ISO/IEC 27035-2:2023-02 (E)

Information technology - Information security incident management - Part 2: Guidelines to plan and prepare for incident response

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms, definitions and abbreviated terms **2**
3.1 Terms and definitions 2
3.2 Abbreviated terms 2

4 Information security incident management policy **2**
4.1 General 2
4.2 Interested parties 3
4.3 Information security incident management policy content 3

5 Updating of information security policies **5**
5.1 General 5
5.2 Linking of policy documents 6

6 Creating information security incident management plan **6**
6.1 General 6
6.2 Information security incident management plan built on consensus 7
6.3 Interested parties 7
6.4 Information security incident management plan content 8
6.5 Incident classification scale 11
6.6 Incident forms 11
6.7 Documented processes and procedures 12
6.8 Trust and confidence 13
6.9 Handling confidential or sensitive information 14

7 Establishing an incident management capability **14**
7.1 General 14
7.2 Incident management team establishment 14
7.2.1 IMT structure 14
7.2.2 IMT roles and responsibilities 16
7.3 Incident response team establishment 17
7.3.1 IRT structure 17
7.3.2 IRT types and roles 18
7.3.3 IRT staff competencies 19

8 Establishing internal and external relationships **20**
8.1 General 20
8.2 Relationship with other parts of the organization 20
8.3 Relationship with external interested parties 21

9 Defining technical and other support **22**
9.1 General 22
9.2 Technical support 24
9.3 Other support 24

10 Creating information security incident awareness and training **24**

11 Testing the information security incident management plan **25**
11.1 General 25
11.2 Exercise 26

11.2.1 Defining the goal of the exercise 26
11.2.2 Defining the scope of an exercise 27
11.2.3 Conducting an exercise 27
11.3 Incident response capability monitoring 27
11.3.1 Implementing an incident response capability monitoring programme 27
11.3.2 Metrics and governance of incident response capability monitoring 28

12 Learn lessons 28
12.1 General 28
12.2 Identifying areas for improvement 29
12.3 Identifying and making improvements to the information security incident management plan 29
12.4 IMT evaluation 30
12.5 Identifying and making improvements to information security control implementation 30
12.6 Identifying and making improvements to information security risk assessment and management review results 31
12.7 Other improvements 31

Annex A (informative) **Considerations related to legal or regulatory requirements 32**

Annex B (informative) **Example forms for information security events, incidents and vulnerability reports 35**

Annex C (informative) **Example approaches to the categorization, evaluation and prioritization of information security events and incidents 47**

Bibliography 52