
CONTENTS

INTRODUCTION: EMBRACING ENTERPRISE RISK MANAGEMENT: PRACTICAL APPROACHES FOR GETTING STARTED	1
Overview and the Question of 'Where to Start?'	1
Keys to Success	2
Theme 1. Support From the Top Is a Necessity	2
Theme 2. Build ERM Using Incremental Steps	3
Theme 3. Focus Initially on a Small Number of Top Risks	4
Theme 4. Leverage Existing Resources	5
Theme 5. Build on Existing Risk Management Activities	5
Theme 6. Embed ERM Into the Business Fabric of the Organisation	5
Theme 7. Provide Ongoing ERM Updates and Continuing Education for Directors and Senior Management	6
Initial Action Steps and Objectives	6
Step 1. Seek Board and Senior Management Leadership, Involvement and Oversight	8
Step 2. Select a Strong Leader to Drive the ERM Initiative	8
Step 3. Establish a Management Risk Committee or Working Group	9
Step 4. Conduct the Initial Enterprise-wide Risk Assessment and Develop an Action Plan	10
Step 5. Inventory the Existing Risk Management Practices	11
Step 6. Develop Your Initial Risk Reporting	13
Step 7. Develop the Next Phase of Action Plans and Ongoing Communications	14
Continuing ERM Implementation	15
Chapter Summary	16
Where to Start: Draft Action Plan for an ERM Initiative	16

1	COMPELLING REASONS FOR ENTERPRISE RISK MANAGEMENT	21
	The Evolution of the COSO Internal Control: Integrated Framework to the COSO ERM Framework	23
2	ENTITY-WIDE RISK ASSESSMENT	25
	Risk Tolerance	26
	Materiality	27
	Objective Setting	31
3	IDENTIFYING RISK: ENTITY-LEVEL VERSUS ACTIVITY-LEVEL	33
	Risk Assessment	38
	Probability	39
	Potential Impact	41
4	RISK MANAGEMENT	45
	Control Maturity	47
	Residual Risk	48
5	ACTIVITY-LEVEL RISK ASSESSMENT	51
	Understanding the Approach: Financial Reporting	51
	Workshop Prerequisites	52
	Risk Factor Rating System	53
	Risk Factor Scale	54
	Weighting of Risk Factors	54
	Activity-Level Risk Factor Rating Table Guidelines	57
	Activity-Level Inherent and Fraud Risks	59
6	UNDERSTANDING AND COMMUNICATING RISK APPETITE	61
	Enterprise Risk Management and Decision Making	62
	Develop Risk Appetite	62
	Communicate Risk Appetite	62

Monitor and Update Risk Appetite	62
Can it Be Done?	63
Overview	64
Risk Appetite Is an Integral Part of Enterprise Risk Management	64
Considerations Affecting Risk Appetite	64
Steps in Adopting Risk Appetite	66
Risk Appetite Statements	66
Characteristics of Effective Risk Appetite Statements	67
Reluctance to Embrace Risk Appetite	68
Risk Appetites Are Not All the Same	68
Examples of Risk Appetite Statements	69
Risk Appetite and Risk Tolerance	71
Linking Risk Appetite and Risk Tolerance	72
Examples of Risk Tolerance Statements	74
Developing Risk Appetite	75
Facilitated Discussions	75
Discussions Related to Objectives and Strategies	76
Development of Performance Models	78
Communicating Risk Appetite	78
Broad Risk Appetite Statement	79
Risks Related to Organisational Objectives	79
Categories of Risk	80
Risk Appetite Cascades Through the Organisation	81
Monitoring and Updating Risk Appetite	82
Creating a Culture	82

Roles	83
Summary of Risk Appetite Considerations	86
EPILOGUE	89
REFERENCES	91
APPENDIX A: KEY TERMS	93
APPENDIX B: SAMPLE RISK LIBRARY	95
APPENDIX C: SAMPLE HEAT MAPS	97
APPENDIX D: SAMPLE CONTROL MATURITY MODELS	103
APPENDIX E: SAMPLE COMPANY MODEL MAPPED TO ENTITY-WIDE RISK LIBRARY	107
APPENDIX F: EXAMPLES OF RISK ASSESSMENT REPORTING	115
APPENDIX G: SAMPLE OF A FINANCIAL REPORTING RISK LIBRARY (INHERENT AND FRAUD RISKS)	125
