

1. Record Nr.	UNINA9910790090303321
Autore	Wheeler Evan
Titolo	Security risk management [[electronic resource] ] : building an information security risk management program from the ground up // Evan Wheeler
Pubbl/distr/stampa	Waltham, MA, : Syngress, 2011
ISBN	1-283-52639-5 9786613838841 1-59749-616-2
Edizione	[1st edition]
Descrizione fisica	1 online resource (361 pages)
Disciplina	005.8 658.4/7 658.47
Soggetti	Computer networks - Security measures Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Front Cover; Security Risk Management: Building an Information Security Risk Management Program from the Ground Up; Copyright; Table of Contents; Preface; Intended Audience; Organization of This Book; Acknowledgments; About the Author; About the Technical Editor; Part I: Introduction to Risk Management; Chapter 1. The Security Evolution; Introduction; How We Got Here; A Risk-Focused Future; Information Security Fundamentals; The Death of Information Security; Summary; References; Chapter 2. Risky Business; Introduction; Applying Risk Management to Information Security Business-Driven Security Program Security as an Investment; Qualitative versus Quantitative; Summary; References; Chapter 3. The Risk Management Lifecycle; Introduction; Stages of the Risk Management Lifecycle; Business Impact Assessment; A Vulnerability Assessment Is Not a Risk Assessment; Making Risk Decisions; Mitigation Planning and Long-Term Strategy; Process Ownership; Summary; Part II: Risk Assessment and Analysis Techniques; Chapter 4. Risk Profiling; Introduction; How Risk Sensitivity Is Measured; Asking the Right

Questions; Assessing Risk Appetite; Summary; Reference  
Chapter 5. Formulating a Risk Introduction; Breaking Down a Risk; Who or What Is the Threat?; Summary; References; Chapter 6. Risk Exposure Factors; Introduction; Qualitative Risk Measures; Risk Assessment; Summary; Reference; Chapter 7. Security Controls and Services; Introduction; Fundamental Security Services; Recommended Controls; Summary; Reference; Chapter 8. Risk Evaluation and Mitigation Strategies; Introduction; Risk Evaluation; Risk Mitigation Planning; Policy Exceptions and Risk Acceptance; Summary; Chapter 9. Reports and Consulting; Introduction; Risk Management Artifacts  
A Consultant's Perspective Writing Audit Responses; Summary; References; Chapter 10. Risk Assessment Techniques; Introduction; Operational Assessments; Project-Based Assessments; Third-Party Assessments; Summary; References; Part III: Building and Running a Risk Management Program; Chapter 11. Threat and Vulnerability Management; Introduction; Building Blocks; Threat Identification; Advisories and Testing; An Efficient Workflow; The FAIR Approach; Summary; References; Chapter 12. Security Risk Reviews; Introduction; Assessing the State of Compliance; Implementing a Process  
Process Optimization: A Review of Key Points The NIST Approach; Summary; References; Chapter 13. A Blueprint for Security; Introduction; Risk in the Development Lifecycle; Security Architecture; Patterns and Baselines; Architectural Risk Analysis; Summary; Reference; Chapter 14. Building a Program from Scratch; Introduction; Designing a Risk Program; Prerequisites for a Risk Management Program; Risk at the Enterprise Level; Linking the Program Components; Program Roadmap; Summary; Reference; Appendix A: Sample Security Risk Profile; A. General Information; B. Information Sensitivity  
C Regulatory Requirements

---

## Sommario/riassunto

The goal of Security Risk Management is to teach you practical techniques that will be used on a daily basis, while also explaining the fundamentals so you understand the rationale behind these practices. Security professionals often fall into the trap of telling the business that they need to fix something, but they can't explain why. This book will help you to break free from the so-called "best practices" argument by articulating risk exposures in business terms. You will learn techniques for how to perform risk assessments for new IT projects, how to efficiently manage daily ri

---