

STN	Informačné technológie. Governancia forenzného digitálneho rámca (ISO/IEC 30121:2015).	STN EN ISO/IEC 30121 36 9755
------------	---	--

Information technology - Governance of digital forensic risk framework (ISO/IEC 30121:2015)

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 01/17

Obsahuje: EN ISO/IEC 30121:2016, ISO/IEC 30121:2015

124046

Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, 2017
Podľa zákona č. 264/1999 Z. z. v znení neskorších predpisov sa môžu slovenské technické normy rozmnožovať a rozširovať iba so súhlasom Úradu pre normalizáciu, metrológiu a skúšobníctvo SR.

EUROPEAN STANDARD

EN ISO/IEC 30121

NORME EUROPÉENNE

EUROPÄISCHE NORM

August 2016

ICS 35.080

English Version

**Information technology - Governance of digital forensic
risk framework (ISO/IEC 30121:2015)**

Technologies de l'information - Gouvernance du cadre
de risque forensique numérique (ISO/IEC 30121:2015)

Informationstechnik - Leitfaden für die
Betriebsführung digitaler Forensik (ISO/IEC
30121:2015)

This European Standard was approved by CEN on 19 June 2016.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents	Page
European foreword.....	3

European foreword

The text of ISO/IEC 30121:2015 has been prepared by Technical Committee ISO/IEC JTC 1 “Information technology” of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and has been taken over as EN ISO/IEC 30121:2016.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2017, and conflicting national standards shall be withdrawn at the latest by February 2017.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 30121:2015 has been approved by CEN as EN ISO/IEC 30121:2016 without any modification.

Information technology — Governance of digital forensic risk framework

*Technologies de l'information — Gouvernance du cadre de risque
forensique numérique*



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 Principles	2
4.1 Responsibility.....	2
4.2 Strategy.....	2
4.3 Acquisition.....	2
4.4 Performance.....	2
4.5 Conformance.....	2
4.6 Human behaviour.....	2
5 The framework	2
5.1 Stakeholder mandate.....	2
5.2 Establishment.....	2
5.3 Evaluate.....	2
5.4 Direct.....	3
5.5 Monitor.....	3
6 Processes	3
6.1 Archival strategy.....	3
6.2 Discovery strategy.....	3
6.3 Disclosure strategy.....	3
6.4 Digital forensic capability strategy.....	3
6.5 Risk compliance strategy.....	3
7 Metrics	4
7.1 General.....	4
7.2 Key goal indicators.....	4
7.3 Key performance indicators.....	4
7.4 Key business indicators.....	4
Annex A (informative) International Standard overview	5
Bibliography	6

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*, Subcommittee SC 40, *IT Service Management and IT Governance*.

Introduction

Organizations of any kind face both internal and external factors and influences that can lead to the occurrence of legal actions and placement of demands on the Information Technology (IT) and related Information Systems (IS) to disclose digital evidence. The occurrence of legal action may be the result of an uncertain, unplanned, or unexpected event or it may occur as a planned course of action against employees, competitors, or service suppliers. Whether a risk is significant or not will depend on the level of risk and the organization's risk attitude. Its risk attitude will be reflected in its risk criteria. Because it is almost certain that digital evidence will be discovered and, therefore, be subject to legal disclosure, organizations should plan and develop capability to deal with such legal actions before they occur.

This International Standard is about the prudent strategic preparation for digital investigation of an organization. Forensic readiness assures that an organization has made the appropriate and relevant strategic preparation for accepting potential events of an evidential nature. Actions may occur as the result of inevitable security breaches, fraud, and reputation assertion. In every situation, IT should be strategically deployed to maximise the effectiveness of evidential availability, accessibility, and cost efficiency.

The responsibility of the Governing body is to provide strategic direction in all matters of relevance to the organization. The Governing body is informed by principles of best practice that provide general guidance on matters of certainty and compliance. These principles may come from legal mandates, standards, or social and cultural imperatives. In this International Standard, the principles come from ISO/IEC 38500 for the guidance of best practice for the governance of IT ([Clause 4](#)).

Principles require implementation. The tasks of governance are to evaluate proposals and plans, to monitor performance and conformance, and to direct strategy and policies. The stakeholders of an organization may provide the mandate for governance and the Governing body has the ultimate ownership of risk. A framework for the governance of digital forensic risk is established by the owners of risk taking appropriate actions to assure the strategic direction of the organization. Hence, the strategic objective is to implement the principles and to assure adequate preparation for digital investigation ([Clause 5](#)).

The framework requires strategic processes to deliver direction to executives and top managers. The strategic processes are selected to assure adequate scope and are principally archival, discovery, disclosure, capability, and risk criteria compliance ([Clause 6](#)).

The goals derived from the principles are measurable through Key Goal Indicators (KGIs), the strategic objectives derived from the strategies are measurable through the Key Performance Indicators (KPIs), and the variation between the KGIs and the KPIs measures is an indication of the organization's business performance (KBIs) ([Clause 7](#)).

This International Standard should be used in conjunction with the vocabulary contained in ISO Guide 73:2009; ISO/IEC 35802, *Information technology — Governance of IT framework and model*; and ISO/IEC 38500, *Information technology — Governance of IT for the organization*.

Information technology — Governance of digital forensic risk framework

1 Scope

This International Standard provides a framework for Governing bodies of organizations (including owners, board members, directors, partners, senior executives, or similar) on the best way to prepare an organization for digital investigations before they occur. This International Standard applies to the development of strategic processes (and decisions) relating to the retention, availability, access, and cost effectiveness of digital evidence disclosure. This International Standard is applicable to all types and sizes of organizations.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 38500, *Information technology — Governance of IT for the organization*

ISO Guide 73:2009, *Risk management — Vocabulary*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN