

# ISO/IEC 27557:2022-11 (E)

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

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>1</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>1</b>
<b>4</b>	<b>Principles of organizational privacy risk management .....</b>	<b>2</b>
<b>5</b>	<b>Framework .....</b>	<b>2</b>
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
<b>6</b>	<b>Risk management process .....</b>	<b>4</b>
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
<b>Annex A (informative)</b>	<b>PII processing identification .....</b>	<b>13</b>
<b>Annex B (informative)</b>	<b>Example privacy events and causes .....</b>	<b>15</b>
<b>Annex C (informative)</b>	<b>Privacy impact and consequence examples .....</b>	<b>17</b>
<b>Annex D (informative)</b>	<b>Template showing the severity scale for privacy impacts on individuals .....</b>	<b>18</b>
<b>Bibliography .....</b>		<b>19</b>