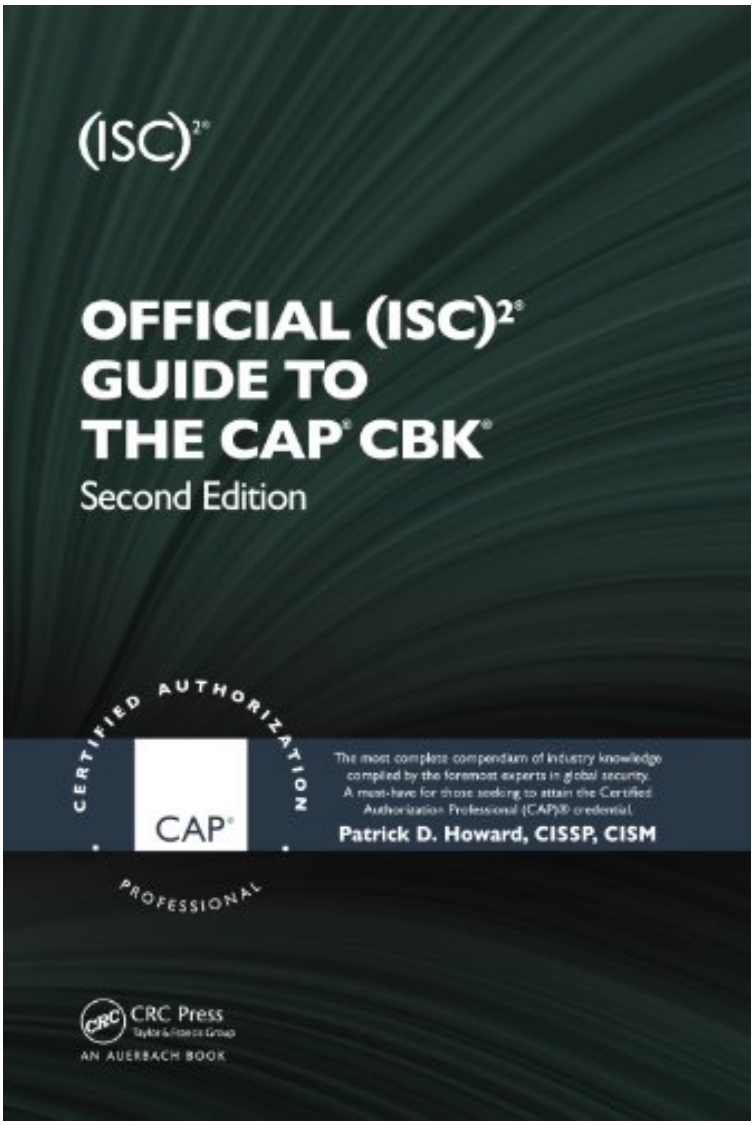
Official (ISC)2reg; Guide to the CAPreg; CBKreg;, Second Edition ((ISC)2 Press)

Patrick D. Howard



#168509 in eBooks 2016-04-19 2016-04-19File Name: B00BBZ4YNM | File size: 49.Mb

Patrick D. Howard : Official (ISC)2reg; Guide to the CAPreg; CBKreg;, Second Edition ((ISC)2 Press) before purchasing it in order to gage whether or not it would be worth my time, and all praised Official (ISC)2reg; Guide to the CAPreg; CBKreg;, Second Edition ((ISC)2 Press):

0 of 0 people found the following review helpful. SEVERLY OUT OF DATBy joy charlottaOFFICCIAL (ISC)2 GUIDE TO THE CAP CBK, Second EditionBy Patrick D. Howard, CISSP, CISMPublished 2012USBN 978-1-4398-2075Steven EddySept 1, 2017The author has done a great job given the state of the Risk Management Framework

(RMF) at the time. He was involved in one of the first RMF assessments which was for the Department of Transportation. This was before the DOD requirement to transition from the DIACAP Certification and Accreditation process to the RMF Assessment and Accreditation (AA) process. NIST Special Publication 800-37Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems a Security Life Cycle Approach is the overarching document for RMF. The problem with this book is that RMF has matured much since it was written. Assessment and Accreditation have been increasingly automated. The process has become more complicated and complex. Roll names have changed almost entirely. Practical steps required for a modern AA process are not given. DISArsquo;s Enterprise Mission Assurance Support Service (eMASS) application and website is essential and mandatory in prosecuting a modern AA effort. eMASS uploads Excel test result spreadsheets and scans, creates the System Security Plan, the POAM, the Implementation Plan, the Risk Assessment Plan (RAR) and the Security Assessment Plan (SAR). Many new roles such as the Security Control Assessor ndash; Reviewer (SCA-R) and Security Control Assessor- Verifier (SCA-V) are not mentioned, although they are two of the most critical roles. The execution of these roles are also accomplished in eMASS.An essential first element in categorizing systems is DoD information technology (IT) is broadly grouped as DoD information systems (IS), platform information technology (PIT) systems. This is not covered. Nor is one of the main advantages of RMF, reciprocity. Reciprocity is the ability to use authorizations of other similar systems to inherit compliance for security controls to a new system, avoiding redundant time and effort. Additionally, in categorization, there are also now categories of Very Low and Very High in addition to the Low, Moderate and High of the past. There is no mention of the Initial Approval to Test, which provides for testing of the system before production development takes place to prove the system concept is workable.FIPS, NIST and CNSS publications need to include titles, and brief summaries early in the book to avoid confusion and tell what subject matter they include in order to make referencing them easier. There is a glossary in the guide, but no acronym list, which is essential particularly in light of the renaming and adding of roles and processes. Inclusion of a compact disc containing a searchable soft copy of the book would be very helpful in studying the subject.Although this book was very well written for its time, it is very much out of date and needs to be updated along with the test it serves. I would not recommend reading or studying this as it will only confuse someone who is currently involved in or wishes to be involved in modern RMF program Assessments and Authorization processes. I have been told that a new test and training materials are being developed by (ISC)2 to update this certification. It is suggested that candidates wait for the new updated test and study materials before studying for the CAP certification. I hope my review will aid them in this effort. In the mean time I would wait for the new material before voyaging forward on a CAPP certification.4 of 4 people found the following review helpful. Reads like a boring dictionaryBy NAIt reads like a dictionary and is not focused on exam topics. I have been doing this kind of work for years and have been CISSP since 2001. This book was more confusing than helpful because it is written so badly. It is just long winded vague and their is no effort to map it to a job skill. It is PURELY CONCEPTUAL. It will make reference to a specific NIST document, but it will not put any context to statements, the graphics are average to poor and generally the book puts you to sleep. I recommend a third party book if you are preparing for the exam or a 3rd party class if you are attempting to gain the skills.7 of 8 people found the following review helpful. Pretty Good Prep MaterialBy BryanIts a read like all ISC books, but the content is pretty straight forward and the flow is logical, I will say that as a DoD IA professional there are some inaccuracies in the book, re: the book states that Physical (DoD 8500 PExx etc..) controls are inherited controls, this is not always true, it depends on the task, as an example, on an Army task I was on doing testing and CA leading to issuance of an ATO all Physical and Personnel controls were NOT inherited, they were considered shared, shared by the site (in this case TRADOC) and Ft Eustis, both entities shared the responsibility and as the accrediting entity we could not write the controls off as "inherited" they either passed or failed-as directed by the Army ODAA, so as with all INFOSEC/IA/Info Security controls, either DoD 8500 or NIST 800.53, they are often very specific to the site environment, task, and branch and variances do exist, it is not always so cut and dry.

Significant developments since the publication of its bestselling predecessor, Building and Implementing a Security Certification and Accreditation Program, warrant an updated text as well as an updated title. Reflecting recent updates to the Certified Authorization Professional (CAPreg;) Common Body of Knowledge (CBKreg;) and NIST SP 800-37, the Official (ISC)2reg; Guide to the CAPreg; CBKreg;, Second Edition provides readers with the tools to effectively secure their IT systems via standard, repeatable processes.Derived from the authorrsquo;s decades of experience, including time as the CISO for the Nuclear Regulatory Commission, the Department of Housing and Urban Development, and the National Science Foundationrsquo;s Antarctic Support Contract, the book describes what it takes to build a system security authorization program at the organizational level in both public and private organizations. It analyzes the full range of system security authorization (formerly CA) processes and explains how they interrelate. Outlining a user-friendly approach for top-down implementation of IT security, the book:Details an approach that simplifies the authorization process, yet still satisfies current federal government criteriaExplains how to combine disparate processes into a unified risk management methodologyCovers all the topics included in the Certified Authorization Professional (CAPreg;) Common Body of Knowledge (CBKreg;)Examines U.S. federal

polices, including DITSCAP, NIACAP, CNSS, NIAP, DoD 8500.1 and 8500.2, and NIST FIPSReviews the tasks involved in certifying and accrediting U.S. government information systemsChapters 1 through 7 describe each of the domains of the (ISC)2reg; CAPreg; CBKreg;. This is followed by a case study on the establishment of a successful system authorization program in a major U.S. government department. The final chapter considers the future of system authorization. The bookrsquo;s appendices include a collection of helpful samples and additional information to provide you with the tools to effectively secure your IT systems.

Praise for the popular first edition: This book focuses on the processes that must be employed by an organization to establish a certification and accreditation program based on current federal government criteriahellip; Pat has structured this book to address the key issues in certification and accreditation, including roles and responsibilities, the life cycle, and even a discussion of pitfalls to avoid. As with all of Patrsquo;s work, he provides the reader with practical information on what works and what does not hellip; Even if government certification and accreditation is not your concern, the new ISO 27002 (formerly ISO17799) will require all of us to look for a process to make certification and accreditation bearable. Pat has succeeded in doing just that with this practical and readable book.?Thomas R. Peltier, Peltier Associates, Member of the ISSA Hall of FameAbout the AuthorPatrick D. Howard, CISSP, CISM, is a senior consultant for SecureInfo, a Kratos Company. He has over 40 years experience in security, including 20 years service as a U.S. Army Military Police officer, and has specialized in information security since 1989. Mr. Howard began his service as the Chief Information Security Officer for the National Science Foundationrsquo;s Antarctic Support Contract in Centennial, Colorado in March 2012. He previously served as CISO for the Nuclear Regulatory Commission in Rockville, Maryland from 2008ndash;2012, and for the Department of Housing and Urban Development from 2005ndash;2008. Mr. Howard was named a Fed 100 winner in 2007, and is the author of three information security books: The Total CISSP Exam Prep Book, 2002; Building and Implementing a Security Certification and Accreditation Program, 2006; and Beyond Compliance: FISMA Principles and Best Practices, 2011. He is a member of the International Information Systems Security Certification Consortiumrsquo;s Government Advisory Board and Executive Writerrsquo;s Bureau, which he chairs. Mr. Howard is also an adjunct professor of Information Assurance at Walsh College, Troy Michigan. He graduated with a Bachelorrsquo;s degree from the University of Oklahoma in 1971 and a Masterrsquo;s degree from Boston University in 1984.