

ISO/IEC 27041:2015-06 (E)

Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method

Contents	Page
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	4
5 Method development and assurance	4
5.1 Overview	4
5.2 General principles	4
5.3 General development and deployment model	4
5.4 Assurance stages	5
5.5 Requirements capture and analysis	6
5.5.1 General principles of requirements	6
5.5.2 Functional Requirements	7
5.5.3 Verification of requirements	7
5.6 Process Design	7
5.6.1 Overview	7
5.6.2 Tool Selection	7
5.6.3 Uncertainty and risk evaluation	7
5.7 Process Implementation	8
5.7.1 Overview	8
5.7.2 Tool choice -- guidance for deployment	8
5.8 Process Verification	8
5.8.1 General principles of verification	8
5.8.2 Verification of processes	9
5.8.3 Verification of tools	9
5.9 Process Validation	9
5.9.1 General principles of validation	9
5.9.2 Comprehensive validation	9
5.9.3 Sufficient validation	9
5.9.4 Fully validated processes	10
5.9.5 Failed validation	10
5.10 Confirmation	10
5.11 Deployment	10
5.11.1 Tool choice	10
5.12 Review and Maintenance	10
6 Assurance Models	11
6.1 Overview	11
6.2 In-house assurance	11
6.3 External assurance	11
6.4 Mixed assurance	11
7 Production of evidence for assurance	11
7.1 Overview	11

7.2	Pre-validation preparation	12
7.3	Producing Evidence of Validation	12
7.4	Maintenance of Validation	12
7.5	Validation of Examinations	12
7.6	Validation of Investigations	13
	Annex A (informative) Examples	14
	Bibliography	18