

# ISO/IEC 27043:2015-03 (E)

## Information technology - Security techniques - Incident investigation principles and processes

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
Introduction .....		vi
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Symbols and abbreviated terms .....	3
5	Digital investigations .....	4
5.1	General principles .....	4
5.2	Legal principles .....	4
6	Digital investigation processes .....	5
6.1	General overview of the processes .....	5
6.2	Classes of digital investigation processes .....	5
7	Readiness processes .....	7
7.1	Overview of the readiness processes .....	7
7.2	Scenario definition process .....	9
7.3	Identification of potential digital evidence sources process .....	9
7.4	Planning pre-incident gathering, storage, and handling of data representing potential digital evidence process .....	11
7.5	Planning pre-incident analysis of data representing potential digital evidence process .....	11
7.6	Planning incident detection process .....	11
7.7	Defining system architecture process .....	11
7.8	Implementing system architecture process .....	12
7.9	Implementing pre-incident gathering, storage, and handling of data representing potential digital evidence process .....	12
7.10	Implementing pre-incident analysis of data representing potential digital evidence process .....	12
7.11	Implementing incident detection process .....	12
7.12	Assessment of implementation process .....	13
7.13	Implementation of assessment results process .....	13
8	Initialization processes .....	13
8.1	Overview of initialization processes .....	13
8.2	Incident detection process .....	14
8.3	First response process .....	15
8.4	Planning process .....	15
8.5	Preparation process .....	15
9	Acquisitive processes .....	16
9.1	Overview of acquisitive processes .....	16
9.2	Potential digital evidence identification process .....	16
9.3	Potential digital evidence collection process .....	17
9.4	Potential digital evidence acquisition process .....	17
9.5	Potential digital evidence transportation process .....	17

9.6	Potential digital evidence storage and preservation process .....	17
10	Investigative processes .....	18
10.1	Overview of investigative processes .....	18
10.2	Potential digital evidence acquisition process .....	19
10.3	Potential digital evidence examination and analysis process .....	19
10.4	Digital evidence interpretation process .....	19
10.5	Reporting process .....	19
10.6	Presentation process .....	20
10.7	Investigation closure process .....	20
11	Concurrent processes .....	20
11.1	Overview of the concurrent processes .....	20
11.2	Obtaining authorization process .....	21
11.3	Documentation process .....	21
11.4	Managing information flow process .....	21
11.5	Preserving chain of custody process .....	21
11.6	Preserving digital evidence process .....	22
11.7	Interaction with physical investigation process .....	22
12	Digital investigation process model schema .....	22
	Annex A (informative) Digital investigation processes: motivation for harmonization .....	24
	Bibliography .....	28