Role of ISO/IEC 25870

Data elements for reporting AI system incidents

Michael Garris

Today's Workshop & ISO/IEC 25870

Workshop (Broad)	**ISO/IEC 25870** (Narrow)
AI incident management (approaches & guidance)	Data elements for reporting AI system incidents
Definitions & lifecycles	One ISO Definition & ISO/IEC AI lifecycle
Emerging AI incident types	Harm-related incidents

ISO/IEC 25870 – Title & SCOPE

Title:

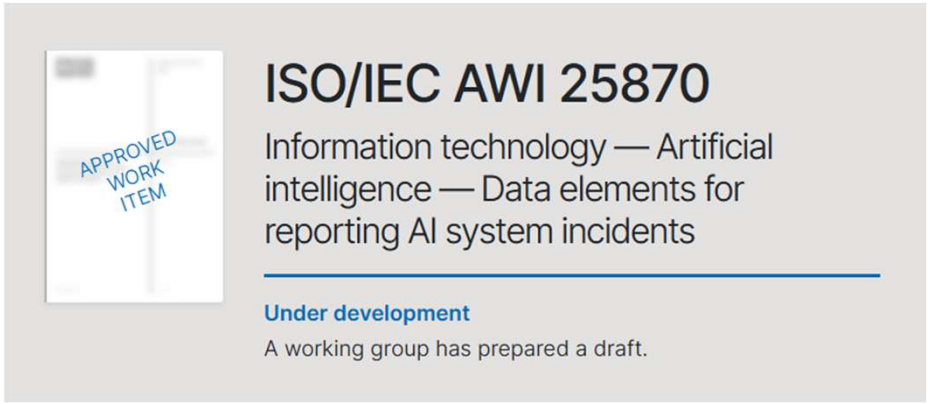
Artificial intelligence — Data elements for reporting AI system incidents

Scope:

This document provides data elements for reporting artificial intelligence (AI) system incidents.

This document is applicable to any organization, regardless of size, type, or nature, that provides or uses products or services that utilize AI systems.

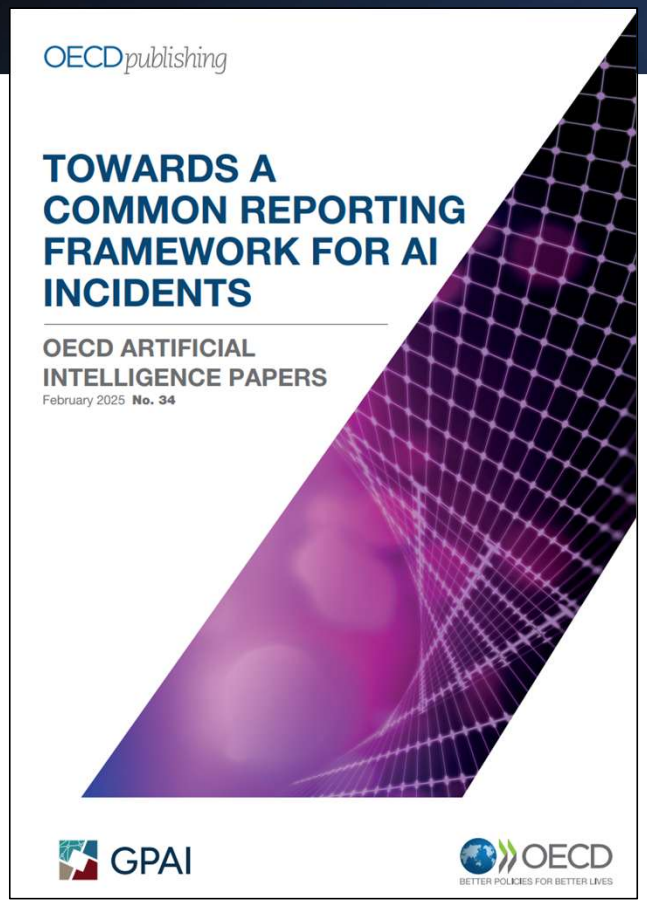
ISO/IEC 25870 – Details



https://www.iso.org/standard/91804.html

- Draft International Standard
- Project Editor: Michael Garris
- Started: 2025-07-06
- Stage: 20.00 Working Draft
- Target Date: 2027-10-19
- Progress: ***WD*** -> CD -> DIS -> FDIS -> IS

ISO/IEC 25870 – Background

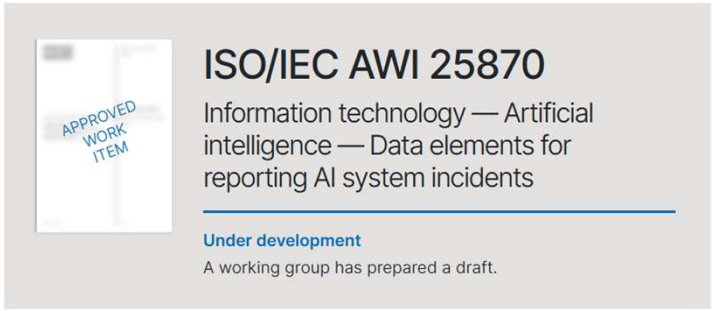


https://www.oecd.org/en/publications/towards-a-common-reporting-framework-for-ai-incidents_f326d4ac-en.html

At ISO/IEC SC42 Plenary – Spring 2025

- OECD presented their framework
  At its core are 29 data elements (Table B.1)
- OECD requested ISO/IEC SC42 turn the framework into an international standard
- ISO/IEC SC42 approved a new work item

ISO/IEC 25870 – Working Draft



https://www.iso.org/standard/91804.html

Transformed OECD framework into ISO/IEC draft standard

- ISO-compliant structure
- Risk-based framing based on ISO/IEC 23894, 42001, and 42005 (referring to reporting or monitoring for risk management)

Utility statement (in body text):

This document specifies a minimally sufficient set of data elements needed to describe an AI incident within an AI incident report.

What this standard does not cover:

- How an AI incident reporting and management system should be designed, developed, deployed, or operated
- Who should own and operate an AI incident reporting and management system
- What criteria must be met to determine when an AI incident should be reported
- Who is responsible for reporting an AI incident
- To whom an AI incident should be reported

Key ISO/IEC Definition – AI System Incident

AI system incident
AI incident
event associated with an AI system that results or can result in harm.

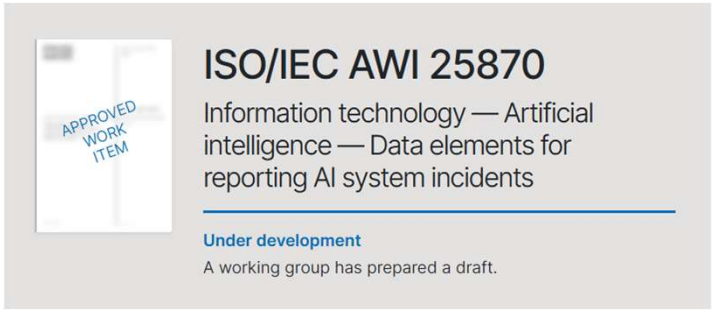
Note 1 to entry: Harm can happen at any point in the AI system life cycle. See ISO/IEC 22989:2022, Clause 6 for stages of the AI system life cycle.

Note 2 to entry: See Clause 5, Table 2 – "Harm type" for possible values describing harm.

Note 3 to entry: Includes cases sometimes known as a near miss.

[ISO/IEC 22989:2022, 3.1.4, modified.]

ISO/IEC 25870 – Core

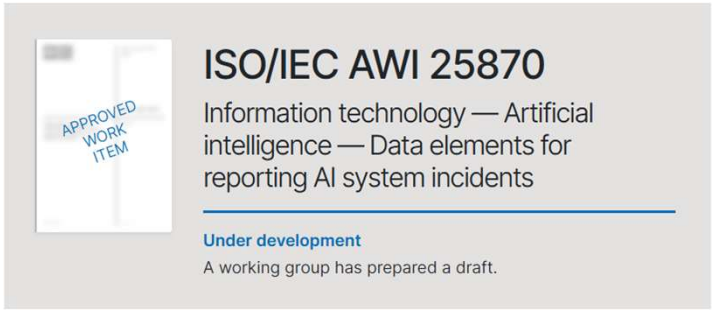


https://www.iso.org/standard/91804.html

Table 2 – Data elements for AI incident reporting

- Currently 36 data elements
- 5 Categories:
  - Administrative information
  - Incident information
  - AI system information
  - Incident analysis
  - Other
- Incident information – describes the harm involved (largest category)
- Guiding Principle – maintain backward compatibility w/ OECD framework

ISO/IEC 25870 – Larger Role



https://www.iso.org/standard/91804.html

ISO/IEC 25870 complements the data models of other incident reporting frameworks

- Describes the AI system involved
- Describes (robustly) harm involved

Frameworks analyzed (to date):

- Security/Cybersecurity:
  - Common Vulnerability & Exposures (CVE)
  - MITRE ATLAS
- Medical:
  - US FDA MedWatch Safety Reporting (Mandatory, Voluntary)
  - US FDA Manufacturer and User Facility Device Experience (MAUDE) Database
  - EU Medical Device Regulation (MDR 2017/745) and In Vitro Diagnostic Regulation (IVDR 2017/746)
- Consumer Products:
  - Consumer Product Safety Commission (CPSC) – Report an Unsafe Product
- AI Acts:
  - EU AI Act
  - USA California SB 53 (Transparency in Frontier Artificial Intelligence Act)

Questions

(mgarris@nist.gov)

Workshop (Broad)	**ISO/IEC 25870** (Narrow)
AI incident management (approaches & guidance)	Data elements for reporting AI system incidents
Definitions & lifecycles	One ISO Definition & ISO/IEC AI lifecycle
Emerging AI incident types	Harm-related incidents