DIN EN ISO/IEC 27043:2016-12 (E)

Information technology - Security techniques - Incident investigation principles and processes (ISO/IEC 27043:2015)

Contents

Page

European foreword ... **4**

Foreword ... **5**

Introduction ... **6**

1 Scope ... **10**

2 Normative references ... **10**

3 Terms and definitions ... **10**

4 Symbols and abbreviated terms ... **12**

5 Digital investigations ... **13**
5.1 General principles ... 13
5.2 Legal principles ... 13

6 Digital investigation processes ... **14**
6.1 General overview of the processes ... 14
6.2 Classes of digital investigation processes ... 14

7 Readiness processes ... **16**
7.1 Overview of the readiness processes ... 16
7.2 Scenario definition process ... 18
7.3 Identification of potential digital evidence sources process ... 18
7.4 Planning pre-incident gathering, storage, and handling of data representing potential digital evidence process ... 20
7.5 Planning pre-incident analysis of data representing potential digital evidence process ... 20
7.6 Planning incident detection process ... 20
7.7 Defining system architecture process ... 20
7.8 Implementing system architecture process ... 21
7.9 Implementing pre-incident gathering, storage, and handling of data representing potential digital evidence process ... 21
7.10 Implementing pre-incident analysis of data representing potential digital evidence process ... 21
7.11 Implementing incident detection process ... 21
7.12 Assessment of implementation process ... 22
7.13 Implementation of assessment results process ... 22

8 Initialization processes ... **22**
8.1 Overview of initialization processes ... 22
8.2 Incident detection process ... 23
8.3 First response process ... 24
8.4 Planning process ... 24
8.5 Preparation process ... 24

9 Acquisitive processes ... **25**
9.1 Overview of acquisitive processes ... 25
9.2 Potential digital evidence identification process ... 25
9.3 Potential digital evidence collection process ... 26
9.4 Potential digital evidence acquisition process ... 26
9.5 Potential digital evidence transportation process ... 26
9.6 Potential digital evidence storage and preservation process ... 26

10 Investigative processes **27**
10.1 Overview of investigative processes 27
10.2 Potential digital evidence acquisition process 28
10.3 Potential digital evidence examination and analysis process 28
10.4 Digital evidence interpretation process 28
10.5 Reporting process 28
10.6 Presentation process 29
10.7 Investigation closure process 29
11 Concurrent processes **29**
11.1 Overview of the concurrent processes 29
11.2 Obtaining authorization process 30
11.3 Documentation process 30
11.4 Managing information flow process 30
11.5 Preserving chain of custody process 30
11.6 Preserving digital evidence process 31
11.7 Interaction with physical investigation process 31
12 Digital investigation process model schema **31**
Annex A (informative) **Digital investigation processes: motivation for harmonization** **33**
Bibliography **37**