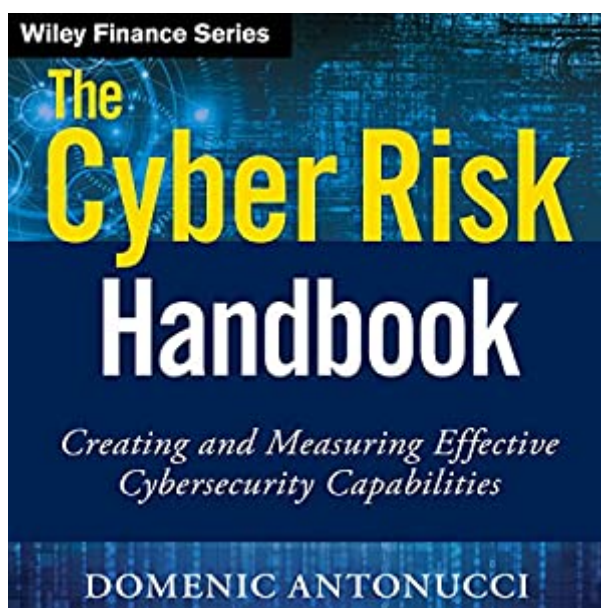The book was found

The Cyber Risk Handbook: Creating And Measuring Effective Cybersecurity Capabilities

Synopsis

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.

Book Information

Audible Audio Edition

Listening Length: 10 hours and 49 minutes

Program Type: Audiobook

Version: Unabridged

Publisher: Audible Studios

Audible.com Release Date: July 17, 2017

Language: English

ASIN: B073X6D3VT

Best Sellers Rank: #11 in Books > Business & Money > Finance > Financial Risk Management #46 in Books > Reference > Encyclopedias & Subject Guides > Business   #61 in Books > Audible Audiobooks > Nonfiction > Computers

Customer Reviews

Fluff. High-level restatements of the obvious. A collection of vanity-essays. Of no value to the practitioner. Go to the NIST website and get all the guidance you'll ever need in this area for free - honed by NIST with taxpayer dollars over more than a decade, with serious usable approaches and none of the pablum that fills this "handbook." Example: makes the claim that there are no value-at-risk measures in the world re cybersecurity, which belies the fact that multiple products which estimate Value at Risk in multiple ways have been available for years. Not only is this book content free, but it's also obviously editor-free.

Download to continue reading...

The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities CYBERSECURITY COMPLIANCE:: New York's Cybersecurity Requirements For Financial Services Company (NYCRR 500) Cybersecurity Exposed: The Cyber House Rules Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Learn To Use the Internet Safely and Responsibly Creating Capabilities: The Human Development Approach How to Measure Anything in Cybersecurity Risk Forensic Assessment of Violence Risk: A Guide for Risk Assessment and Risk Management COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance (GRC) Processes Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management Risk Adjustment for Measuring Healthcare Outcomes, Fourth Edition Political Warfare in Sub-Saharan Africa: U.S. Capabilities and Chinese Operations in Ethiopia, Kenya, Nigeria, and South Africa The Systems Thinking Playbook: Exercises to Stretch and Build Learning and Systems Thinking Capabilities Fluency 5 with Information Technology: Skills, Concepts, and Capabilities, 5th Edition Human Rights, Disability, and Capabilities Measuring and Monitoring Biological Diversity. Standard Methods for Amphibians (Biological Diversity Handbook) The Devil Inside the Beltway: The Shocking Expose of the US Government's Surveillance and Overreach Into Cybersecurity, Medicine and Small Business Cybersecurity and

Cyberwar: What Everyone Needs to Know Cybersecurity: Home and Small Business Cybersecurity and Infrastructure Protection