DIN ISO 31000:2018-10 (E)

Risk management - Guidelines (ISO 31000:2018)

Contents

Page

National foreword ... **3**

National Annex NA (informative) **Bibliography** ... **4**

Foreword ... **5**

Introduction ... **6**

1 Scope ... **7**

2 Normative references ... **7**

3 Terms and definitions ... **7**

4 Principles ... **8**

5 Framework ... **10**
5.1 General ... 10
5.2 Leadership and commitment ... 11
5.3 Integration ... 11
5.4 Design ... 12
5.4.1 Understanding the organization and its context ... 12
5.4.2 Articulating risk management commitment ... 12
5.4.3 Assigning organizational roles, authorities, responsibilities and accountabilities 13
5.4.4 Allocating resources ... 13
5.4.5 Establishing communication and consultation ... 13
5.5 Implementation ... 13
5.6 Evaluation ... 14
5.7 Improvement ... 14
5.7.1 Adapting ... 14
5.7.2 Continually improving ... 14

6 Process ... **14**
6.1 General ... 14
6.2 Communication and consultation ... 15
6.3 Scope, context and criteria ... 16
6.3.1 General ... 16
6.3.2 Defining the scope ... 16
6.3.3 External and internal context ... 16
6.3.4 Defining risk criteria ... 16
6.4 Risk assessment ... 17
6.4.1 General ... 17
6.4.2 Risk identification ... 17
6.4.3 Risk analysis ... 18
6.4.4 Risk evaluation ... 18
6.5 Risk treatment ... 19
6.5.1 General ... 19
6.5.2 Selection of risk treatment options ... 19
6.5.3 Preparing and implementing risk treatment plans ... 20
6.6 Monitoring and review ... 20
6.7 Recording and reporting ... 20

Bibliography ... **22**