1.	Record Nr.	UNINA9910800115103321
	Autore	Lincke Susan
	Titolo	Information Security Planning : A Practical Approach / / by Susan Lincke
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2024
	ISBN	3-031-43118-9
	Edizione	[2nd ed. 2024.]
	Descrizione fisica	1 online resource (446 pages)
	Disciplina	005.8
	Soggetti	Computer security Data protection Data protection - Law and legislation Business information services Computers - Law and legislation Information technology - Law and legislation Principles and Models of Security Data and Information Security Privacy Business Information Systems Legal Aspects of Computing
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di bibliografia	Includes bibliographical references.
	Nota di contenuto	Part. I. The Problem of Security -- Chapter. 1. Security Awareness: Brave New World -- Chapter. 2. Combatting Fraud -- Chapter. 3. Complying with the PCI DSS Standard -- Part. II. Strategic Security Planning -- Chapter. 4. Managing Risk -- Chapter. 5. Addressing Business Impact Analysis and Business Continuity -- Chapter. 6. Governing: Policy, Maturity Models and Planning -- Part. III. Tactical Security Planning -- Chapter. 7. Designing Information Security -- Chapter. 8. Planning for Network Security -- Chapter. 9. Designing Physical Security -- Chapter. 10. Attending to Information Privacy -- Chapter. 11. Planning for Alternative Networks: Cloud Security and Zero Trust -- Chapter. 12. Organizing Personnel Security -- Part. IV. Planning for Detect, Respond, Recover -- Chapter. 13. Planning for

Sommario/riassunto

This book demonstrates how information security requires a deep understanding of an organization's assets, threats and processes, combined with the technology that can best protect organizational security. It provides step-by-step guidance on how to analyze business processes from a security perspective, while also introducing security concepts and techniques to develop the requirements and design for security technologies. This interdisciplinary book is intended for business and technology audiences, at student or experienced levels. Organizations must first understand the particular threats that an organization may be prone to, including different types of security attacks, social engineering, and fraud incidents, as well as addressing applicable regulation and security standards. This international edition covers Payment Card Industry Data Security Standard (PCI DSS), American security regulation, and European GDPR. Developing a risk profile helps to estimate the potential costs that an organization may be prone to, including how much should be spent on security controls. Security planning then includes designing information security, as well as network and physical security, incident response and metrics. Business continuity considers how a business may respond to the loss of IT service. Optional areas that may be applicable include data privacy, cloud security, zero trust, secure software requirements and lifecycle, governance, introductory forensics, and ethics. This book targets professionals in business, IT, security, software development or risk. This text enables computer science, information technology, or business students to implement a case study for an industry of their choosing.