# ISO/IEC 27035-1:2023-02 (E)

## Information technology - Information security incident management - Part 1: Principles and process

## Contents

Page


**Foreword** ... **iv**

**Introduction** ... **v**

**1 Scope** ... **1**

**2 Normative references** ... **1**

**3 Terms, definitions and abbreviated terms** ... **1**
3.1 Terms and definitions ... 1
3.2 Abbreviated terms ... 3

**4 Overview** ... **3**
4.1 Basic concepts ... 3
4.2 Objectives of incident management ... 4
4.3 Benefits of a structured approach ... 6
4.4 Adaptability ... 7
4.5 Capability ... 7
4.5.1 General ... 7
4.5.2 Policies, plan and process ... 8
4.5.3 Incident management structure ... 8
4.6 Communication ... 10
4.7 Documentation ... 10
4.7.1 General ... 10
4.7.2 Event report ... 10
4.7.3 Incident management log ... 10
4.7.4 Incident report ... 11
4.7.5 Incident register ... 11

**5 Process** ... **11**
5.1 Overview ... 11
5.2 Plan and prepare ... 15
5.3 Detect and report ... 16
5.4 Assess and decide ... 17
5.5 Respond ... 18
5.6 Learn lessons ... 20

**Annex A** (informative) **Relationship to investigative standards** ... **22**

**Annex B** (informative) **Examples of information security incidents and their causes** ... **25**

**Annex C** (informative) **Cross-reference table of ISO/IEC 27001 to the ISO/IEC 27035 series** ... **29**

**Annex D** (informative) **Considerations of situations discovered during the investigation of an incident** ... **31**

**Bibliography** ... **32**