

1. Record Nr.	UNINA9910462678003321
Autore	Calder Alan <1957->
Titolo	ISO27001 / ISO27002 : a pocket guide / / Alan Calder
Pubbl/distr/stampa	Ely, Cambridgeshire, United Kingdom : , : IT Governance Publishing, , 2013
ISBN	1-84928-523-3
Edizione	[Second edition.]
Descrizione fisica	1 online resource (78 p.)
Disciplina	78
Soggetti	Computer security Data protection Business enterprises - Computer networks - 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.
Nota di contenuto	Foreword; About the Author; Acknowledgements; contents; Introduction; Risks to information assets; Information Security Management System; Chapter 1: The ISO/IEC 27000 Family of Information Security Standards; ISO/IEC 27001:2013 (ISO27001); ISO/IEC 27002:2013 (ISO27002); ISO/IEC 27003; ISO/IEC 27004; ISO/IEC 27005:2011; ISO/IEC 27006:2011; Definitions; Chapter 2: Background to the Standards; BS7799-2; ISO27001:2005; Correspondence between ISO27001 and ISO27002; Use of the Standards; Chapter 3: Specification vs Code of Practice; Chapter 4: Certification Process; Certification bodies Chapter 5: The ISMS and ISO27001 Definition of information security; The ISMS; Chapter 6: Overview of ISO/IEC 27001:2013; Chapter 7: Overview of ISO/IEC 27002:2013; The security categories; Chapter 8: Documentation and Records; Document control requirements; Contents of the ISMS documentation; Annex A document controls; Chapter 9: Management Responsibility; Management direction; Management-related controls; Requirement for management review; Chapter 10: Process Approach and the PDCA Cycle; PDCA and ISO27001; The PDCA cycle and the clauses of ISO27001; Chapter 11: CONTEXT, Policy and Scope The scoping exercise Legal and regulatory framework; Policy definition;

Policy and business objectives; Chapter 12: Risk Assessment; Link to ISO/IEC 27005; Objectives of risk treatment plans; Risk assessment process; Identify risks (6.1.2.c.1); Threats; Vulnerabilities; Identify risk owners (6.1.2.c.2); Assess the consequences of the risk (6.1.2.d.1); Likelihood (6.1.2.d.2); Levels of risk (6.1.2.d.3); Comparing the risk analysis with the risk criteria (6.1.2.e.1); Prioritise the risks (6.1.2.e.2); Risk treatment plan; Chapter 13: The Statement of Applicability (SoA); SoA and external parties
Controls and Annex A Controls (6.1.3.b); Residual risks; Control objectives; Plan for security incidents; Chapter 14: Implementation; Chapter 15: Check and Act; Monitoring; Auditing; Reviewing; Act - maintain and improve the ISMS; Chapter 16: Management Review; Chapter 17: ISO27001 Annex A; Annex A control areas and controls; Clause A5: Information security policies; Clause A6: Organisation of information security; Clause A7: Human resource security; Clause A8: Asset management; Clause A9: Access control; Clause A10: Cryptography; ITG Resources

Sommario/riassunto

Information is one of your organisation's most important resources. Keeping it secure is therefore vital to your business. This handy pocket guide is an essential overview of two key information security standards that cover the formal requirements (ISO27001:2013) for creating an Information Security Management System (ISMS), and the best-practice recommendations (ISO27002:2013) for those responsible for initiating, implementing or maintaining it.
