ISO/IEC 27557:2022-11 (E)

Information security, cybersecurity and privacy protection - Application of ISO 31000:2018 for organizational privacy risk management

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Principles of organizational privacy risk management 2

5 Framework 2
5.1 General 2
5.2 Leadership and commitment 2
5.3 Integration 3
5.4 Design 3
5.4.1 Understanding the organization and its context 3
5.4.2 Articulating risk management commitment 3
5.4.3 Assigning organizational roles, authorities, responsibilities and accountabilities 3
5.4.4 Allocating resources 3
5.4.5 Establishing communication and consultation 4
5.5 Implementation 4
5.6 Evaluation 4
5.7 Improvement 4
5.7.1 Adapting 4
5.7.2 Continually improving 4

6 Risk management process 4
6.1 General 4
6.2 Communication and consultation 4
6.3 Scope, context and criteria 5
6.3.1 General 5
6.3.2 Defining the scope 5
6.3.3 External and internal context 5
6.3.4 Defining risk criteria 5
6.4 Risk assessment 6
6.4.1 General 6
6.4.2 Risk identification 6
6.4.3 Risk analysis 9
6.4.4 Risk evaluation 10
6.5 Risk treatment 10
6.5.1 General 10
6.5.2 Selection of risk treatment options 10
6.5.3 Preparing and implementing risk treatment plans 11
6.6 Monitoring and review 11
6.7 Recording and reporting 12

Annex A (informative)PIIprocessingidentification 13

Annex B (informative) Example privacy events and causes 15

Annex C (informative) Privacy impact and consequence examples 17

Annex D (informative) Template showing the severity scale for privacy impacts on individuals 18

Bibliography 19