ISO/IEC 27035:2011-09 (E)

Information technology - Security techniques - Information security incident management

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Overview 2
4.1 Basic concepts 2
4.2 Objectives 3
4.3 Benefits of a structured approach 4
4.4 Adaptability 5
4.5 Phases 6
4.6 Examples of information security incidents 7

5 Plan and prepare phase 8
5.1 Overview of key activities 8
5.2 Information security incident management policy 10
5.3 Information security incident management integration in other policies 12
5.4 Information security incident management scheme 13
5.5 Establishment of the ISIRT 18
5.6 Technical and other support (including operational support) 19
5.7 Awareness and training 20
5.8 Scheme testing 22

6 Detection and reporting phase 22
6.1 Overview of key activities 22
6.2 Event detection 25
6.3 Event reporting 25

7 Assessment and decision phase 26
7.1 Overview of key activities 26
7.2 Assessment and initial decision by the PoC 28
7.3 Assessment and incident confirmation by the ISIRT 30

8 Responses phase 31
8.1 Overview of key activities 31
8.2 Responses 32

9 Lessons learnt phase 40
9.1 Overview of key activities 40
9.2 Further information security forensic analysis 40
9.3 Identifying the lessons learnt 41
9.4 Identifying and making improvements to information security control implementation 42
9.5 Identifying and making improvements to information security risk assessment and management review results 42
9.6 Identifying and making improvements to the information security incident management scheme 42

9.7 Other improvements 43

Annex B (informative) Examples of information security incidents and their causes 47

Annex C (informative) Example approaches to the categorization and classification of information security events and incidents 50

Annex D (informative) Example information security event, yncident and vulnerability reports and forms 62

Annex E (informative) Legal and regulatory aspects 74

Bibliography 76