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

*Technologies de l'information — Techniques de sécurité — Directives
sur la façon d'assurer l'aptitude à l'emploi et l'adéquation d'une
méthode d'investigation d'incident*



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

The committee responsible for this document is ISO/IEC JTC 1, *Information technology, SC 27, IT Security techniques*.

Introduction

About this International Standard

This International Standard is concerned with providing assurance that the investigative process used is appropriate for the incident under investigation and the results which are required. It also describes, at an abstract level, the concept of breaking seemingly complex processes into a series of smaller atomic parts, which should aid in the development of simple, yet robust, investigation methods. It should be considered by any person authorising, giving instruction for, managing, or conducting an investigation. It should be applied prior to any investigation, in the context of principles and processes (defined in ISO/IEC 27043:2015) and sound preparation and planning (defined in ISO/IEC 27035-2¹⁾) to ensure the suitability of methods to be applied in the investigative processes described in ISO/IEC 27037:2012 and ISO/IEC 27042:2015.

Relationship to other standards

This International Standard is intended to complement other standards and documents which give guidance on the investigation of, and preparation to investigate, information security incidents. It is not a comprehensive guide, but lays down certain fundamental principles which are intended to ensure that tools, techniques, and methods can be selected appropriately and shown to be fit for purpose should the need arise.

This International Standard also intends to inform decision-makers that need to determine the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyse, and present potential digital evidence. It is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence.

This International Standard describes part of a comprehensive investigative process which includes, but is not limited to, the following topic areas:

- incident management, including preparation and planning for investigations;
- handling of digital evidence;
- use of, and issues caused by, redaction;
- intrusion prevention and detection systems, including information which can be obtained from these systems;
- security of storage, including sanitization of storage;
- ensuring that investigative methods are fit for purpose;
- carrying out analysis and interpretation of digital evidence;
- understanding principles and processes of digital evidence investigations;
- security incident event management, including derivation of evidence from systems involved in security incident event management;
- relationship between electronic discovery and other investigative methods, as well as the use of electronic discovery techniques in other investigations;
- governance of investigations, including forensic investigations.

These topic areas are addressed, in part, by the following ISO/IEC standards:

- ISO/IEC 27037:2012

1) To be published.