

# ISO/IEC 27554:2024-07 (E)

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

---

<b>Contents</b>	<b>Page</b>
Foreword.....	iv
Introduction.....	v
<b>1 Scope.....</b>	<b>1</b>
<b>2 Normative references.....</b>	<b>1</b>
<b>3 Terms and definitions.....</b>	<b>1</b>
<b>4 Principles.....</b>	<b>3</b>
<b>5 Framework.....</b>	<b>3</b>
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
<b>6 Process.....</b>	<b>4</b>
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
<b>7 Identity-related context establishment.....</b>	<b>5</b>
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
<b>8 Identity-related risk assessment.....</b>	<b>6</b>
<b>9 Identity-related risk identification.....</b>	<b>6</b>
<b>10 Identity-related risk analysis.....</b>	<b>7</b>
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
<b>11 Identity-related risk evaluation.....</b>	<b>9</b>
<b>12 Identity-related risk treatment.....</b>	<b>9</b>
<b>Annex A (informative) Standards related to identity-management risk assessment.....</b>	<b>10</b>
<b>Annex B (informative) Risk impact assessment.....</b>	<b>13</b>
<b>Bibliography.....</b>	<b>18</b>