ISO 31000:2018-02 (E)

Risk management - Guidelines

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Principles 2

5 Framework 4
5.1 General 4
5.2 Leadership and commitment 5
5.3 Integration 5
5.4 Design 6
5.4.1 Understanding the organization and its context 6
5.4.2 Articulating risk management commitment 6
5.4.3 Assigning organizational roles, authorities, responsibilities and accountabilities 7 5.4.4 Allocating resources 7
5.4.5 Establishing communication and consultation 7
5.5 Implementation 7
5.6 Evaluation 8
5.7 Improvement 8
5.7.1 Adapting 8
5.7.2 Continually improving 8

6 Process 8
6.1 General 8
6.2 Communication and consultation 9
6.3 Scope, context and criteria 10
6.3.1 General 10
6.3.2 Defining the scope 10
6.3.3 External and internal context 10
6.3.4 Defining risk criteria 10
6.4 Risk assessment 11
6.4.1 General 11
6.4.2 Risk identification 11
6.4.3 Risk analysis 12
6.4.4 Risk evaluation 12
6.5 Risk treatment 13
6.5.1 General 13
6.5.2 Selection of risk treatment options 13
6.5.3 Preparing and implementing risk treatment plans 14
6.6 Monitoring and review 14
6.7 Recording and reporting 14

Bibliography 16