Department Of Defense Risk Management Guide For Defense

AR 525-26 06/22/2004 INFRASTRUCTURE RISK MANAGEMENT (ARMY) , Survival Ebooks

The U.S. military relies on the defense industrial base (DIB) to meet requirements to fulfill the National Military Strategy. The potential destruction, incapacitation, or exploitation of critical DIB assets by attack, crime, technological failure, natural disaster, or man-made catastrophe could jeopardize the success of U.S. military operations. GAO was asked to review the Department of Defense's (DOD) Defense Critical Infrastructure Program and has already reported that DOD has not developed a comprehensive management plan for its implementation. This, the second GAO report, has (1) determined the status of DOD's efforts to develop and implement a risk management approach to ensure the availability of DIB assets, and (2) identified challenges DOD faces in its approach to risk management. GAO analyzed plans, guidance, and other documents on identifying, prioritizing, and assessing critical domestic and foreign DIB assets and held discussions with DOD and contractor officials.

Within the contents of this black and white version of the book, we will explore establishing a cyber strategy, morphing the cyber strategy into cyber accountability, and managing threat throughout the process. This book will focus on the US Department of Defense Risk Management Framework (RMF). Learning will be broken down into actionable comments with direct relationships to solve challenges in implementing a Risk Management Framework. We will walk through, step-by-step the crucial details and creativity required to win the cyber war as the Continentals did in 1783. The strategies and discussion herein can be easily applied to any implementation of cyber defense, indeed not isolated to the US Department of Defense

"Risk Management Framework (RMF) is the unified information security framework for the entire Federal government that is replacing the legacy Certification and Accreditation (C&A) processes within Federal government departments and agencies, the Department of Defense (DoD) and the Intelligence Community (IC). DoD has officially begun its transition from legacy DIACAP processes to the new RMF for DOD process.Department of Defense Risk Management Framework enables practitioners to immediately apply the training to their daily work. Each activity in the Risk Management Framework is covered in detail, as is each component of the documentation package and the continuous monitoring process. DoDI 8510.01, NIST 800-53 Security Controls and NIST 800-53a Evaluation Procedures are also covered in detail. Class participation exercises reinforce key concepts. RMF is designed for those who need to become proficient in the nuts and bolts of FISMA RMF implementation. This course provides the practical knowledge you need, without being slanted in favor of a specific software tool set."

FISMA and the Risk Management Framework: The New Practice of Federal Cyber Security deals with the Federal Information Security Management Act (FISMA), a law that provides the framework for securing information systems and managing risk associated with information resources in federal government agencies. Comprised of 17 chapters, the book explains the FISMA legislation and its provisions, strengths and limitations, as well as the expectations and obligations of federal agencies subject to FISMA. It also discusses the processes and activities necessary to implement effective information security management following the passage of FISMA, and it describes the National Institute of Standards and Technology's Risk Management Framework. The book looks at how information assurance, risk management, and information systems security is practiced in federal government agencies; the three primary documents that make up the security authorization package: system security plan, security assessment report, and plan of action and milestones; and federal information security-management requirements and initiatives not explicitly covered by FISMA. This book will be helpful to security officers, risk managers, system owners, IT managers, contractors, consultants, service providers, and others involved in securing, managing, or overseeing federal information systems, as well as the mission functions and business processes supported by those systems. Learn how to build a robust, near real-time risk management system and comply with FISMA Discover the changes to FISMA compliance and beyond Gain your systems the authorization they need

The Department of Defense (DoD) has significant experience in planning for and managing risk and uncertainty. The effects of climate and extreme weather represent additional risks to incorporate into the Department's various planning and risk management processes. Various studies have identified a broad range of effects that could impact our ability to fully execute the Defense mission of protecting and maintaining the security interests of the United States at home and around the world.

The U.S. military relies on the defense industrial base (DIB) to meet requirements to fulfill the National Military Strategy. The potential destruction, incapacitation, or exploitation of critical DIB assets by attack, crime, technological failure, natural disaster, or man-made catastrophe could jeopardize the success of U.S. military operations. GAO was asked to review the

Department of Defense's (DOD) Defense Critical Infrastructure Program and has already reported that DOD has not developed a comprehensive management plan for its implementation. This, the second GAO report, has (1) determined the status of DOD's efforts to develop and implement a risk management approach to ensure the availability of DIB assets, and (2) identified challenges DOD faces in its approach to risk management. GAO analyzed plans, guidance, and other documents on identifying, prioritizing, and assessing critical domestic and foreign DIB assets and held discussions with DOD and contractor officials. GAO recommends that DOD take specific actions to implement its risk management framework. DOD partially concurred with all of GAO's recommendations. DOD's comments cited actions it planned to take that are generally responsive to our recommendations.

The Department of Defense (DOD) believes it is increasingly likely that an adversary of the United States will use chemical or biological weapons against U.S. forces to degrade superior U.S. conventional warfare capabilities, placing service members' lives and effective military operations at risk. During the past 6 years, GAO has identified many problems with DOD's capabilities to defend against chemical and biological weapons and sustain operations in the midst of their use. Although GAO has found that DOD has made some improvements--in equipment, training, and reporting, and in the coordination of research and development activities--it has continuing concerns in each of these areas. One particular issue is the supply of chemical protective clothing and the way associated risk is assessed. Due to the upcoming expiration of existing protective suits, the slower rate at which new suits are entering the inventory, and DOD's method of assessing risk for individual items rather than complete protective ensembles, GAO believes that the risk for protective clothing shortages may

increase dramatically from now through 2007. GAO is also concerned that certain management weaknesses, such as program organizational complexity and prolonged vacancies in key leadership positions, may have sent a message throughout the department about the relative priority and importance of the Chemical and Biological Defense Program.
Acquisition excellence has changed the way the Department of Defense (DoD) designs, develops, manufactures, and supports systems. Our technical, business, and management approach for acquiring and operating systems has, and continues to, evolve. For example, we no longer can rely on military specifications and standards to define and control how our developers design, build, and support our new systems. Today we use commercial hardware and software, promote open systems architecture, and encourage streamlining processes, just to name a few of the initiatives that affect the way we do business. At the same time, the Office of the Secretary of Defense (OSD) has reduced the level of oversight and review of programs and manufacturers' plants.

This book is a complete course on the Federal Risk Management Framework from the Department of Defense perspective. Department of Defense Risk Management Framework enables practitioners to immediately apply the training to their daily work. Each activity in the Risk Management Framework is covered in detail, as is each component of the documentation package and the continuous monitoring process. NIST 800-53 Security Controls and NIST 800-53a Evaluation Procedures are also covered in detail. Class participation exercises reinforce key concepts, and slides are available to support classroom instruction. RMF is designed for those who need to become proficient in the "nuts and bolts" of FISMA RMF implementation. This course provides the practical knowledge you need, without being slanted in favor of a specific software tool set.

This monograph offers key considerations for DoD as it works through the on-going defense review. The author outlines eight principles for a risk management defense strategy. He argues that these principles provide "measures of merit" for evaluating the new administration's defense choices. This monograph builds on two previous works-- Known unknowns: unconventional "strategic shocks" in defense strategy development and The new balance: limited armed stabilization and the future of U.S. landpower. Combined, these three works offer key insights on the most appropriate DoD responses to increasingly "unconventional" defense and national security conditions. This work in particular provides DoD leaders food for thought, as they balance mounting defense demands and declining defense resources.

Congress needs the best available data about the Department of Defense’s (DoD’s) resource tradeoffs between the dual priorities of transformation and fighting terrorism. In 2001 DoD developed a capabilities-based approach focused on how future adversaries might fight, and a risk management framework to ensure that current defense needs are balanced against future requirements. Because the Future Years Defense Program (FYDP) is DoD’s centralized report providing data on current and planned resource allocations, this 2004 report assessed the extent to which the FYDP provides Congress visibility over projected defense spending, and implementation of DoD’s capabilities-based defense strategy and risk management framework. Figures and tables. This is a print on demand report.

Written by two INFOSEC experts, this book provides a systematic and practical approach for establishing, managing and operating a comprehensive Information

Assurance program. It is designed to provide ISSO managers, security managers, and INFOSEC professionals with an understanding of the essential issues required to develop and apply a targeted information security posture to both public and private corporations and government run agencies. There is a growing concern among all corporations and within the security industry to come up with new approaches to measure an organization's information security risks and posture. Information Assurance explains and defines the theories and processes that will help a company protect its proprietary information including: * The need to assess the current level of risk. * The need to determine what can impact the risk. * The need to determine how risk can be reduced. The authors lay out a detailed strategy for defining information security, establishing IA goals, providing training for security awareness, and conducting airtight incident response to system compromise. Such topics as defense in depth, configuration management, IA legal issues, and the importance of establishing an IT baseline are covered in-depth from an organizational and managerial decision-making perspective. Experience-based theory provided in a logical and comprehensive manner. Management focused coverage includes establishing an IT security posture, implementing organizational awareness and training, and understanding the dynamics of new technologies. Numerous real-world examples provide a baseline for assessment and comparison.

Legal risk covers all areas of business where regulation and the law impact on operations and decisions. From risks arising from contract drafting and management, through to regulators' new focus on conduct, as well as compliance, regulatory and dispute risks, the effective management of legal risk is key for organizations that want to maximise value while minimizing cost and exposure to legal losses. The Legal Risk Management Handbook is a practical guide to making sure your business is legal, protected and making the most of its opportunities. Written by experts in law and risk management, this highly practical guide sets out a clear definition for legal risk and a framework for its management. Covering the full spectrum of legal risks that international businesses can face, it translates legal concepts into clear mitigatory actions. Whether you are an in-house lawyer needing a clear approach to managing risk in your areas of influence, or a member of the risk management function needing a jargon-free guide to your company's legal responsibilities, you will find authoritative insight and guidance. Containing case studies from international businesses and real-life insights from those at the coal-face of legal risk management, The Legal Risk Management Handbook is essential reading for everyone who needs a better understanding of this important business topic.

The book is about RBPS (Risk Based Problem Solving) and RBDM (Risk Based Decision Making). Every project is subjected to the known risks and the unknown risks. Known risks are the four constraints of a project. The four constraints are; scope; schedule; cost; and quality. Unknown risks are the uncertainties and variances that surround every project. The book discusses in detail, with examples and risk stories to support the points made in the book, PM, RM, EVM, and Subcontract Management (SM). Understanding these four disciplines and how to incorporate them into a project, is essential to effective RBPS and RBDM. Project Management knowledge and skills are necessary to manage the known risks. Risk Management knowledge and skills are essential to identifying, assessing and mitigating unknown risks. Earned Value Management is important to tracking and controlling risk mitigation plans. Many companies outsource most of their work scope to subcontractors, so having Subcontract Management knowledge and skills is key to mitigating subcontract risks. The future of work is also discussed in detail. Future work will be projectized more. Working remotely is a trend that is increasing. Project Managers will have a more difficult problem in the future managing a diverse workforce of on-site, remote, and part-time workers. You need to be aware of future trends. The book is structured in a logical sequence and is easy to read. Step by step processes are presented in a logical way with practical examples to help you understand the process. Most of the methods and techniques discussed in the book are based on my DOD experience. However, these techniques also apply to the IT, and Construction Industries.

System security and information assurance requirements and specifications incorporated into the architectural design of a network enterprise must be driven by an adaptable and evolving network enterprise risk management plan. Network Risk Management must start at concept design and relate to the network's Concept of Operations. The purpose of this thesis is to examine some of the essential elements necessary in a network enterprise risk management plan for a complex global networked system similar to the Global Information Grid (GIG). It compares the current Department of Defense (DoD) framework for risk management with other popular network risk management process models. An important but difficult part of the risk management process is determining the value of network assets. Another important, but overlooked element of risk management processes, is evaluating the network for resiliency; the ability to return to normal in time to prevent the compromise of a mission. The contention is that risk management planning must include planning for network survivability and resiliency. Selected elementary network architectures are analyzed for attributes of the architectures that promote information assurance qualities of confidentiality, integrity, and availability. Finally, recommendations are made on applying important elements of network risk management into the conceptual architecture of a global network.

As part of ongoing efforts by the Office of the Under Secretary of Defense for Policy to develop an enterprise-wide risk management framework to guide Department of Defense (DoD) decisionmaking, the Office of the Secretary of Defense for Policy contracted a CSIS study team to identify risk management lessons learned and best practices among non-DoD U.S. government agencies and members of the international community, including foreign governments and international organizations. This report summarizes the CSIS study team's findings based on its literature review, two workshop meetings, and 14 case studies.

This book details decision analysis techniques with applications in engineering design and management and also analyzes decision making and risk management processes to better understand and improve decision making systems. Most books on decision analysis fall into two categories: those that are straightforward management decision making texts that that do not delve into more sophisticated techniques and concepts and those that emphasize the theoretical and analytical aspects, but do not discuss other perspectives on decision making. As such, this is the first book to present multiple perspectives on decision making without being too theoretical, all in effort to be useful to current and future engineers. The book presents three varied perspectives on decision making: problem-solving; the decision making process; and decision making systems. Practical examples and applications are plentiful and illustrate how to model and improve decision making systems. The mathematical rigor is kept to a minimum and is only used when comparing and contrasting different techniques. Extensive instructor resources are available, including worked solutions to all exercises, daily lesson plans for lectures, in-class activities, and sample assignments and exams. Topical coverage includes: an introduction to engineering decision making; decision making fundamentals; multi-criteria decision making; group decision making; decision making under uncertainty; game theory; decision making processes; the value of information; risk management; decision making systems; and modeling and improving decision making systems.

Although the Department of Defense's (DoD's) current risk management direction presents a comprehensive and robust approach to identifying, assessing, and managing risk, it does not adequately emphasize the interface between risk management and contract administration. In essence, a well- crafted, risk-appropriate contract can temper the sensitivity between technical risk and the probability of cost and schedule overruns, while a poorly crafted contract can actually increase the probability of cost and schedule overruns. By better linking sound risk management practices with sound contract administration practices, the DoD stands to continue being the bellwether federal agency for pushing the state-of-the-art in effective risk management.

Risk Management for Computer Security provides IT professionals with an integrated plan to establish and implement a corporate risk assessment and management program. The book covers more than just the fundamental elements that make up a good risk program for computer security. It presents an integrated how-to approach to implementing a corporate program, complete with tested methods and processes, flowcharts, and checklists that can be used by the reader and immediately implemented into a computer and overall corporate security program. The challenges are many and this book will help professionals in meeting their challenges as we progress through the twenty-first century. This book is organized into five sections. Section I introduces the reader to the theories of risk management and describes the field's changing environment as well as the art of managing risks. Section II deals with threat assessment and its input to risk assessment; topics covered include the threat assessment method and an example of threat assessment. Section III focuses on operating system vulnerabilities and discusses application vulnerabilities; public domain vs. COTS; and connectivity and dependence. Section IV explains what risk assessment is and Section V explores qualitative vs. quantitative tools and types of risk assessment and concludes with an assessment of the future of risk management. Corporate security professionals around the world will find this book a highly valuable source of information. Presents material in an engaging, easy-to-follow manner that will appeal to both advanced INFOSEC career professionals and network administrators entering the information security profession Addresses the needs of both the individuals who are new to the subject as well as of experienced professionals Provides insight into the factors that need to be considered and fully explains the numerous methods, processes and procedures of risk management

Non-developmental Items (NDI) acquisition programs are enjoying popular support as faster, cheaper alternatives to full-scale development programs. Unfortunately, DOD policy with respect to risk management in NDI programs is lacking. Tailoring DOD risk management policy to support NDI program management leaves the program manager (PM) much guess-work. A NDI PM's risk management program cannot reasonably benefit from DOD risk management guidance, procedures, and risk management tools because they are oriented to developmental program risks and risk management practices. Missing is any explicit consideration of the unique risks and risk management requirements in NDI programs. NDI PMs need more explicit guidance in policy and instruction regarding NDI risk management in the streamlined, accelerated NDI environment. This need is brought out in a case study of the Forward Area Air Defense Sensors Product Office which attempts to implement sound risk management into its NDI products without the benefit of definitive NDI risk identification, assessment, or response policy material. A lesson learned is the need for a published Risk Management Plan as the source of NDI risk management program decisions and actions. Specific recommendations are contained for inclusion in DOD policy with respect to NDI risk management.

DoD RMF ManualDepartment of Defense Risk Management Framework ProcessAn

Examination of Department of Defense Risk Management Policy for Nondevelopmental Items Acquisition Programs

Security Risk Management is the definitive guide for building or running an information security risk management program. This book teaches practical techniques that will be used on a daily basis, while also explaining the fundamentals so students understand the rationale behind these practices. It explains how to perform risk assessments for new IT projects, how to efficiently manage daily risk activities, and how to qualify the current risk level for presentation to executive level management. While other books focus entirely on risk analysis methods, this is the first comprehensive text for managing security risks. This book will help you to break free from the so-called best practices argument by articulating risk exposures in business terms. It includes case studies to provide hands-on experience using risk assessment tools to calculate the costs and benefits of any security investment. It explores each phase of the risk management lifecycle, focusing on policies and assessment processes that should be used to properly assess and mitigate risk. It also presents a roadmap for designing and implementing a security risk management program. This book will be a valuable resource for CISOs, security managers, IT managers, security consultants, IT auditors, security analysts, and students enrolled in information security/assurance college programs. Named a 2011 Best Governance and ISMS Book by InfoSec Reviews Includes case studies to provide hands-on experience using risk assessment tools to calculate the costs and benefits of any security investment Explores each phase of the risk management lifecycle, focusing on policies and assessment processes that should be used to properly assess and mitigate risk Presents a roadmap for designing and implementing a security risk management program

This thesis discusses risk in Department of Defense (DoD) weapon systems acquisition. It uses the Marine Corps' Advanced Amphibious Assault Vehicle (AAAV) as a case study in risk management strategy and techniques. The AAAV will provide the Marine Corps with a fast deploying, over-the-horizon, and waterborne insertion capability. The AAAV's improvements over the currently fielded Amphibious Assault Vehicle (AAV) will provide Marines with a highly survivable and lethal weapon system ashore. Risk is the possibility of damage, injury or loss. The severity of a risk is determined by a combination of both the probability of an unfavorable event occurring and the severity of the event's occurrence. Risks are present in virtually all DoD developmental programs. Programs suffer from risks in technical challenges, unstable system requirements, missing schedule milestones, unpredictable funding and cost overruns. The DoD currently uses techniques to mitigate risks inherent in advanced system development. This thesis analyzes the AAAV's Program Definition and Risk Reduction (PDRR) acquisition phase risk management strategy. The thesis concludes by drawing from the lessons learned in the AAAV program during PDRR and analyzing the application of the lessons learned during the AAAV's current acquisition phase, System Development and Demonstration (SDD).

This article describes the risk management defense extensions to the 2000 Project Management Institute (PMI) Project Management Body of Knowledge (2000 PMBOK(trademark) Guide). The Department of Defense (DoD) Draft Extension was developed to provide recommended tailoring of the 2000 PMBOK(trademark) Guide to Department of Defense-specific applications. The focus of this article is on Department of Defense-specific tailoring associated with risk management information that appears in Chapter 11 of the 2000 PMBOK(trademark) Guide including key supplemental information and enhancements.

RMF enables practitioners to immediately apply the training to their daily work. Each activity in the Risk Management Framework is covered in detail, as is each component of the documentation package and the continuous monitoring process. DoDI 8510.01, NIST 800-53 Security Controls and NIST 800-53a Evaluation Procedures are also covered in detail. Class participation exercises reinforce key concepts. RMF is designed for those who need to become proficient in the nuts and bolts of FISMA RMF implementation. This course provides the practical knowledge you need, without being slanted in favor of a specific software tool set.

In the last decade, the integration of unmanned aerial systems (UAS) into military operations has grown substantially. UAS have significantly contributed to U.S. military tactical, operational and strategic operations. Recently, the U.S. military has made increasing use of commercial off-the-shelf (COTS) UAS, yet none of the U.S. military services have a defined cybersecurity risk management process for COTS UAS. These systems have been susceptible to cyber attacks, leading to the May 2018 ban on the use of these systems across the Department of Defense (DoD). This research effort has developed a multi-echelon cybersecurity risk assessment process for the DoD. The proposed process would enable strategic, operational and tactical commanders to assess and communicate cybersecurity risks associated with COTS UAS. The process combined four steps from the Joint Risk Analysis Methodology (JRAM) framework and seven steps from a strategic risk business management process. This process would allow commanders to have an enhanced awareness of cybersecurity risks associated with COTS UAS operations, improved current cyber threat assessments, and tailored action plans for their areas of responsibility. The proposed process would help units and agencies across the DoD to resume their use, test and purchase of COTS UASs without the need for the current centralized waiver process.This compilation includes a reproduction of the 2019 Worldwide Threat Assessment of the U.S. Intelligence Community.