

CONTENTS

Introduction.....	10
Chapter 1: Risk Management.....	16
Risk management: two phases	17
Enterprise risk management.....	21
Chapter 2: Risk Assessment Methodologies.....	26
Publicly available risk assessment standards	27
Qualitative versus quantitative.....	31
Quantitative risk analysis	32
Qualitative risk analysis – the ISO27001 approach.....	33
Other risk assessment methodologies	37
Chapter 3: Risk Management Objectives.....	42
Risk acceptance or tolerance.....	42
Information security risk management objectives	44
Risk management and PDCA	48
Chapter 4: Roles and Responsibilities.....	54
Senior management commitment	54
The (lead) risk assessor	56
Other roles and responsibilities.....	59
Chapter 5: Risk Assessment Software	64
Gap analysis tools	67
Vulnerability assessment tools.....	67
Penetration testing.....	68
Risk assessment tools.....	69
Risk assessment tool descriptions.....	72
Chapter 6: Information Security Policy and Scoping ..	79
Information security policy.....	79
Scope of the ISMS	83
Chapter 7: The ISO27001 Risk Assessment	91
Overview of the risk assessment process.....	92
Chapter 8: Information Assets	98

Contents

Assets within the scope	98
Grouping of assets	101
Asset dependencies	102
Asset owners	103
Sensitivity classification	104
Are vendors assets?	105
What about duplicate copies and backups?	107
Identification of existing controls	109
Chapter 9: Threats and Vulnerabilities	110
Threats	113
Vulnerabilities	114
Technical vulnerabilities	116
Chapter 10: Impact and Asset Valuation	118
Impacts	118
Defining impact	121
Estimating impact	124
The asset valuation table	127
Business, legal and contractual impact values	130
Reputation damage	131
Chapter 11: Likelihood	135
Risk analysis	135
Information to support assessments	138
Chapter 12: Risk Level	140
The risk scale	140
Boundary calculations	143
Mid-point calculations	145
Chapter 13: Risk Treatment and the Selection of Controls	147
Types of controls	148
Risk assessment and existing controls	154
Residual risk	155
Risk transfer	156
Optimising the solution	157

Contents

Chapter 14: The Statement of Applicability	159
Drafting the Statement of Applicability.....	159
Chapter 15: The Gap Analysis and Risk Treatment Plan	
.....	164
Gap analysis	164
Risk Treatment Plan.....	165
Chapter 16: Repeating and Reviewing the Risk	
Assessment	168
Appendix 1: Carrying out an ISO27001 Risk	
Assessment using vsRisk™.....	171
How the tool actually works	171
Training requirements	173
Start using vsRisk™ for your risk assessment.....	174
Identify the assets.....	174
Identify the risks	176
Assess the risks	178
Identify and evaluate options for the treatment of risks	178
Select control objectives and controls for treatment of the	
risks	179
Appendix 2: ISO27001 Implementation Resources	181
Books by the Same Authors	183
ITG Resources.....	185