

ISO/IEC 27554:2024-07 (E)

Information security, cybersecurity and privacy protection - Application of ISO 31000 for assessment of identity-related risk

Contents	Page
Foreword.....	iv
Introduction.....	v
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions.....	1
4 Principles.....	3
5 Framework.....	3
5.1 General.....	3
5.2 Leadership and commitment.....	3
5.3 Integration.....	3
5.4 Design.....	4
5.5 Implementation.....	4
5.6 Evaluation.....	4
5.7 Improvement.....	4
6 Process.....	4
6.1 General.....	4
6.2 Communication and consultation.....	4
6.3 Scope, context and criteria.....	4
6.4 Risk assessment.....	4
6.5 Risk treatment.....	5
6.6 Monitoring and review.....	5
6.7 Recording and reporting.....	5
7 Identity-related context establishment.....	5
7.1 General.....	5
7.2 Actors.....	5
7.2.1 Subscribers/Actors.....	5
7.2.2 Administrators.....	5
7.3 Types of personal data.....	5
7.4 Policies and regulations.....	5
7.5 Service and transaction scope.....	5
8 Identity-related risk assessment.....	6
9 Identity-related risk identification.....	6
10 Identity-related risk analysis.....	7
10.1 General.....	7
10.2 Affected parties.....	7
10.3 Identity theft or fabrication.....	7
10.4 Categories of consequences of identity-related risk.....	8
10.5 Risk impact assessment.....	8
11 Identity-related risk evaluation.....	9
12 Identity-related risk treatment.....	9
Annex A (informative) Standards related to identity-management risk assessment.....	10
Annex B (informative) Risk impact assessment.....	13
Bibliography.....	18