1. Record Nr. UNINA9910830594603321

Autore	Minoli Daniel <1952->
Titolo	Information technology risk management in enterprise environments [[electronic resource]] : a review of industry practices and a practical guide to risk management teams / / Jake Kouns, Daniel Minoli
Pubbl/distr/stampa	Hoboken, NJ, : Wiley, c2010
ISBN	1-118-21161-8 1-282-68665-8 9786612686658 0-470-55813-X 0-470-55811-3
Descrizione fisica	1 online resource (441 p.)
Altri autori (Persone)	KounsJake
Disciplina	658.4/78 658.472
Soggetti	Business enterprises - Computer networks - Security measures Information technology - Security measures Data protection Computer security Risk management
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di contenuto	INFORMATION TECHNOLOGY RISK MANAGEMENT IN ENTERPRISE ENVIRONMENTS; CONTENTS; PREFACE; ABOUT THE AUTHORS; PART I INDUSTRY PRACTICES IN RISK MANAGEMENT; 1. INFORMATION SECURITY RISK MANAGEMENT IMPERATIVES AND OPPORTUNITIES; 1.1 Risk Management Purpose and Scope; 1.1.1 Purpose of Risk Management; 1.1.2 Text Scope; References; Appendix 1A: Bibliography of Related Literature; 2. INFORMATION SECURITY RISK MANAGEMENT DEFINED; 2.1 Key Risk Management Definitions; 2.1.1 Survey of Industry Definitions; 2.1.2 Adopted Definitions; 2.2 A Mathematical Formulation of Risk 2.2.1 What Is Risk? A Formal Definition2.2.2 Risk in IT Environments; 2.2.3 Risk Management Procedures; 2.3 Typical Threats/Risk Events; 2.4 What is an Enterprise Architecture?; References; Appendix 2A: The

CISSPforum/ISO27k Implementers Forum Information Security Risk List for 2008; Appendix 2B: What is Enterprise Risk Management (ERM)?; 3. INFORMATION SECURITY RISK MANAGEMENT STANDARDS; 3.1 ISO/IEC 13335; 3.2 ISO/IEC 17799 (ISO/IEC 27002:2005); 3.3 ISO/IEC 27000 SERIES
3.3.1 ISO/IEC 27000, Information Technology-Security Techniques-Information Security Management Systems-Fundamentals and Vocabulary3.3.2 ISO/IEC 27001:2005, Information Technology-Security Techniques-Specification for an Information Security Management System; 3.3.3 ISO/IEC 27002:2005, Information Technology-Security Techniques-Code of Practice for Information Security Management; 3.3.4 ISO/IEC 27003 Information Technology-Security Techniques-Information Security Management System Implementation Guidance
3.3.5 ISO/IEC 27004 Information Technology-Security Techniques-Information Security Management-Measurement3.3.6 ISO/IEC 27005: 2008 Information Technology-Security Techniques-Information Security Risk Management; 3.4 ISO/IEC 31000; 3.5 NIST STANDARDS; 3.5.1 NIST SP 800-16; 3.5.2 NIST SP 800-30; 3.5.3 NIST SP 800-39; 3.6 AS/NZS 4360; References; Appendix 3A: Organization for Economic CoOperation and Development (OECD) Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security; 4. A SURVEY OF AVAILABLE INFORMATION SECURITY RISK MANAGEMENT METHODS AND TOOLS
4.1 Overview4.2 Risk Management/Risk Analysis Methods; 4.2.1 Austrian IT Security Handbook; 4.2.2 CCTA Risk Assessment and Management Methodology (CRAMM); 4.2.3 Dutch A&K Analysis; 4.2.4 EBIOS; 4.2.5 ETSI Threat Vulnerability and Risk Analysis (TVRA) Method; 4.2.6 FAIR (Factor Analysis of Information Risk); 4.2.7 FIRM (Fundamental Information Risk Management); 4.2.8 FMEA (Failure Modes and Effects Analysis); 4.2.9 FRAP (Facilitated Risk Assessment Process); 4.2.10 ISAMM (Information Security Assessment and Monitoring Method); 4.2.11 ISO/IEC Baselines; 4.2.12 ISO 31000 Methodology
4.2.13 IT-Grundschutz (IT Baseline Protection Manual)

Sommario/riassunto

Discusses all types of corporate risks and practical means of defending against them.Security is currently identified as a critical area of Information Technology management by a majority of government, commercial, and industrial organizations.Offers an effective risk management program, which is the most critical function of an information security program.