

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

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

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Overview	2
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
5	Coordinated incident management process	4
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
6	Guidelines for key activities of coordinated incident management	10
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
Annex A (informative) Examples of information security incident management coordination		19
Bibliography		22