ETSI TS 104 158-2 V1.1.1 (2026-03)

TECHNICAL SPECIFICATION

Securing Artificial Intelligence (SAI);
AI Incident Reporting;
Part 2: AI Common Incident Expression (AICIE) Common Container

Reference
DTS/SAI-0027

Keywords
artificial intelligence, cybersecurity

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Securing Artificial Intelligence (SAI).

The present document is part 2 of a multi-part deliverable covering AI Incident Reporting, as identified below:

Part 1: "AI Common Incident Expression (AICIE) Global Framework";

Part 2: "AI Common Incident Expression (AICIE) Common Container";

Part 3: "AI Common Incident Expression (AICIE) Security Container".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The common resource framework record described in Part 1 of the present document (ETSI TS 104 158-1 [1]) enables any kind of AI incident related resources to be made known to others in almost any manner and basis of their choosing, including similar lists, specifications, and repositories of information "containers."

Part 1 (ETSI TS 104 158-1 [1]) enables many different containers. Most of the information fields optional. The present part of the present document provides for a generic data record for an AICIE "common container" derived from work of the OECD, published government and industry requirements, and other current researchers and providers of AI incident reporting that attempts to bridge the highly diverse reporting and user communities [i.1] thru [i.33].

1 Scope

The present document provides a technical specification for an AI Common Incident Expression Common Container for AI Incident Reporting.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 104 158-1: "Securing Artificial Intelligence (SAI); AI Incident Reporting; Part 1: AI Common Incident Expression (AICIE) Global Framework".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI TS 104 223 (V1.1.1): "Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems".

[i.2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[i.3] UK DSIT: "AI Cyber Security Code of Practice".

[i.4] UK NCSC: "Guidelines for secure AI system development".

[i.5] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[i.6] Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.

[i.7] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[i.8] GCVE.EU: "GCVE: Global CVE Allocation System".

[i.9] Sean McGregor, et al. (2025): "In-House Evaluation Is Not Enough: Towards Robust Third-Party Flaw Disclosure for General-Purpose AI", Cornell University SarXiv:2503.16861v1 [cs.AI].

[i.10] OECD: "Towards a Common Reporting Framework for AI Incidents", OECD Artificial Intelligence Papers, February 2025, No. 34.

[i.11] OECD: "AIM: AI Incidents and Hazards Monitor".

[i.12] OECD: "Defining AI Incidents and Related Terms", OECD Artificial Intelligence Papers, May 2024, No. 16.

[i.13] McGregor, S. (2021): "Preventing Repeated Real World AI Failures by Cataloging Incidents: The AI Incident Database", Proceedings of the AAAI Conference on Artificial Intelligence, 35(17), 15458-15463.

[i.14] OECD: "OECD Framework for the Classification of AI Systems", OECD Digital Economy Papers, February 2022, No. 323.

[i.15] NCSC: "Where to Report a Cyber Incident".

[i.16] NCSC: "Responding to a cyber incident - a guide for CEOs".

[i.17] Confédération Suisse, Federal Office for Cybersecurity BACS: "Information on the reporting obligation".

[i.18] H. Frase, R.B. L. Dixon: "AI Incidents, Key Components for a Mandatory Reporting Regime", CSET, January 2025.

[i.19] OWASP Gen AI Incident/Exploit Round-up Submission.

[i.20] Recommendation ITU-T X.1500: "Overview of cybersecurity information exchange".

[i.21] ETSI TR 104 003: "Cyber Security (CYBER); The vulnerability disclosure ecosystem".

[i.22] ETSI TR 103 331: "Cyber Security (CYBER); Structured threat information sharing".

[i.23] CISA: "Cybersecurity Incident & Vulnerability Response Playbooks".

[i.24] NIST AI 600-1: "Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile".

[i.25] AIID: "AI Incident Database".

[i.26] MIT: "AI Risk Repository".

[i.27] AVID: "AI Vulnerability Database".

[i.28] OECD: "Overview and methodology of the AI Incidents and Hazards Monitor".

[i.29] Partnership on AI: "AI Incident Database".

[i.30] Kaggle: "AI Incident Database".

[i.31] JSON-LD.org: "JSON for Linking Data".

[i.32] Sharkov: "Unveiling the invisible: Knowledge Graph-Driven Discovery of Hidden Cascade Risks in Critical Infrastructure Supply Chains", IEEE™ CSR.

[i.33] UN: "International Standard Industrial Classification of All Economic Activities".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 104 158-1 [1] apply.

3.2 Symbols

For the purposes of the present document, the symbols given in ETSI TS 104 158-1 [1] apply.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 104 158-1 [1] apply.

4 AICIE Common Container Record

4.1 AICIE Common Container Record Format and Values

4.1.1 Introduction

The AICIE Common Container Record format is depicted in Figure 4.1-1 and captures a set of minimum essential information concerning an AI incident reporting resource. **BOLD** field names are mandatory, enum=enumeration, cb=checkbox and "…" indicates free-form content. The AICE Common Container JSON record format is defined using the JSON Schema in Annex A. A MindMap version of the schema version 1.0.0 is shown in Figure 4.1-1. The value for each data element is described in detail below.

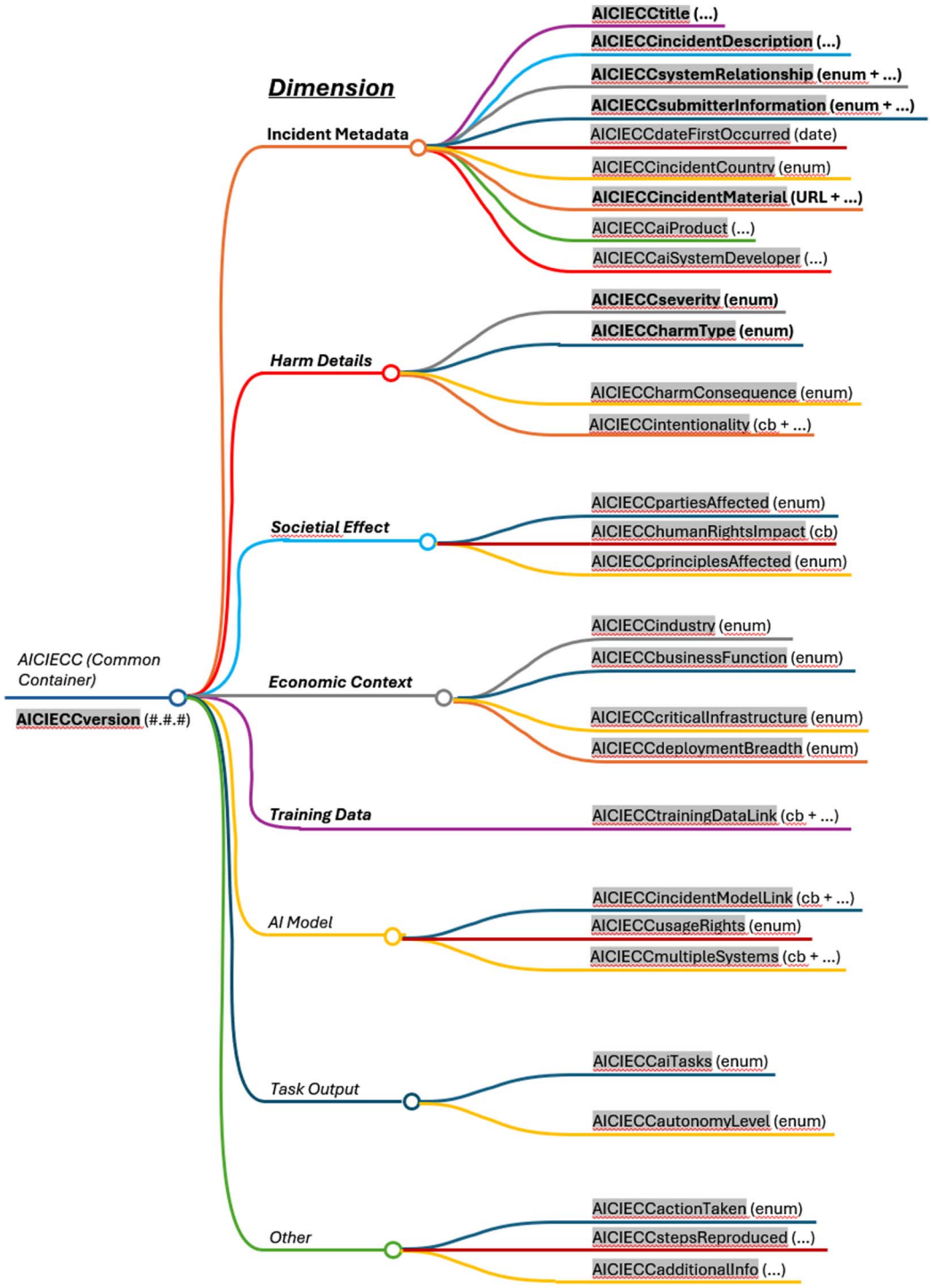

Figure 4.1-1: Mindmap of the AICIE Common Container Record

4.1.2 AICIECCversion

This required value describes the present AICIE Common Container Record specification version being used and expressed as three numbers separated by commas and set initially to 1.0.0.

4.1.3 AICIECCtitle

This required value without any constraints describes a title for the AI incident.

4.1.4 AICIECCincidentDescription

This required value without any constraints describes the AI incident.

4.1.5 AICIECCsystemRelationship

This required value describes the how the AI system(s) are related to the incident using one or more of the following non-case-sensitive enumerations, including an unconstrained free-form option.

direct cause
contributing factor
failure to act
overreliance and intentional misuse
human error
legal obligation omission
… (free-form content)

4.1.6 AICIECCsubmitterInformation

This required value describes the information without any constraints for the entity submitting the incident report including entity name, affiliation, physical address, a useable email address, stakeholder group, including one or more of the following non-case sensitive affiliation enumerations.

government or regulatory body
public interest body or non-government organisation
AI system developer or provider
AI system user
affected stakeholder
knowledgeable of the incident
… (free-form content)

4.1.7 AICIECCdateFirstOccurred

This optional value describes the date of first known occurrence of the AI incident in Coordinated Universal Timenumbers [year]-[month]-[day].

4.1.8 AICIECCincidentCountry

This optional value describes the countries where the AI incident occurred as an enumerated string of country identifiers separated by commas.

4.1.9 AICIECCincidentMaterial

This required value without any constraints describes the AI incident supporting materials address location - preferably as a persistent, precise, accessible Uniform Resource Location (URL) or a link capable of providing the resource.

4.1.10 AICIECCaiProduct

This optional value without any constraints describes a title for the name and version of the AI system(s) or product(s) that gave rise to the reported AI incident.

4.1.11 AICIECCaiSystemDeveloper

This optional value without any constraints describes the organisation(s) that developed and/or deployed the AI product(s) or services that gave rise to the reported AI incident.

4.1.12 AICIECCseverity

This required value describes the assessed severity of the AI incident reported using one or more of the following non-case-sensitive enumerations, or other using an unconstrained free-form option.

serious hazard
hazard
incident
serious incident
incident
… (free-form content)

4.1.13 AICIECCharmType

This required value describes the harm type of the AI incident reported using one or more of the following non-case-sensitive enumerations, including an unconstrained free-form option.

physical
psychological
reputational
economic/property
environmental
public interest
critical infrastructure
human or fundamental rights
… (free-form content)

4.1.14 AICIECCharmConsequence

This optional value describes, if applicable, a quantification of the harm using one or more of the following non-case-sensitive enumerations, including an unconstrained free-form option.

economic losses
death
injury
compensation
quantification
… (free-form content)

4.1.15 AICIECCintentionality

If applicable using an indicator flag, this optional value describes without any constraints how an AI incident was linked in an unintended or wrongful way to an AI system and how.

4.1.16 AICIECCpartiesAffected

This optional value describes, if applicable, the affected parties using one or more of the following non-case-sensitive enumerations, including an unconstrained free-form option.

consumer
children
workers
business
trade union
government
civil society
general public
… (free-form content)

4.1.17 AICIECCchumanRightsImpact

If applicable using an indicator flag, this optional value describes without any constraints any adverse impacts on human rights or fundamental values.

4.1.18 AICIECCprinciplesAffected

This optional value describes associated AI principles using one or more of the following non-case-sensitive enumerations.

accountability
fairness
inclusivity
privacy
data governance
respect of human rights
robustness
digital security
safety
environmental sustainability
transparency
explainability
democracy
human autonomy

4.1.19 AICIECCindustry

This optional value describes industries associated with the AI incident using a string of comma separated numbers of industry classifications using International Standard Industrial Classification of All Economic Activities (ISIC) [i.33].

4.1.20 AICIECCbusinessFunction

This optional value describes business functions where the AI incident occurred using one or more of the following non-case-sensitive enumerations.

human resource management
sales
ICT management and information security
marketing and advertisement
logistics
citizen/customer service
procurement
maintenance
accounting
monitoring and quality control
production
planning and budgeting
research and development
compliance and justice
… (free-form content)

4.1.21 AICIECCcriticalInfrastructure

If applicable, if critical infrastructure capabilities are significantly affected this optional value indicates those critical infrastructures using one or more of the following non-case-sensitive enumerations.

energy, including oil and gas
water supply and wastewater management
healthcare and public health
transportation and logistics
telecommunications and ICT infrastructure
food and agriculture
financial services
public safety and emergency services
government operations and public administration, including electoral systems
manufacturing and industry
education and research
housing and urban infrastructure
public utilities and environmental protection
supply chain and distribution networks
national defence and border security
… (free-form content)

4.1.22 AICIECCdeploymentBreadth

This optional value describes the breadth of AI system deployment associated with the AI incident occurred using one of the following non-case-sensitive enumerations.

pilot project (e.g. team/small group)
narrow deployment (e.g. company/city)
broad deployment (e.g. sector/country
widespread deployment (e.g. sectors/countries)
… (free-form content)

4.1.23 AICIECCtrainingDataLink

If applicable using an indicator flag, where the AI incident is linked to the training data, this optional value describes without any constraints how the incident is linked.

4.1.24 AICIECCincidentModelLink

If applicable using an indicator flag, where the AI incident is linked to the AI model, this optional value describes without any constraints how the incident is linked.

4.1.25 AICIECCusageRights

This optional value describes the usage rights associated with the AI system giving rise to the incident using one or more of the following non-case-sensitive enumerations.

one-time license
fee-based
research purposes only
non-commercial
restricted access
free of charge
creative commons
open source/permissive
copyleft/share alike
… (free-form content)

4.1.26 AICIECCmultipleSystems

If applicable using an indicator flag, where the AI incident is linked to multiple AI systems, this optional value describes without any constraints how the incident is linked.

4.1.27 AICIECCaiTasks

This optional value describes the tasks associated with the AI system giving rise to the incident using one or more of the following non-case-sensitive enumerations.

recognition/object detection
organisation/recommenders
event/anomaly detection
forecasting/prediction
interaction support/chatbots
goal-driven organisation
reasoning with knowledge structures/planning
… (free-form content)

4.1.28 AICIECCautonomyLevel

This optional value describes the maximum autonomy level associated with the AI system giving rise to the incident using one of the following non-case-sensitive enumerations.

no-action autonomy (human support)
low-action autonomy (human-in-the-loop)
medium-action autonomy (human-on-the-loop)
high-action autonomy (human-out-of-the-loop)
… (free-form content)

4.1.29 AICIECCactionTaken

This optional value describes the actions taken, if any, in response to the AI incident using one or more of the following non-case-sensitive enumerations.

prevention
mitigation
ceasing
remediation
… (free-form content)

4.1.30 AICIECCstepsReproduced

If applicable, this optional value without any constraints describes the steps taken to reproduce the AI incident.

4.1.31 AICIECCadditionalInfo

This optional value without any constraints describes any other information associated with the AI incident.

Annex A (normative): AICIE Common Container JSON record Format V1.0.1

```
{
    "$schema": "http://[tbd]",
    "title": "JSON Schema for AI Common Incident Expression Common Record Container version 1.0.1",
    "$id": "https://www.etsi.org/[tbd]",
    "properties": {
        "AICIECCversion": {
            "description": "present AICIE Common Container Record specification version being used
and expressed as three numbers separated by commas and set initially to 1.0.1",
            "type": "string"
        },
        "AICIECCtitle": {
            "description": "title for the AI incident",
            "type": "string"
        },
        "AICIECCincidentDescription": {
            "description": "the AI incident",
            "type": "string"
        },
        "AICIECCsystemRelationship": {
            "description": "how the AI system(s) are related to the incident",
            "enum": [
             "direct cause"
             "contributing factor",
             "failure to act",
             "overreliance and intentional misuse"
             "human error",
             "legal obligation omission"
            ],
            "type": "string"
        },
        "AICIECCsubmitterInformation": {
            "description": "information for the entity submitting the incident report including
entity name, affiliation, physical address, a useable email address, stakeholder group, including
one or more of the following non-case sensitive affiliation enumerations",
            "enum": [
             "government or regulatory body",
             "public interest body or non-government organisation"
             "AI system developer or provider",
             "AI system user",
             "affected stakeholder",
             "knowledgeable of the incident"
            ],
            "type": "string"
        },
        "AICIECCdateFirstOccurred": {
            "description": "date of first known occurrence of the AI incident in Coordinated
Universal Time",
            "type": "string"
            {
             "day":,
             "month":,
             "year":,
             }
        },
        "AICIECCincidentCountry": {
            "description": "countries where the AI incident occurred as an enumerated string of
country identifiers separated by commas",
            "type": "string"
        },
        "AICIECCincidentMaterial": {
            "description": "organisation(s) that developed and/or deployed the AI product(s) or
services that gave rise to the reported AI incident",
            "type": "string"
        },
        "AICIECCaiProduct": {
            "description": "title for the name and version of the AI system(s) or product(s) that
gave rise to the reported AI incident",
            "type": "string"
        },
        "AICIECCaiSystemDeveloper": {
```

```
            "description": "organisation(s) that developed and/or deployed the AI product(s) or
services that gave rise to the reported AI incident",
            "type": "string"
        },
        "AICIECCseverity": {
            "description": "assessed severity of the AI incident reported",
            "enum": [
            "serious hazard",
            "hazard",
            "incident",
            "serious incident",
            "incident"
           ],
            "type": "string"
        },
        "AICIECCharmType": {
            "description": "harm type of the AI incident reported",
            "enum": [
             "physical",
             "psychological"
             "reputational"
             "economic/property",
             "environmental",
             "public interest",
             "critical infrastructure",
             "human or fundamental rights"
            ],
            "type": "string"
        },
        "AICIECCharmConsequence": {
            "description": "affected parties",
            "enum": [
             "economic losses",
             "death",
             "injury",
             "compensation",
             "quantification"
            ],
            "type": "string",
        },
        "AICIECCintentionality": {
            "description": "if applicable, how an an AI incident was linked in an unintended or
wrongful way to an AI system and how",
            "type":
            {true, false}
            "string"
        },
        "AICIECCpartiesAffected": {
            "description": "if applicable, the affected parties",
            "enum": [
             "consumer",
             "children",
             "workers",
             "business",
             "trade union",
             "government",
             "civil society",
             "general public"
            ],
            "type": "string"
        },
        "AICIECChumanRightsImpact": {
            "description": "if applicable using an indicator flag, any adverse impacts on human
rights or fundamental values",
            "type":
            {true, false}
            "string"
        },
        "AICIECCprinciplesAffected": {
            "description": "associated AI principles",
            "enum": [
             "accountability",
             "fairness",
             "inclusivity",
             "privacy",
             "data governance",
             "respect of human rights",
             "robustness",
```

```
            "digital security",
            "safety",
            "environmental sustainability",
            "transparency",
            "explainability",
            "democracy",
            "human autonomy"
           ],
           "type": "string"
       },
       "AICIECCindustry": {
           "description": "industries associated with the AI incident using a string of comma
separated numbers of industry classifications using International Standard Industrial Classification
of All Economic Activities (ISIC)",
           "type": "string"
       },
       "AICIECCbusinessFunction": {
           "description": "business functions where the AI incident occurred",
           "enum": [
            "human resource management",
            "sales",
            "ICT management and information security",
            "marketing and advertisement",
            "logistics",
            "citizen/customer service",
            "procurement",
            "maintenance",
            "accounting",
            "monitoring and quality control",
            "production",
            "planning and budgeting",
            "research and development",
            "compliance and justice"
           ],
           "type": "string"
       },
       "AICIECCcriticalInfrastructure": {
           "description": "if critical infrastructure capabilities are significantly affected,
those critical infrastructures",
           "enum": [
            "energy, including oil and gas",
            "water supply and wastewater management",
            "healthcare and public health",
            "transportation and logistics",
            "telecommunications and ICT infrastructure",
            "food and agriculture",
            "financial services",
            "public safety and emergency services",
            "government operations and public administration including electoral systems",
            "manufacturing and industry",
            "education and research",
            "housing and urban infrastructure",
            "public utilities and environmental protection",
            "supply chain and distribution networks",
            "national defense and border security"
           ],
           "type": "string"
       },
       "AICIECCdeploymentBreadth": {
           "description": "breadth of AI system deployment associated with the AI incident
occurred",
           "enum": [
            "pilot project (e.g., team/small group)",
            "narrow deployment (e.g., company/city)",
            "broad deployment (e.g., sector/country",
            "widespread deployment (e.g., sectors/countries)"
           ],
           "type": "string"
       },
       "AICIECCtrainingDataLink": {
           "description": "if applicable using an indicator flag, where the AI incident is linked
to the training data, how the incident is linked",
          "type":
           {true, false}
           "string"
       },
       "AICIECCincidentModelLink": {
```

```
            "description": "if applicable using an indicator flag, where and how the AI incident is
linked to the AI model",
           "type":
            {true, false}
            "string"
        },
        "AICIECCusageRights": {
            "description": "usage rights associated with the AI system giving rise to the incident",
            "enum": [
             "one-time license",
             "fee-based",
             "research purposes only",
             "non-commercial",
             "restricted access",
             "free of charge",
             "creative commons",
             "open source/permissive",
             "copyleft/share alike"
            ],
            "type": "string"
        },
        "AAICIECCmultipleSystems": {
            "description": "if applicable using an indicator flag, where and how the AI incident is
linked to multiple AI systems",
            "type":
            {true, false}
            "string"
        },
        "AICIECCaiTasks": {
            "description": "tasks associated with the AI system giving rise to the incident",
            "enum": [
             "recognition/object detection",
             "organisation/recommenders",
             "event/anomaly detection",
             "forecasting/prediction",
             "interaction support/chatbots",
             "goal-driven organisation",
             "reasoning with knowledge structures/planning"
           ],
            "type": "string"
         },
        "AICIECCautonomyLevel": {
            "description": "maximum autonomy level associated with the AI system giving rise to the
incident",
            "enum": [
             "no-action autonomy (human support)",
             "low-action autonomy (human-in-the-loop)",
             "medium-action autonomy (human-on-the-loop)",
             "high-action autonomy (human-out-of-the-loop)
           ],
            "type": "string"
        },
        "AICIECCactionTaken": {
            "description": "any actions taken in response to the AI incident",
            "enum": [
             "prevention",
             "mitigation",
             "ceasing",
             "remediation
           ],
            "type": "string"
        },
        "AICIECCstepsReproduced": {
            "description": "any actions taken in response to the AI incident",
            "type": "string"
        },
        "AICIECCadditionalInfo": {
            "description": "any other information associated with the AI incident",
            "type": "string"
        }
    },
    "required": [
     "AICIECCversion",
     "AICIECCtitle",
     "AICIECCincidentDescription",
     "AICIECCsystemRelationship",
     "AICIECCsubmitterInformation",
     "AICIECCincidentMaterial",
```

```
      "AICIECCseverity",
      "AICIECCharmType"
    ]
}
```

Annex B (informative): Common reporting framework recommendations

The OECD Framework for the Classification of AI systems provides a table to summarize the information needed to understand an AI incident, at the same time allowing for additional details to provide more nuanced insights to policymakers and regulators, see Table B-1. References in the OECD report table have been removed. A second study published as a Cornell University [i.9] note is provided as Table B-2.

Table B-1 is an adaptation of an original work by the OECD [i.10]. The opinions expressed and arguments employed in this adaptation should not be reported as representing the official views of the OECD or of its Member countries. The only adaption made is the removal of references that were present in the original table.

Table B-1: Detailed criteria of the OECD common reporting framework [i.10]

	Dimension	Incidents reporting framework criteria	Answer format	Sub-criteria
1	Incident metadata	Title*	Open text	N/A
2	Incident metadata	**Description of the incident***	Open text	N/A
3	Incident metadata	How is the AI system(s) related to the incident*	Multi-selection with open text	Direct cause; contributing factor; failure to act; overreliance and intentional misuse; human error; failure to comply with legal frameworks; other (specify for all)
4	Incident metadata	Submitter information (role, affiliation, etc.)*	Open text and multi-selection	Role; email; affiliation; stakeholder group or source type; relation to the incident: "I represent a government or regulatory body", "I work or am affiliated to a public interest body or NGO", "I work in or am affiliated to the organisation that developed or provided the related AI system", "I am a user of the related AI system", "I am an affected stakeholder", "None of the above, but have partial or substantial knowledge of the incident (e.g. first-hand knowledge, research etc.)", "Other (specify)"
5	Incident metadata	**Date of first known occurrence**	Date	N/A
6	Incident metadata	**Country(ies) where incident occurred**	Multi-selection	List of countries
7	Incident metadata	**Supporting material(s) about the incident***	Open text, URLs and upload button	N/A
8	Incident metadata	Name and version of the AI system(s)/product(s)	Open text	N/A
9	Incident metadata	Organisation(s) that developed and/or deployed the AI system	Open text	N/A
10	Harm details	**Severity***	Multi-selection	Hazard; serious hazard; incident; serious incident; disaster; other (specify)
11	Harm details	**Harm type***	Multi-selection	Physical; psychological; reputational; economic/property; environmental; public interest/critical infrastructure; human or fundamental rights; other (specify)
12	Harm details	If applicable, quantification of harm	Multi-selection	Economic losses; death; injury; number of affected stakeholders; compensation; other (specify)
13	Harm details	Incident linked to use of AI system(s) in unintended/wrongful way (and how)	Checkbox	If selected, specify (short answer, limited characters)
14	People & planet	**Affected stakeholder(s)**	Multi-selection	Consumer; children; workers; trade unions; business; government; civil society; general public; other (specify)
15	People & planet	Adverse impacts on human rights or fundamental rights	Checkbox	If selected, specify (short answer, limited characters)

	Dimension	Incidents reporting framework criteria	Answer format	Sub-criteria
16	People & planet	Associated AI Principles	Multi-selection	Accountability; fairness; inclusive growth; privacy; data governance; respect of human rights; robustness; digital security; safety; environmental sustainability; transparency; explainability; democracy; human autonomy
17	Economic context	**Industry(ies)**	Multi-selection	Classification from the International Standard Industrial Classification of All Economic Activities (ISIC)
18	Economic context	Business function(s) where the AI incident occurred	Multi-selection	Human resource management; sales; ICT management and information security; marketing and advertisement; logistics; citizen/customer service; procurement; maintenance; accounting; monitoring and quality control; production; planning and budgeting; research and development; compliance and justice; other (specify)
19	Economic context	Incident linked to the functioning of critical functions/infrastructure	Checkbox	Energy, including oil and gas; water supply and wastewater management; healthcare and public health; transportation and logistics; telecommunications and ICT infrastructure; food and agriculture; financial services; public safety and emergency services; government operations and public administration, including electoral systems; manufacturing and industry; education and research; housing and urban infrastructure; public utilities and environmental protection; supply chain and distribution networks; national defence and border security; other (specify)
20	Economic context	Breadth of deployment	Single choice	Pilot project (e.g. team/small group); narrow deployment (e.g. company/city); broad deployment (e.g. sector/country); widespread deployment (e.g. sectors/countries); other (specify)
21	Data & input	Incident linked to the training data of AI system(s) (and how)	Checkbox	If selected, specify (short answer, limited characters)
22	AI model	Incident linked to the AI model (and how)	Checkbox	If selected, specify (short answer, limited characters)
23	AI model	Usage rights	Multi-selection	One-time license; fee-based; research purposes only; non-commercial; restricted access; free of charge; creative commons; open source/permissive; copyleft/share alike; other (specify)
24	AI model	Incident linked to interaction of multiple AI systems	Checkbox	If selected, specify (short answer, limited characters)
25	Task & output	Task(s) of AI system(s)	Multi-selection	Recognition/object detection; organisation/recommenders; event/anomaly detection; forecasting/prediction; interaction support/chatbots; goal-driven organisation; reasoning with knowledge structures/planning; content generation; other (specify)
26	Task & output	Maximum autonomy level of AI system(s)	Single choice	No-action autonomy (human support); low-action autonomy (human-in-the-loop); medium-action autonomy (human-on-the-loop); high- action autonomy (human-out-of-the-loop); other (specify)
27	Other	If applicable, action(s) taken	Open text, multi- selection	Prevention; mitigation; ceasing; remediation; other (specify for all)
28	Other	If applicable, steps to reproduce the incident	Open text	If selected, specify (open text)
29	Other	Additional information	Open text	N/A
NOTE: * = OECD Mandatory Criteria. **BOLD** = Criteria found in at least three AI reporting frameworks.				

Table B-2: AI Flaw Report Card Schema [i.9]

Report Type	Field Name	Field Description
Collected for All Flaw Reports	Reporter ID	Anonymous or real identity of flaw reporter
	Report ID	Unique flaw report ID. The flaw report ID can be referenced in future submissions or mitigation efforts, similar to vulnerability identifiers such as CVE identifiers in computer security (Cybersecurity and Infrastructure Security Agency, 2022).
	System Version(s)	AI system(s) and version(s) involved; multiple systems can be selected
	Report Status	Current status of the report, recorded with timestamps as updated by the submitter or receiving company. Initially, the status of a report is "Submitted", but once it is submitted the status field will be updated to reflect current status of addressing the flaw (e.g., "Under investigation" or "Fixed") (Cybersecurity and Infrastructure Security Agency, 2022).
	Session ID	System session ID(s) for tracing flaw environment
	Report Timestamp	Report submission timestamp
	Flaw Timestamp(s)	Time(s) where flaws occurred
	Context Info	Versions of other software or hardware systems involved
	Flaw Description	Description of the flaw, its identification, reproduction, and how it violates system policies or user expectations
	Policy Violation	Detail of how the expectations of the system are violated or undocumented, pointing to the terms of use, acceptable use policy, system card, or other documentation. Policies may be explicitly or implicitly violated.
	Developer	Triage tag with name of system developer
	System	Triage tag with name and version of system
	Severity	Triage tag with worst-case scenario estimate of how negatively stakeholders will be impacted
	Prevalence	Triage tag with rough estimate of how often the flaw might be expressed across system deployments
	Impacts	Triage tag indicating how impacted stakeholders may suffer if the flaw is not addressed
	Impacted Stakeholder(s)	Triage tag(s) indicating who may be harmed if the flaw is not addressed
	Risk Source	Triage tag indicating worst-case scenario estimate of how negatively stakeholders will be impacted
	Bounty Eligibility	Triage tag indicating whether the submitter believes the flaw report meets the criteria for bounty programs
Collected for Real-World Events	Description of the Incident(s)	Details on specific real-world event(s) that have occurred
	Implicated Systems	Systems involved in real-world event(s) which generalized flaw reports might cover
	Submitter Relationship	How the submitter is related to the event (e.g., "affected stakeholder" or "independent observer")
	Event Date(s)	Date when the incident(s) occurred
	Event Location(s)	Geographical location of the incident(s)
	Experienced Harm Types	Physical; psychological; reputational; economic/property; environmental; public interest/critical infrastructure; fundamental rights; other
	Experienced Harm Severity	Maximum severity of harm experienced in the real world
	Harm Narrative	Justification of why the event constitutes harm and how system flaws contributed to it
Malign Actor	Tactic Select	Tactics observed or used (e.g., from MITRE's ATLAS Matrix)
	Impact	Confidentiality/privacy, integrity, availability, abuse
Security Incident Report	Threat Actor Intent	Deliberate, unintentional, unknown
	Detection	How the reporter knows about the security incident, including observation methods
Vulnerability Report	Proof-of-Concept Exploit	A code and documentation archive proving the existence of a vulnerability
Hazard Report	Examples	A list of system inputs/outputs to help understand the replication packet
	Replication Packet	Files evidencing the flaw statistically, including test data, custom evaluators, and structured datasets
	Statistical Argument	Argument supporting sufficient evidence of a flaw

History

Version	Date	Status
V1.1.1	March 2026	Publication