ISO 31000:2009-11 (E)

Risk management - Principles and guidelines

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Terms and definitions 1

3 Principles 7

4 Framework 8
4.1 General 8
4.2 Mandate and commitment 9
4.3 Design of framework for managing risk 10
4.3.1 Understanding of the organization and its context 10
4.3.2 Establishing risk management policy 10
4.3.3 Accountability 11
4.3.4 Integration into organizational processes 11
4.3.5 Resources 11
4.3.6 Establishing internal communication and reporting mechanisms 12
4.3.7 Establishing external communication and reporting mechanisms 12
4.4 Implementing risk management 12
4.4.1 Implementing the framework for managing risk 12
4.4.2 Implementing the risk management process 13
4.5 Monitoring and review of the framework 13
4.6 Continual improvement of the framework 13

5 Process 13
5.1 General 13
5.2 Communication and consultation 14
5.3 Establishing the context 15
5.3.1 General 15
5.3.2 Establishing the external context 15
5.3.3 Establishing the internal context 15
5.3.4 Establishing the context of the risk management process 16
5.3.5 Defining risk criteria 17
5.4 Risk assessment 17
5.4.1 General 17
5.4.2 Risk identification 17
5.4.3 Risk analysis 18
5.4.4 Risk evaluation 18
5.5 Risk treatment 18
5.5.1 General 18
5.5.2 Selection of risk treatment options 19
5.5.3 Preparing and implementing risk treatment plans 20
5.6 Monitoring and review 20
5.7 Recording the risk management process 21

Annex A (informative) Attributes of enhanced risk management 22

Bibliography 24