

# ISO/IEC 27035-4:2024-12 (E)

## Information technology - Information security incident management - Part 4: Coordination

---

<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>Overview .....</b>	<b>2</b>
4.1	General .....	2
4.2	Coordination team .....	3
4.3	Principles of coordination .....	4
4.3.1	Timeliness principle .....	4
4.3.2	Roles and responsibilities principle .....	4
4.3.3	Common understanding principle .....	4
4.3.4	Confidentiality principle .....	4
<b>5</b>	<b>Coordinated incident management process .....</b>	<b>4</b>
5.1	Overview .....	4
5.2	Coordinated plan and prepare .....	5
5.3	Coordinated detect and report .....	6
5.4	Coordinated assessment and decision .....	7
5.5	Coordinated respond .....	8
5.6	Coordinated learn lessons .....	9
<b>6</b>	<b>Guidelines for key activities of coordinated incident management .....</b>	<b>10</b>
6.1	Developing coordination policies .....	10
6.2	Establishing communications .....	11
6.3	Threat and event Information sharing .....	11
6.3.1	Overview .....	11
6.3.2	Information types .....	12
6.3.3	Establishing information sharing relationships .....	13
6.3.4	Participating information sharing relationships .....	14
6.4	Conducting coordinated exercises .....	16
6.5	Building trust .....	17
<b>Annex A (informative) Examples of information security incident management coordination .....</b>		<b>19</b>
<b>Bibliography .....</b>		<b>22</b>