1. Record Nr. UNINA9911007013903321

Autore	Calder Alan
Titolo	Cyber Resilience : Defence-In-depth Principles
Pubbl/distr/stampa	Ely : , : IT Governance Ltd, , 2023 ©2023
ISBN	9781787784406 1787784401 9781787784390 1787784398
Edizione	[1st ed.]
Descrizione fisica	1 online resource (142 pages)
Disciplina	658.478
Soggetti	Computer security Business enterprises - Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di contenuto	Cover -- Title -- Copyright -- About the Author -- Acknowledgments -- Contents -- Introduction -- Part 1: Security principles -- Chapter 1: The cyber threat landscape -- Chapter 2: Legal and contractual requirements -- Chapter 3: Key terms and concepts -- Chapter 4: Managing the risks -- Chapter 5: Three security pillars -- Chapter 6: Layers of defence in depth -- Chapter 7: Mapping the layers against the Part 2 reference controls -- Chapter 8: Implementation tips -- Part 2: Reference controls -- Chapter 9: Asset management -- Chapter 10: Board-level commitment and involvement -- Chapter 11: Business continuity management -- Chapter 12: Configuration and patch management -- Chapter 13: Continual improvement process -- Chapter 14: Encryption -- Chapter 15: External certification/validation -- Chapter 16: Identity and access control -- Chapter 17: Incident response management -- Chapter 18: Internal audits -- Chapter 19: Malware protection -- Chapter 20: Network and communications security -- Chapter 21: Physical and environmental security -- Chapter 22: Security monitoring -- Chapter 23: Security policies -- Chapter 24: Staff training and awareness -- Chapter 25: Supply chain security -- Chapter 26: System security -- Chapter 27: Vulnerability scanning and

	penetration testing -- GRC International Group PLC resources.
Sommario/riassunto	This book will give you a good understanding of the fundamentals of cyber security and resilience, without tying them to specific standards, frameworks or solutions, and provide an excellent starting point for any cyber resilience implementation project.