1. Record Nr. UNINA9910824268803321

Autore	Sutton David
Titolo	Information risk management : a practitioner's guide / / David Sutton
Pubbl/distr/stampa	England : , : BCS Learning & Development Limited, , [2021] ©2021
ISBN	1-5231-4835-7 1-78017-574-4
Edizione	[2nd ed.]
Descrizione fisica	1 online resource (240 pages)
Disciplina	658.4038
Soggetti	Information technology - Management Risk management
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover -- CONTENTS -- LIST OF FIGURES AND TABLES -- AUTHOR -- OTHER WORKS BY THE AUTHOR -- ACKNOWLEDGEMENTS -- ABBREVIATIONS -- PREFACE -- 1. THE NEED FOR INFORMATION RISK MANAGEMENT -- WHAT IS INFORMATION? -- WHO SHOULD USE INFORMATION RISK MANAGEMENT? -- THE LEGAL FRAMEWORK -- THE CONTEXT OF RISK IN THE ORGANISATION -- HOT TOPICS TO CONSIDER IN INFORMATION RISK MANAGEMENT -- THE BENEFITS OF TAKING ACCOUNT OF INFORMATION RISK -- OVERVIEW OF THE INFORMATION RISK MANAGEMENT PROCESS -- SUMMARY -- 2. REVIEW OF INFORMATION SECURITY FUNDAMENTALS -- INFORMATION CLASSIFICATION -- PLAN-DO-CHECK-ACT -- SUMMARY -- 3. THE INFORMATION RISK MANAGEMENT PROGRAMME -- GOALS, SCOPE AND OBJECTIVES -- ROLES AND RESPONSIBILITIES -- GOVERNANCE OF THE RISK MANAGEMENT PROGRAMME -- INFORMATION RISK MANAGEMENT CRITERIA -- SUMMARY -- 4. RISK IDENTIFICATION -- THE RISK IDENTIFICATION PROCESS -- THE APPROACH TO RISK IDENTIFICATION -- IMPACT ASSESSMENT -- SUMMARY -- 5. THREAT AND VULNERABILITY ASSESSMENT -- CONDUCTING THREAT ASSESSMENTS -- CONDUCTING VULNERABILITY ASSESSMENTS -- IDENTIFICATION OF EXISTING CONTROLS -- SUMMARY -- 6. RISK ANALYSIS AND RISK EVALUATION -- ASSESSMENT OF LIKELIHOOD -- RISK ANALYSIS -- RISK

EVALUATION -- SUMMARY -- 7. RISK TREATMENT -- STRATEGIC RISK OPTIONS -- TACTICAL RISK MANAGEMENT CONTROLS -- OPERATIONAL RISK MANAGEMENT CONTROLS -- EXAMPLES OF CRITICAL CONTROLS AND CONTROL CATEGORIES -- SUMMARY -- 8. RISK REPORTING AND PRESENTATION -- BUSINESS CASES -- RISK TREATMENT DECISION-MAKING -- RISK TREATMENT PLANNING AND IMPLEMENTATION -- BUSINESS CONTINUITY AND DISASTER RECOVERY -- DISASTER RECOVERY FAILOVER TESTING -- SUMMARY -- 9. COMMUNICATION, CONSULTATION, MONITORING AND REVIEW -- SKILLS REQUIRED FOR AN INFORMATION RISK PROGRAMME MANAGER -- COMMUNICATION -- CONSULTATION -- RISK REVIEWS AND MONITORING -- SUMMARY. 10. THE NCSC CERTIFIED PROFESSIONAL SCHEME -- SFIA -- THE CIISEC SKILLS FRAMEWORK -- SUMMARY -- 11. HMG SECURITY-RELATED DOCUMENTS -- HMG SECURITY POLICY FRAMEWORK -- THE NATIONAL SECURITY STRATEGY -- CONTEST, THE UNITED KINGDOM'S STRATEGY FOR COUNTERING TERRORISM -- THE MINIMUM CYBER SECURITY STANDARD -- THE UK CYBER SECURITY STRATEGY 2016-2021 -- UK GOVERNMENT SECURITY CLASSIFICATIONS -- SUMMARY -- 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 CONTROLS -- TACTICAL CONTROLS -- OPERATIONAL CONTROLS -- THE CENTRE FOR INTERNET SECURITY CONTROLS VERSION 8 -- ISO/IEC 27001:2017 CONTROLS -- NIST SPECIAL PUBLICATION 800-53 REVISION 5 -- APPENDIX E - METHODOLOGIES, GUIDELINES AND TOOLS -- METHODOLOGIES -- OTHER GUIDELINES AND TOOLS -- APPENDIX F - TEMPLATES -- APPENDIX G - HMG CYBERSECURITY 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 -- NCSC CERTIFIED PROFESSIONAL SCHEME -- OTHER UK GOVERNMENT PUBLICATIONS -- RISK MANAGEMENT METHODOLOGIES -- UK AND INTERNATIONAL STANDARDS -- APPENDIX I - DEFINITIONS, STANDARDS AND GLOSSARY OF TERMS -- DEFINITIONS AND GLOSSARY OF TERMS -- INFORMATION RISK MANAGEMENT STANDARDS -- INDEX -- Back cover.

Sommario/riassunto

Information risk management (IRM) is about identifying, assessing, prioritising and treating risks to keep information secure and available. This 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.