

DIN EN ISO/IEC 27041:2016-12 (E)

Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method (ISO/IEC 27041:2015)

| Contents | | Page |
|-------------------------|--|-------------|
| European foreword | | 3 |
| Foreword | | 4 |
| Introduction | | 5 |
| 1 | Scope | 9 |
| 2 | Normative references | 9 |
| 3 | Terms and definitions | 9 |
| 4 | Symbols and abbreviated terms | 12 |
| 5 | Method development and assurance | 12 |
| 5.1 | Overview | 12 |
| 5.2 | General principles | 12 |
| 5.3 | General development and deployment model | 12 |
| 5.4 | Assurance stages | 13 |
| 5.5 | Requirements capture and analysis | 14 |
| 5.5.1 | General principles of requirements | 14 |
| 5.5.2 | Functional Requirements | 15 |
| 5.5.3 | Verification of requirements | 15 |
| 5.6 | Process Design | 15 |
| 5.6.1 | Overview | 15 |
| 5.6.2 | Tool Selection | 15 |
| 5.6.3 | Uncertainty and risk evaluation | 15 |
| 5.7 | Process Implementation | 16 |
| 5.7.1 | Overview | 16 |
| 5.7.2 | Tool choice — guidance for deployment | 16 |
| 5.8 | Process Verification | 16 |
| 5.8.1 | General principles of verification | 16 |
| 5.8.2 | Verification of processes | 17 |
| 5.8.3 | Verification of tools | 17 |
| 5.9 | Process Validation | 17 |
| 5.9.1 | General principles of validation | 17 |
| 5.9.2 | Comprehensive validation | 17 |
| 5.9.3 | Sufficient validation | 17 |
| 5.9.4 | Fully validated processes | 18 |
| 5.9.5 | Failed validation | 18 |
| 5.10 | Confirmation | 18 |
| 5.11 | Deployment | 18 |
| 5.11.1 | Tool choice | 18 |
| 5.12 | Review and Maintenance | 18 |
| 6 | Assurance Models | 19 |
| 6.1 | Overview | 19 |
| 6.2 | In-house assurance | 19 |
| 6.3 | External assurance | 19 |
| 6.4 | Mixed assurance | 19 |

7 Production of evidence for assurance **20**
7.1 Overview 20
7.2 Pre-validation preparation 20
7.3 Producing Evidence of Validation 20
7.4 Maintenance of Validation 20
7.5 Validation of Examinations 20
7.6 Validation of Investigations 21
Annex A (informative) Examples **22**
Bibliography **26**