

**INFORMATION SECURITY RISK MANAGEMENT FOR ISO 27001/
ISO17799 (SOFT COVER)**

INTRODUCTION	1
CHAPTER 1: RISK MANAGEMENT	7
Risk management: two phases.....	8
Enterprise Risk Management.....	11
CHAPTER 2: RISK ASSESSMENT METHODOLOGIES ..	17
Publicly available risk assessment standards.....	18
Qualitative v quantitative.....	23
Quantitative risk analysis.....	24
Qualitative risk analysis – the ISO27001 approach.....	25
Other risk assessment methodologies.....	28
CHAPTER 3: RISK MANAGEMENT OBJECTIVES	33
Risk acceptance or tolerance.....	33
Information security risk management objectives.....	35
Risk management and PDCA.....	39
CHAPTER 4: ROLES AND RESPONSIBILITIES	45
Senior management commitment.....	45
The risk assessor.....	47
Other roles and responsibilities.....	49
CHAPTER 5: RISK ASSESSMENT SOFTWARE	55
Gap analysis tools.....	57
Vulnerability assessment tools.....	58
Penetration testing.....	59
Risk assessment tools.....	60
Risk assessment tool descriptions.....	62
CHAPTER 6: INFORMATION SECURITY POLICY AND SCOPING	71
Information security policy.....	71
Scope of the ISMS.....	75
CHAPTER 7: THE ISO27001 RISK ASSESSMENT	83
Overview of the risk assessment process.....	84
CHAPTER 8: INFORMATION ASSETS	91
Assets within the scope.....	91
Grouping of assets.....	94
Asset dependencies.....	95
Asset owners.....	96
Sensitivity classification.....	97
Are vendors assets?.....	98
What about duplicate copies and backups?.....	100

BUY ONLINE AT: <http://www.27001.com/products/24>

CHAPTER 9: THREATS AND	
.... VULNERABILITIES.....	103
Threats.....	105
Vulnerabilities.....	107
Technical vulnerabilities.....	108
CHAPTER 10: IMPACT AND ASSET	
.... VALUATION.....	111
Impacts.....	111
Defining impact.....	114
Estimating impact.....	117
The asset valuation table.....	120
Business, legal and contractual impact values.....	122
Reputation damage.....	123
CHAPTER 11: LIKELIHOOD.....	127
Risk analysis.....	127
Information to support assessments.....	130
CHAPTER 12: RISK LEVEL.....	133
The risk scale.....	133
Boundary calculations.....	136
Mid-point calculations.....	138
CHAPTER 13: RISK TREATMENT AND THE SELECTION OF	
CONTROLS	141
Types of controls.....	142
Risk assessment and existing controls.....	147
Residual risk.....	148
Risk transfer.....	149
Optimising the solution.....	150
CHAPTER 14: THE STATEMENT OF APPLICABILITY	153
Drafting the Statement of Applicability.....	153
CHAPTER 15: THE GAP ANALYSIS AND RISK TREATMENT PLAN	
	159
Gap analysis.....	159
Risk Treatment Plan.....	160
CHAPTER 16: REPEATING AND REVIEWING THE RISK ASSESSMENT	
	163
APPENDIX 1: CARRYING OUT AN ISO27001 RISK ASSESSMENT USING	
vsRISK™	167
How the tool actually works.....	167
Training requirements.....	169
Start using vsRisk™ for your risk assessment.....	170

BUY ONLINE AT: <http://www.27001.com/products/24>

Identify the assets.....	170
Identify the risks.....	172
Assess the risks.....	174
Identify and evaluate options for the treatment of risks.....	174
Select control objectives and controls for treatment of the risks....	174
APPENDIX 2: ISO27001 IMPLEMENTATION RESOURCES..	177
INDEX.....	181
TABLE OF ISO27001 CLAUSES.....	185