurity Capability Maturity Model White Paper** now is not type of inspiring means. You could not without help going later than ebook accretion or library or borrowing from your links to contact them. This is an entirely simple means to specifically acquire guide by on-line. This online statement Cybersecurity Capability Maturity Model White Paper can be one of the options to accompany you as soon as having additional time.

It will not waste your time. believe me, the e-book will extremely declare you new situation to read. Just invest little grow old to approach this on-line publication **Cybersecurity Capability Maturity Model White Paper** as skillfully as review them wherever you are now.

Research Anthology on Advancements in Cybersecurity Education CRC Press
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.
Research Anthology on Privatizing and Securing Data Academic Press
Cybersecurity for medical devices is no longer optional. We must not allow sensationalism or headlines to drive the discussion… Nevertheless, we must proceed with urgency. In the end, this is about preventing patient harm and preserving patient trust. A comprehensive guide to medical device secure lifecycle management, this is a book for engineers, managers, and regulatory specialists. Readers gain insight into the security aspects of every phase of the product lifecycle, including concept, design, implementation, supply chain, manufacturing, postmarket surveillance, maintenance, updates, and end of life. Learn how to mitigate or completely avoid common cybersecurity vulnerabilities introduced during development and production. Grow your awareness of cybersecurity development topics ranging from high-level concepts to practical solutions and tools. Get insight into emerging regulatory and customer expectations. Uncover how to minimize schedule impacts and accelerate time-to-market while still accomplishing the main goal: reducing patient and business exposure to cybersecurity risks. Medical Device Cybersecurity for Engineers and Manufacturers is designed to help all stakeholders lead the charge to a better medical device security posture and improve the resilience of our medical device ecosystem.
The Digital Supply Chain IGI Global
This book offers a compact guide to IEC61850 systems, including wide-area implementation, as it has been applied to real substations worldwide. It utilises technical brochures and papers based on existing practice of IEC61850 systems that give stakeholders from different disciplines an understanding of systems in use, their features, how they are applied and approach for implementation. The book offers a holistic practical view considering all relevant interfaces and possibilities. It includes the different applications, practical implementation considerations and choices made for IEC61850 PACS (Protection Automation & Control System) designs. Power system engineers, planners, technicians and researchers will find the book useful for exploring, developing and delivering these systems.
Software Process Improvement and Capability Determination IGI Global
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.
CERT Resilience Management Model (CERT-RMM) Apress
The Power Grid: Smart, Secure, Green and Reliable offers a diverse look at the traditional engineering and physics aspects of power systems, also examining the issues affecting clean power generation, power distribution, and the new security issues that could potentially affect the availability and reliability of the grid. The book looks at growth in new loads that are consuming over 1% of all the electrical power produced, and how combining those load issues of getting power to the regions experiencing growth in energy demand can be addressed. In addition, it considers the policy issues surrounding transmission line approval by regulators. With truly multidisciplinary content, including failure analysis of various systems, photovoltaic, wind power, quality issues with clean power, high-voltage DC transmission, electromagnetic radiation, electromagnetic interference, privacy concerns, and data security, this reference is relevant to anyone interested in the broad area of power grid stability. Discusses state – of-the-art trends and issues in power grid reliability Offers guidance on purchasing or investing in new technologies Includes a technical document relevant to public policy that can help all stakeholders understand the technical issues facing a green, secure power grid
Transportation Systems and Engineering: Concepts, Methodologies, Tools, and Applications McGraw-Hill Education
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
Best Practices for Planning a Cybersecurity Workforce and the National Initiative for Cybersecurity Education (NICE) Cybersecurity Capability Maturity Model - Benefits of Workforce Planning Springer
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.
Cyber-Physical Security Addison-Wesley Professional
Previously, professionals had to make judgment calls based on subjective criteria, including their own acumen, in their decision making. In order to combat this subjectivity, maturity models can be implemented to allow organizations a means of assessing everyday processes and to offer a path towards advancement using transparent objective criteria. Diverse Applications and Transferability of Maturity Models is a pivotal reference source that provides vital research on the application of maturity models in organizational development in a variety of work environments. While highlighting topics such as open government, archives and records management, enterprise content management, and digital economy, this publication explores methods to help organizations effectively implement plans in any given management system. This book is ideally designed for professionals and researchers seeking current research on a variety of social science and applied science fields including business studies, computer science, digital preservation, information governance, information science, information systems, public administration, records management, and project management.
Building an Effective Security Program for Distributed Energy Resources and Systems DIANE Publishing
The Digital Supply Chain is a thorough investigation of the underpinning technologies, systems, platforms and models that enable the design, management, and control of digitally connected supply chains. The book examines the origin, emergence and building blocks of the Digital Supply Chain, showing how and where the virtual and physical supply chain worlds interact. It reviews the enabling technologies that underpin digitally controlled supply chains and examines how the discipline of supply chain management is affected by enhanced digital connectivity, discussing purchasing and procurement, supply chain traceability, performance management, and supply chain cyber security. The book provides a rich set of cases on current digital practices and challenges across a range of industrial and business sectors including the retail, textiles and clothing, the automotive industry, food, shipping and international logistics, and SMEs. It concludes with research frontiers, discussing network science for supply chain analysis, challenges in Blockchain applications and in digital supply chain surveillance, as well as the need to re-conceptualize supply chain strategies for digitally transformed supply chains. Covers both theoretical and practical points-of-view Contains material that readers from different backgrounds and disciplines will find informative Examines digital practices and challenges in-depth across a wide range of sectors Provides up-to-date, critical insights on the design, management and control of digitally connected supply chains Written by experts with strong backgrounds in the field
Cybercrime and Cybersecurity in the Global South IGI Global
The evidence continues to grow that the effective management of risk is the very kernel of successful project management. Its absence frequently leaves project sponsors lamenting missed objectives and shareholders coming to terms with an organisation ' s poor bottom line performance. Dr Robert Chapman's The Rules of Project Risk Management stands out from other risk management texts because it provides very practical guidance, supported by numerous mini case studies, many of which have attracted considerable publicity. The book brings to life both the benefits of project risk management when effectively applied and the ramifications when it is misunderstood or receives scant attention. The structure of the book is based on International Standard ISO 31000 seen through the lens of general systems theory - where projects are undertaken by organisations which have an external context and internal sub-systems. A project system is seen to be composed of seven key subject areas. Practical short ' rules ' or implementation guidelines, written in an engaging style, are offered to support each of these subject areas and aid quick assimilation of key risk management messages. Each rule focuses on a specific aspect of effective risk management which warrants attention in its own right. Taken together the rules will provide those implementing projects with the building blocks to secure a project ' s objectives. They have been drawn from a wealth of experience gained from applying risk management practices across multiple industries from Europe to Africa, the Middle East and Asia.
Modern CTO Best Practices for Planning a Cybersecurity Workforce and the National Initiative for Cybersecurity Education (NICE) Cybersecurity Capability Maturity Model - Benefits of Workforce PlanningBook 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 * CONCLUSIONMedical Device Cybersecurity for Engineers and Manufacturers

As society continues to heavily rely on software and databases, the risks for cyberattacks have increased rapidly. As the dependence on computers has become gradually widespread throughout communities and governments, there is a need for cybersecurity programs that can assist in protecting sizeable networks and significant amounts of data at once. Implementing overarching security policies for software systems is integral to protecting community-wide data from harmful attacks. Establishing Cyber Security Programs Through the Community Cyber Security Maturity Model (CCSMM) is an essential reference source that discusses methods in applying sustainable cybersecurity programs and policies within organizations, governments, and other communities. Featuring research on topics such as community engagement, incident planning methods, and information sharing, this book is ideally designed for cybersecurity professionals, security analysts, managers, researchers, policymakers, students, practitioners, and academicians seeking coverage on novel policies and programs in cybersecurity implementation.

Medical Device Cybersecurity for Engineers and Manufacturers IGI Global

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.

Cybersecurity and Homeland Security Springer Nature

Best Practices for Planning a Cybersecurity Workforce and the National Initiative for Cybersecurity Education (NICE) Cybersecurity Capability Maturity Model - Benefits of Workforce Planning

Guide to Automotive Connectivity and Cybersecurity Springer

From driverless cars to vehicular networks, recent technological advances are being employed to increase road safety and improve driver satisfaction. As with any newly developed technology, researchers must take care to address all concerns, limitations, and dangers before widespread public adoption. Transportation Systems and Engineering: Concepts, Methodologies, Tools, and Applications addresses current trends in transportation technologies, such as smart cars, green technologies, and infrastructure development. This multivolume book is a critical reference source for engineers, computer scientists, transportation authorities, students, and practitioners in the field of transportation systems management.

Energy and Water Development Appropriations for 2015: Department of Energy fiscal year 2015 justifications Routledge

This book presents the latest trends in attacks and protection methods of Critical Infrastructures. It describes original research models and applied solutions for protecting major emerging threats in Critical Infrastructures and their underlying networks. It presents a number of emerging endeavors, from newly adopted technical expertise in industrial security to efficient modeling and implementation of attacks and relevant security measures in industrial control systems; including advancements in hardware and services security, interdependency networks, risk analysis, and control systems security along with their underlying protocols. Novel attacks against Critical Infrastructures (CI) demand novel security solutions. Simply adding more of what is done already (e.g. more thorough risk assessments, more expensive Intrusion Prevention/Detection Systems, more efficient firewalls, etc.) is simply not enough against threats and attacks that seem to have evolved beyond modern analyses and protection methods. The knowledge presented here will help Critical Infrastructure authorities, security officers, Industrial Control Systems (ICS) personnel and relevant researchers to (i) get acquainted with advancements in the field, (ii) integrate security research into their industrial or research work, (iii) evolve current practices in modeling and analyzing Critical Infrastructures, and (iv) moderate potential crises and emergencies influencing or emerging from Critical Infrastructures.

Federal Register Springer

Cybersecurity refers to three things: measures to protect information technology; the information it contains, processes, and transmits, and associated physical and virtual elements (which together comprise cyberspace); the degree of protection resulting from application of those measures; and the associated field of professional endeavor. Virtually any element of cyberspace can be at risk, and the degree of interconnection of those elements can make it difficult to determine the extent of the cybersecurity framework that is needed. Identifying the major weaknesses in U.S. cybersecurity is an area of some controversy; the defense against attacks on computer systems and associated infrastructure has appeared to be generally fragmented and varying widely in effectiveness.

Resilience and Risk Routledge

The Global South is recognized as one of the fastest growing regions in terms of Internet population as well as the region that accounts for the majority of Internet users. However, It cannot be overlooked that with increasing connectivity to and dependence on Internet-based platforms and services, so too is the potential increased for information and cybersecurity threats and attacks. Further, it has long been established that micro, small, and medium enterprises (MSMEs) play a key role in national economies, serving as important drivers of economic growth in Global South economies. Yet, little is known about information security, cybersecurity and cybercrime issues and strategies contextualized to these developing economies and MSMEs. Cybercrime and Cybersecurity in the Global South: Concepts, Strategies and Frameworks for Greater Resilience examines the prevalence, nature, trends and impacts of cyber-related incidents on Global South economies. It further explores cybersecurity challenges, potential threats, and risks likely faced by MSMEs and governments of the Global South. A major thrust of this book is to offer tools, techniques, and legislative frameworks that can improve the information, data, and cybersecurity posture of Global South governments and MSMEs. It also provides evidence-based best practices and strategies relevant to the business community and general Information Communication Technology (ICT) users in combating and preventing cyber-related incidents. Also examined in this book are case studies and experiences of the Global South economies that can be used to enhance students ' learning experience. Another important feature of this book is that it outlines a research agenda to advance the scholarship of information and cybersecurity in the Global South. Features: Cybercrime in the Caribbean Privacy and security management Cybersecurity compliance behaviour Developing solutions for managing cybersecurity risks Designing an effective cybersecurity programme in the organization for improved resilience The cybersecurity capability maturity model for sustainable security advantage Cyber hygiene practices for MSMEs A cybercrime classification ontology

The Power Grid Springer Nature

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.

The Defense Industrial Base Elsevier

Modern society has become dependent on technology, allowing personal information to be input and used across a variety of personal and professional systems. From banking to medical records to e-commerce, sensitive data has never before been at such a high risk of misuse. As such, organizations now have a greater responsibility than ever to ensure that their stakeholder data is secured, leading to the increased need for cybersecurity specialists and the development of more secure software and systems. To avoid issues such as hacking and create a safer online space, cybersecurity education is vital and not only for those seeking to make a career out of cybersecurity, but also for the general public who must become more aware of the information they are sharing and how they are using it. It is crucial people learn about cybersecurity in a comprehensive and accessible way in order to use the skills to better protect all data. The Research Anthology on Advancements in Cybersecurity Education discusses innovative concepts, theories, and developments for not only teaching cybersecurity, but also for driving awareness of efforts that can be achieved to further secure sensitive data. Providing information on a range of topics from cybersecurity education requirements, cyberspace security talents training systems, and insider threats, it is ideal for educators, IT developers, education professionals, education administrators, researchers, security analysts, systems engineers, software security engineers, security professionals, policymakers, and students.

Critical Infrastructure Security and Resilience IGI Global

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.