SLOVENSKI STANDARD
oSIST prEN 18228:2026

01-julij-2026

Obvladovanje tveganj AI

AI Risk Management

Risikomanagement für Künstliche Intelligenz

Gestion des risques liés à l'IA

Ta slovenski standard je istoveten z: **prEN 18228**

ICS:

35.240.01	Uporabniške rešitve informacijske tehnike in tehnologije na splošno	Application of information technology in general

oSIST prEN 18228:2026 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 18228

May 2026

ICS 35.240.01

English version

AI Risk Management

Gestion des risques liés à l'IA

Risikomanagement für Künstliche Intelligenz

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/CLC/JTC 21.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN and CENELEC 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 and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Ref. No. prEN 18228:2026 E

Contents

Page

European foreword

This document (prEN 18228:2026) has been prepared by the Joint Technical Committee CEN-CENELEC/ JTC 21 “Artificial Intelligence”, the secretariat of which is held by DS.

This document is currently submitted to the CEN Enquiry.

This document has been prepared under a standardization request addressed to CEN-CENELEC by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

For the relationship with EU Legislation, see informative Annex ZA, which is an integral part of this document.

Introduction

This document was developed primarily for *providers* of *AI systems* on the basis of established principles of product-safety-focused *risk management*, in support of EU AI Act regulatory purposes.

The requirements contained in this document provides a framework to systematically identify and mitigate the *risks* associated with the use of *AI systems* throughout their *life cycle*. This *risk management* system is a continuous and iterative *process*, planned and run throughout the entire *life cycle* of an *AI system*, requiring regular systematic review and updating.

This document contains *processes* for managing *risks* to health, safety and *fundamental rights* which are associated with *AI systems*. *Risks* can also be related to damage to property (for example objects, data, other equipment), the environment and *critical infrastructure* when they can impact the health, safety and *fundamental rights* of *persons*.

For the purposes of this document, the concept of *risk* has two key components:

— the probability of occurrence of *harm*; and

— the *severity* of that *harm*.

The *provider* reduces *risks* and makes evaluations of the acceptability of the *residual risks*. The *provider* takes into account the generally acknowledged *state of the art*, in order to determine the suitability of an *AI system* to be placed on the market for its *intended purpose*.

This document provides a *process* for:

— *risk* acceptability criteria establishment in the context of the *AI system intended purpose* and under conditions of *reasonably foreseeable misuse*;

— determining *hazards* associated with the *AI system*, analysing and evaluating the *risks* associated with these *hazards*;

— finally, controlling and mitigating these *risks* and monitoring the effectiveness of the controls throughout the *life cycle* of the *AI system*.

For any particular *AI system*, other standards or regulations can require the application of specific methods for managing *risk*.

1 Scope

This document specifies requirements and provides guidance for *risk management* of *AI systems*. It specifies terminology, principles and a *process* for *risk management*.

The *process* described in this document intends to assist *providers* of *AI systems* to identify the *hazards* associated with the *AI systems*, to estimate and evaluate the associated *risks*, to control these *risks*, and to monitor the effectiveness of the controls. The *process* described in this document applies to *risks* to health, safety and *fundamental rights* associated with an *AI system*. The *process* described in this document is applied throughout the *life cycle* of the *AI system*.

This document requires *providers* to establish objective criteria for *risk* acceptability but does not specify *acceptable risk* levels.

This document is intended for use by organizations providing *AI systems*, regardless of their size, nature or location. This document is not intended for managing *risk* faced by organizations. This document is intended to support the organization in meeting applicable regulatory requirements.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

prEN 18229-1:20XX, *AI trustworthiness framework — Part 1: Logging, transparency and human oversight*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp/

— IEC Electropedia: available at https://www.electropedia.org/

3.1 Terms relating to the AI Act

3.1.1
AI system
Artificial intelligence system
machine-based system that is designed to operate with varying levels of autonomy and that can exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments

[SOURCE: REGULATION (EU) 2024/1689, Article 3(1), modified — removed “means a”, “may” replaced by “can”]

3.1.2
intended purpose
use for which an *AI system* (3.3.1) is intended by the *provider* (3.1.5), including the specific context and conditions of use, as specified in the information supplied by the *provider* (3.1.5) in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation

Note 1 to entry: Technical documentation is not *accompanying documentation* (3.2.1). Information on technical documentation can be found in Article 11 of the EU AI Act [1].

[SOURCE: REGULATION (EU) 2024/1689, Article 3(12), modified — removed “means the”, note to entry added]

3.1.3
reasonably foreseeable misuse
use of an *AI system* (3.1.1) in a way that is not in accordance with its *intended purpose* (3.1.2), but which can result from reasonably foreseeable human behaviour or interaction with other systems, including other *AI systems* (3.1.1)

Note 1 to entry: Reasonably foreseeable human behaviour includes the behaviour of all types of relevant *users* (3.5.7).

Note 2 to entry: Reasonably foreseeable misuse can be intentional or unintentional.

[SOURCE: AI Act Art. 3(13), modified — removed “means the”, “may” replaced by “can”, notes 1 and 2 to entry added]

3.1.4
performance
<AI system> ability of an *AI system* (3.1.1) to achieve its *intended purpose* (3.1.2)

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance is evaluated in the context of use of the *AI system* (3.1.1). The use conditions under which performance is evaluated can result in significant performance outcomes and which can be explicitly stated

[SOURCE: REGULATION (EU) 2024/1689, Article 3(18), modified — removed “the”]

3.1.5
provider
natural or legal person, public authority, agency or other body that develops an *AI system* (3.1.1) or a general purpose AI model or that has an *AI system* (3.1.1) or a general-purpose AI model developed and places it on the market or puts the *AI system* (3.1.1) into service under its own name or trademark, whether for payment or free of charge

Note 1 to entry: A distributor, importer, *deployer* (3.1.6) or other third party can be considered a provider of an *AI system* (3.1.1) in certain circumstances.

[SOURCE: REGULATION (EU) 2024/1689, Article 3(3), modified — removed “means a”, note to entry added]

3.1.6
deployer
natural or legal person, public authority, agency or other body using an *AI system* (3.1.1) under its authority except where the *AI system* (3.1.1) is used in the course of a personal non-professional activity

[SOURCE: REGULATION (EU) 2024/1689, Article 3(4), modified — removed “means a”]

3.1.7
post-market monitoring system
activities carried out by *providers* (3.1.5) of *AI systems* (3.1.1) to collect and review experience gained from the use of *AI systems* (3.1.1) they place on the market or put into service for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions

Note 1 to entry: For the purpose of this document, activities shall mean all activities.

[SOURCE: REGULATION (EU) 2024/1689, Article 3(25), modified — removed “means all”, added note to entry]

3.1.8
placing on the market
first making available of an *AI system* (3.1.1) on the Union market

Note 1 to entry: See *making available on the market* (3.1.9).

Note 2 to entry: Further information on this concept can be found in the Blue Guide [2], section 2.

[SOURCE: REGULATION (EU) 2024/1689, Article 3(9), modified — removed “means the”, added notes to entry]

3.1.9
making available on the market
supply of an *AI system* (3.1.1) for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge

[SOURCE: REGULATION (EU) 2024/1689, Article 3(10), modified — removed “means the”]

3.1.10
putting into service
supply of an *AI system* (3.1.1) for first use directly to the *deployer* (3.1.6) or for own use in the Union for its *intended purpose* (3.1.2)

Note 1 to entry: Further information on this concept can be found in the Blue Guide [2], section 2.

[SOURCE: REGULATION (EU) 2024/1689, Article 3(11), modified — removed “means the”, added note to entry]

3.1.11
serious incident
incident or malfunctioning of an *AI system* (3.1.1) that directly or indirectly leads to any of the following:

a) the death of a *person* (3.5.9) or serious *harm* (3.6.3) to a *person* (3.5.9)'s health;

b) a serious and irreversible disruption of the management or operation of *critical infrastructure* (3.6.18);

c) the infringement of obligations under applicable regulatory requirements intended to protect *fundamental rights* (3.5.1);

d) serious *harm* (3.6.3) to property or the environment

[SOURCE: REGULATION (EU) 2024/1689, Article 3(49), modified — removed "means an"]

3.1.12
subject
natural person who participates in testing in real-world conditions

Note 1 to entry: Participating in *testing* (3.3.1) can require *informed consent* (3.5.12) of subjects.

[SOURCE: REGULATION (EU) 2024/1689, Article 3(58), modified — removed "for the purpose of real-world testing, means a", note to entry added]

3.1.13
real-world conditions testing
temporary *testing* (3.3.1) of an *AI system* (3.1.1) for its *intended purpose* (3.1.2) in its intended context of use or deployment environment outside a laboratory or otherwise simulated environment

Note 1 to entry: Assessing and verifying conformity of the *AI system* (3.1.1) with the requirements of this document includes that the overall *residual risk* (3.6.6) of the *AI system* (3.1.1) is acceptable in accordance with its *intended purpose* (3.1.2) and *reasonably foreseeable misuse* (3.1.3).

Note 2 to entry: *Real-world conditions testing* can pertain to technical and non-technical aspects, including *performance* (3.1.4) *verification* (3.2.9) or usability study.

Note 3 to entry: *Real-world conditions testing* can require the participation of *subjects* (3.1.12).

[SOURCE: REGULATION (EU) 2024/1689, Article 3(57), modified — removed "means the", replaced "in real-world conditions" with "in its intended context of use or deployment environment", removed text after "with a view" for substitutability and because it contains references to specific parts of (EU) 2024/1689]

3.2 Terms related to the risk management system

3.2.1
accompanying documentation
materials accompanying an *AI system* (3.1.1) and containing information for the *user* (3.5.7) or those accountable for the use, maintenance, decommissioning and disposal of the *AI system* (3.1.1)

Note 1 to entry: The accompanying documentation can consist of the instructions for use, technical description, installation manual, quick reference guide, etc.

Note 2 to entry: The accompanying documentation is not necessarily a written or printed document but can involve auditory, visual, or tactile materials and multiple media types.

Note 3 to entry: Materials include information relevant for the protection of health, safety and *fundamental rights*, where each is applicable.

3.2.2
objective evidence
data supporting the existence or verity of something

Note 1 to entry: Objective evidence can be obtained through observation, measurement, test or by other means.

[SOURCE: ISO 9000:2015, 3.8.3, modified — note 2 to entry deleted]

3.2.3
procedure
specified way to carry out an activity or a *process* (3.2.4)

Note 1 to entry: Procedures can be documented or not.

[SOURCE: ISO 9000:2015, 3.4.5]

3.2.4
process
set of interrelated or interacting activities that use inputs to deliver an intended result

Note 1 to entry: Whether the intended result of a process is called output, product or service depends on the context of the reference.

Note 2 to entry: Inputs to a process are generally the outputs of other processes and outputs of a process are generally the inputs to other processes.

Note 3 to entry: Two or more interrelated and interacting processes in series can also be referred to as a process.

[SOURCE: ISO 9000:2015, 3.4.1, modified — notes 4-6 to entry deleted]

3.2.5
record
document stating results achieved or providing evidence of activities performed

Note 1 to entry: Records can be used, for example, to formalize traceability and to provide evidence of verification, preventive action and corrective action.

3.2.6
risk management
systematic and continuous application of management policies, *procedures* (3.2.3) and practices to the tasks of analysing, evaluating, controlling and monitoring *risk* (3.6.5) throughout the entire *life cycle* (3.4.1) of an *AI system* (3.1.1)

[SOURCE: ISO/IEC Guide 63:2019, 3.15, modified — reference to life cycle of the AI system added]

3.2.7
state of the art
generally acknowledged state of the art
developed stage of technical capability at a given time as regards products, *processes* (3.2.4) and services, based on the relevant consolidated findings of science, technology and experience

Note 1 to entry: The state of the art embodies what is currently and generally accepted as good practice in technology. The state of the art does not necessarily imply the latest scientific research still in an experimental stage or with insufficient technological maturity.

[SOURCE: ISO/IEC Guide 2:2004, 1.4, modified — note to entry added]

3.2.8
top management
person (3.5.9) or group of people who directs and controls a *provider* (3.1.5) at the highest level

[SOURCE: ISO 9000:2015, 3.1.1, modified — “an organization” replaced by “a provider”, notes to entry deleted]

3.2.9
verification
confirmation, through the provision of *objective evidence* (3.2.2), that specified requirements have been fulfilled

Note 1 to entry: The *objective evidence* (3.2.2) needed for a verification can be the result of an inspection, *testing* (3.3.1) or of other forms of determination such as performing alternative calculations or reviewing documents.

Note 2 to entry: The activities carried out for verification are sometimes called a qualification *process* (3.2.4).

Note 3 to entry: The word “verified” is used to designate the corresponding status.

[SOURCE: ISO 9000:2015, 3.8.12, modified — note 1 to entry modified]

3.2.10
international norms of behaviour
expectations of socially responsible organizational behaviour derived from customary international law, generally accepted principles of international law, or intergovernmental agreements that are universally or nearly universally recognized

Note 1 to entry: Intergovernmental agreements include treaties and conventions.

Note 2 to entry: Although customary international law, generally accepted principles of international law and intergovernmental agreements are directed primarily at states, they express goals and principles to which all organizations can aspire.

Note 3 to entry: International norms of behaviour evolve over time.

[SOURCE: ISO 26000:2010, 2.11]

3.2.11
risk management file
set of *records* (3.2.5) and other documents that are produced by *risk management* (3.2.6)

[SOURCE: EN ISO 14971:2019, 3.25]

3.3 Terms relating to testing

3.3.1
testing
set of activities conducted to facilitate discovery and evaluation of properties of *test items* (3.3.2)

Note 1 to entry: Testing activities include planning, preparation, execution, reporting, and management activities, insofar as they are directed towards testing.

[SOURCE: ISO/IEC/IEEE 29119-1:2022, 3.131]

3.3.2
test item
test object
work product to be tested

EXAMPLE Software component, system, requirements document, design specification, *user* (3.5.7) guide.

[SOURCE: ISO/IEC/IEEE 29119-1:2022, 3.107]

3.3.3
test objective
reason for performing *testing* (3.3.1)

[SOURCE: ISO/IEC/IEEE 29119-1:2022, 3.114, modified — EXAMPLE removed]

3.3.4
test completion report
test summary report
report that provides a summary of the *testing* (3.3.1) that was performed

Note 1 to entry: The report may contain statistical analysis.

[SOURCE: ISO/IEC/IEEE 29119-1:2022, 3.87, modified — added note to entry]

3.3.5
test plan
detailed description of *test objectives* to be achieved and the means and schedule for achieving them, organized to coordinate *testing* (3.3.1) activities for some *test item* (3.3.2) or set of *test items* (3.3.2)

Note 1 to entry: A *test plan* is a written document included in the *risk management file* (3.2.11)

[SOURCE: ISO/IEC/IEEE 29119-1:2022, 3.117, modified — note to entry modified]

3.3.6
test monitoring and control process
test management *process* (3.2.4) that aims to ensure that *testing* (3.3.1) is performed in line with a *test plan* (3.3.5) and with organizational test specifications

[SOURCE: ISO/IEC/IEEE 29119-1:2022, 3.113]

3.4 Terms related to the AI system

3.4.1
life cycle
evolution of a system, product, service, project or other human-made entity, from conception through retirement

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.23]

3.4.2
pre-market
every *life cycle* (3.4.1) stage before *putting into service* (3.1.10) or *placing on the market* (3.1.8) the *AI system* (3.1.1)

Note 1 to entry: *Pre-market* can include *real-world conditions testing* (3.3.4).

3.4.3
post-market
every *life cycle* (3.4.1) stage after *putting into service* (3.1.10) or *placing on the market* (3.1.8) the *AI system* (3.1.1)

EXAMPLE Installation, use, maintenance, repair, modifications and decommissioning.