

1. Record Nr.	UNINA9910463651603321
Autore	Sutton David (Information security practitioner)
Titolo	Information risk management : a practitioner's guide / / David Sutton
Pubbl/distr/stampa	Wiltshire, England : , : BCS The Chartered Institute for IT, , 2014 ©2014
ISBN	1-78017-265-6 1-78017-266-4
Edizione	[1st edition]
Descrizione fisica	1 online resource (245 p.)
Disciplina	658.4038
Soggetti	Information technology - Management 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	Cover; Copyright; CONTENTS; LIST OF FIGURES AND TABLES; AUTHOR; ACKNOWLEDGMENTS; ABBREVIATIONS; DEFINITIONS, STANDARDS AND GLOSSARY OF TERMS; PREFACE; 1 THE NEED FOR INFORMATION RISK MANAGEMENT; INTRODUCTION; WHAT IS INFORMATION?; THE INFORMATION LIFE CYCLE; WHO SHOULD USE INFORMATION RISK MANAGEMENT?; THE LEGAL FRAMEWORK; THE CONTEXT OF RISK IN THE ORGANISATION; THE BENEFITS OF TAKING ACCOUNT OF INFORMATION RISK; OVERVIEW OF THE INFORMATION RISK MANAGEMENT PROCESS; 2 REVIEW OF INFORMATION SECURITY FUNDAMENTALS; INFORMATION CLASSIFICATION; PLAN, DO, CHECK, ACT 3 THE INFORMATION RISK MANAGEMENT PROGRAMMEGOALS, SCOPE AND OBJECTIVES; ROLES AND RESPONSIBILITIES; GOVERNANCE OF THE RISK MANAGEMENT PROGRAMME; INFORMATION RISK MANAGEMENT CRITERIA; 4 RISK IDENTIFICATION; THE APPROACH TO RISK IDENTIFICATION; IMPACT ASSESSMENT; TYPES OF IMPACT; QUALITATIVE AND QUANTITATIVE ASSESSMENTS; 5 THREAT AND VULNERABILITY ASSESSMENT; CONDUCTING THREAT ASSESSMENTS; CONDUCTING VULNERABILITY ASSESSMENTS; IDENTIFICATION OF EXISTING CONTROLS; 6 RISK ANALYSIS AND RISK EVALUATION; ASSESSMENT OF LIKELIHOOD; RISK ANALYSIS; RISK EVALUATION; 7 RISK TREATMENT STRATEGIC RISK OPTIONSTACTICAL RISK MANAGEMENT CONTROLS;

OPERATIONAL RISK MANAGEMENT CONTROLS; EXAMPLES OF CRITICAL CONTROLS AND CONTROL CATEGORIES; 8 RISK REPORTING AND PRESENTATION; BUSINESS CASES; RISK TREATMENT DECISION-MAKING; RISK TREATMENT PLANNING AND IMPLEMENTATION; BUSINESS CONTINUITY AND DISASTER RECOVERY; 9 COMMUNICATION, CONSULTATION, MONITORING AND REVIEW; COMMUNICATION; CONSULTATION; RISK REVIEWS AND MONITORING; 10 THE CESG IA CERTIFICATION SCHEME; THE CESG IA CERTIFICATION SCHEME; SKILLS FRAMEWORK FOR THE INFORMATION AGE (SFIA); THE IISP INFORMATION SECURITY SKILLS FRAMEWORK
11 HMG SECURITY-RELATED DOCUMENTS
HMG SECURITY POLICY FRAMEWORK; UK GOVERNMENT SECURITY CLASSIFICATIONS; APPENDIX A TAXONOMIES AND DESCRIPTIONS; INFORMATION RISK; TYPICAL IMPACTS OR CONSEQUENCES; APPENDIX B TYPICAL THREATS AND HAZARDS; MALICIOUS INTRUSION (HACKING); ENVIRONMENTAL THREATS; ERRORS AND FAILURES; SOCIAL ENGINEERING; MISUSE AND ABUSE; PHYSICAL THREATS; MALWARE; APPENDIX C TYPICAL VULNERABILITIES; ACCESS CONTROL; POOR PROCEDURES; PHYSICAL AND ENVIRONMENTAL SECURITY; COMMUNICATIONS AND OPERATIONS MANAGEMENT; PEOPLE-RELATED SECURITY FAILURES; APPENDIX D INFORMATION RISK CONTROLS
STRATEGIC CONTROL
TACTICAL CONTROLS; OPERATIONAL CONTROLS; CRITICAL SECURITY CONTROLS VERSION 5.0; ISO/IEC 27001 CONTROLS; NIST SPECIAL PUBLICATION 800-53 REVISION 4; APPENDIX E METHODOLOGIES, GUIDELINES AND TOOLS; METHODOLOGIES; OTHER GUIDELINES AND TOOLS; APPENDIX F TEMPLATES; APPENDIX G HMG CYBER SECURITY GUIDELINES; HMG CYBER ESSENTIALS SCHEME; 10 STEPS TO CYBER SECURITY; APPENDIX H REFERENCES AND FURTHER READING; PRIMARY UK LEGISLATION; GOOD PRACTICE GUIDELINES; OTHER REFERENCE MATERIAL; CESG CERTIFIED PROFESSIONAL SCHEME; OTHER UK GOVERNMENT PUBLICATIONS; RISK MANAGEMENT METHODOLOGIES
NEWS ARTICLES ETC.

Sommario/riassunto

Information risk management (IRM) is about identifying, assessing and prioritising risks to keep information secure and available. This accessible book provides practical guidance to the principles and development of a strategic approach to an IRM programme. The only textbook for the BCS Practitioner Certificate in Information Risk Management.
