1. Record Nr. UNINA9910146407603321

Autore	Brotby W. Krag
Titolo	Information security governance [[electronic resource]] : a practical development and implementation approach / / Krag Brotby
Pubbl/distr/stampa	Hoboken, N.J., : John Wiley & Sons, c2009
ISBN	1-118-58551-8 1-282-13756-5 9786612137563 0-470-47601-X 0-470-47600-1
Descrizione fisica	1 online resource (207 p.)
Collana	Wiley series in systems engineering and management
Disciplina	658.4 658.4/78 658.472 658.478
Soggetti	Data protection Computer security - Management Information technology - Security measures Electronic books.
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	INFORMATION SECURITY GOVERNANCE; Contents; Acknowledgments; Introduction; 1. Governance Overview-How Do We Do It? What Do We Get Out of It?; 1.1 What Is It?; 1.2 Back to Basics; 1.3 Origins of Governance; 1.4 Governance Definition; 1.5 Information Security Governance; 1.6 Six Outcomes of Effective Security Governance; 1.7 Defining Information, Data, Knowledge; 1.8 Value of Information; 2. Why Governance?; 2.1 Benefits of Good Governance; 2.1.1 Aligning Security with Business Objectives; 2.1.2 Providing the Structure and Framework to Optimize Allocations of Limited Resources 2.1.3 Providing Assurance that Critical Decisions are Not Based on Faulty Information2.1.4 Ensuring Accountability for Safeguarding Critical Assets; 2.1.5 Increasing Trust of Customers and Stakeholders;

2.1.6 Increasing the Company's Worth; 2.1.7 Reducing Liability for Information Inaccuracy or Lack of Due Care in Protection; 2.1.8 Increasing Predictability and Reducing Uncertainty of Business Operations; 2.2 A Management Problem; 3. Legal and Regulatory Requirements; 3.1 Security Governance and Regulation; 4. Roles and Responsibilities; 4.1 The Board of Directors; 4.2 Executive Management 4.3 Security Steering Committee4.4 The CISO; 5. Strategic Metrics; 5.1 Governance Objectives; 5.1.1 Strategic Direction; 5.1.2 Ensuring Objectives are Achieved; 5.1.3 Risks Managed Appropriately; 5.1.4 Verifying that Resources are Used Responsibly; 6. Information Security Outcomes; 6.1 Defining Outcomes; 6.1.1 Strategic Alignment-Aligning Security Activities in Support of Organizational Objectives; 6.1.2 Risk Management-Executing Appropriate Measures to Manage Risks and Potential Impacts to an Acceptable Level
6.1.3 Business Process Assurance/Convergence-Integrating All Relevant Assurance Processes to Improve Overall Security and Efficiency6.1.4 Value Delivery-Optimizing Investments in Support of Organizational Objectives; 6.1.5 Resource Management-Using Organizational Resources Efficiently and Effectively; 6.1.6 Performance Measurement-Monitoring and Reporting on Security Processes to Ensure that Objectives are Achieved; 7. Security Governance Objectives; 7.1 Security Architecture; 7.1.1 Managing Complexity; 7.1.2 Providing a Framework and Road Map
7.1.3 Simplicity and Clarity through Layering and Modularization7.1.4 Business Focus Beyond the Technical Domain; 7.1.5 Objectives of Information Security Architectures; 7.1.6 SABSA Framework for Security Service Management; 7.1.7 SABSA Development Process; 7.1.8 SABSA Life Cycle; 7.1.9 SABSA Attributes; 7.2 CobiT; 7.3 Capability Maturity Model; 7.4 ISO/IEC 27001/27002; 7.4.1 ISO 27001; 7.4.2 ISO 27002; 7.5 Other Approaches; 7.5.1 National Cybersecurity Task Force, Information Security Governance: A Call to Action; 8. Risk Management Objectives; 8.1 Risk Management Responsibilities
8.2 Managing Risk Appropriately

Sommario/riassunto

The Growing Imperative Need for Effective Information Security Governance With monotonous regularity, headlines announce ever more spectacular failures of information security and mounting losses. The succession of corporate debacles and dramatic control failures in recent years underscores the necessity for information security to be tightly integrated into the fabric of every organization. The protection of an organization's most valuable asset information can no longer be relegated to low-level technical personnel, but must be considered an essential element of corporate governance that i