

ISO/IEC 27035-1:2016-11 (E)

Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Overview	2
4.1	Basic concepts and principles	2
4.2	Objectives of incident management	3
4.3	Benefits of a structured approach	5
4.4	Adaptability	6
5	Phases	6
5.1	Overview	6
5.2	Plan and Prepare	9
5.3	Detection and Reporting	9
5.4	Assessment and Decision	10
5.5	Responses	11
5.6	Lessons Learnt	12
Annex A (informative) Relationship to investigative standards		13
Annex B (informative) Examples of information security incidents and their causes		16
Bibliography		21