TAF: A Semantic Governance Framework for Assessing EU AI Act Article 15 Safeguards in AI-Based Digital Forensic Tool Procurement

Darren McCabe[1], David Lewis[1]

[1]ADAPT Centre, Trinity College Dublin, Ireland

Abstract

AI-based digital forensic tools are increasingly being considered for organisational investigations into insider threats, data leakage, fraud, policy breaches, unauthorised access, and cybersecurity incidents. These tools may use machine learning or Large Language Models to classify artefacts, summarise communications, generate timelines, identify relevant evidence, and support investigative decision-making. In in-house digital forensic contexts, these outputs may affect employees, contractors, and other data subjects, and may influence disciplinary, employment, legal, or regulatory outcomes. This creates a procurement governance problem: organisations must assess whether AI-based forensic tools provide explicit safeguards for accuracy, robustness, cybersecurity, traceability, human oversight, and the protection of fundamental rights before deployment.

This paper proposes the Trustworthy AI Forensics (TAF) framework, a semantic governance framework for assessing whether procurement documentation for AI-based digital forensic tools operationalises safeguards derived from the EU Artificial Intelligence Act, with a particular focus on Article 15 requirements for accuracy, robustness, and cybersecurity [1]. The framework represents legal provisions, legal sub-provisions, competency questions, governance safeguards, evidence indicators, risk dimensions, and structural procurement risks through the Mapping Trustworthy AI to Law Ontology (MTALO), an ontology-supported traceability model. It is paired with the Mapping Accuracy Quality Assessment method, a deterministic screening approach that checks procurement artefacts for explicit textual evidence of governance safeguards.

The framework is implemented as a prototype using RDF/XML, SHACL, SPARQL, JSON taxonomy files, a Python screening pipeline, and an HTML reporting layer. Validation confirms a full traceability model from legal provisions to structural procurement-risk outputs. It reports 12 legal provisions, 33 legal sub-provisions, 31 competency questions, 12 governance safeguards, 3 evidence indicator categories, 4 risk dimensions, 7 structural procurement risk classes, and 12 full-chain rows. Prototype results across three procurement use cases demonstrate how procurement records can be screened for documentary evidence coverage, advisory review gaps, readiness, and structural procurement risk. The contribution is a standards-oriented semantic model for making AI forensic procurement safeguards explicit, traceable, queryable, and reviewable.

Keywords

Trustworthy AI, Digital Forensics, EU AI Act, Article 15, AI Procurement, Semantic Web, Ontology, Governance Safeguards, Structural Procurement Risk, Fundamental Rights

1. Introduction

Digital forensic practice is increasingly shaped by artificial intelligence. Organisations now process large volumes of endpoint data, cloud logs, identity records, email exports, chat messages, collaboration-platform records, file metadata, and security alerts. AI-based tools promise to reduce investigation time by classifying artefacts, filtering large datasets, summarising communications, extracting entities, identifying relevant events, and assisting forensic analysts in constructing timelines and investigative narratives. Large Language Models further extend these possibilities through question answering over evidence collections, semantic search, and draft report generation.

These capabilities create opportunities, but they also introduce significant governance risks. Digital forensic investigations are not ordinary analytics exercises. They may produce or influence evidence

NXDG 2026: NeXt-generation Data Governance workshop, September 15, 2026, co-located with 22nd SEMANTiCS, September 15–17, 2026, Ghent, Belgium

mccabed9@tcd.ie (D. McCabe); delewis@tcd.ie (D. Lewis)

https://www.tcd.ie/ (D. McCabe); https://www.tcd.ie/ (D. Lewis)

© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

used in disciplinary proceedings, employment decisions, litigation, regulatory reporting, fraud investigations, or referrals to law enforcement. In in-house investigations, affected individuals may include employees, contractors, customers, or third parties whose communications, system activity, documents, or metadata are examined. Errors in AI-supported forensic analysis can therefore affect privacy, data protection, non-discrimination, procedural fairness, effective remedy, and confidence in the reliability of digital forensic practice [2, 3].

The procurement stage is a critical control point in the responsible adoption of AI systems. If an AI-based forensic tool is acquired without explicit requirements for accuracy, robustness, cybersecurity, logging, data governance, human oversight, and safeguards for fundamental rights, those gaps may become embedded in investigative workflows. Procurement documentation often contains broad supplier claims such as "accurate", "secure", "compliant", "transparent", or "explainable". Such claims may be insufficient unless they are linked to measurable safeguards, documentary evidence, contractual obligations, validation data, and reviewable risk outputs.

The EU Artificial Intelligence Act introduces requirements for high-risk AI systems, including Article 15 obligations relating to accuracy, robustness, and cybersecurity [1]. Article 15 is particularly relevant to digital forensic procurement because unreliable outputs, weak robustness, or poor cybersecurity may compromise evidential integrity and individual rights. However, translating Article 15 into procurement practice remains challenging. Procurement teams must decide which safeguard-related information and evidence to request from providers, how requirements should be expressed in the contract, how claims should be evaluated, and how safeguard gaps should be documented before contracts are awarded or AI systems deployed.

This paper proposes the Trustworthy AI Forensics framework, referred to as TAF. TAF is a semantic governance framework for procuring AI-based digital forensic tools, centred on the Mapping Trustworthy AI to Law Ontology (MTALO). It operationalises legal, technical, forensic, and procurement requirements into a machine-readable structure of governance safeguards, evidence indicators, risk dimensions, and structural procurement-risk outputs. In MTALO these are implemented as semantic model concepts rather than ordinary prose labels, with camel-case identifiers such as `GovernanceSafeguard` used only where the paper refers to ontology classes. The framework is supported by the Mapping Accuracy Quality Assessment method, referred to as MAQA, which performs deterministic screening of procurement documentation for explicit textual evidence of safeguards.

The contribution is not a claim that semantic technologies can automate legal compliance. TAF does not replace model validation, forensic expert review, conformity assessment, or legal interpretation. Instead, the contribution is a standards-oriented method for making AI procurement safeguards explicit, traceable, queryable, and auditable.

The paper makes four contributions. First, it introduces a semantic traceability model for AI-based digital forensic procurement, linking legal provisions, legal sub-provisions, competency questions, governance safeguards, evidence indicators, risk dimensions, and structural procurement-risk outputs. Second, it operationalises Article 15 accuracy, robustness, and cybersecurity requirements as procurement-level safeguards. Third, it presents a deterministic screening method to identify explicit safeguard evidence in procurement artefacts. Fourth, it evaluates the implemented artefact using ontology validation and three procurement use-case outputs.

2. Background and Related Work

Digital forensics involves the identification, preservation, collection, examination, analysis, and presentation of digital evidence. Traditional forensic practice depends on evidence integrity, chain of custody, repeatability, documentation, expert interpretation, and defensible methods [4, 5]. AI-based forensic tools can assist with artefact classification, anomaly detection, malware triage, image analysis, entity extraction, communication review, and timeline generation. However, such tools can also alter the evidential process by prioritising artefacts, summarising evidence, suggesting investigative hypotheses, or producing confidence scores that influence human judgement.

The risks are particularly significant in in-house investigations. These investigations may be conducted by corporate security, cyber resilience, insider threat, fraud, legal, HR, compliance, or internal audit teams. They may be concerned about suspected data exfiltration, unauthorised access, system misuse, intellectual property theft, policy breaches, harassment, fraud, malware incidents, or insider risk activity. Although organisations have legitimate interests in investigating misconduct and protecting systems, affected individuals retain rights relating to privacy, data protection, proportionality, non-discrimination, fair procedures, and effective remedy [2, 3].

The EU AI Act establishes a risk-based framework for AI systems. It imposes requirements on high-risk systems, including risk management, data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness, and cybersecurity [1]. Article 15 requires high-risk AI systems to achieve appropriate levels of accuracy, robustness, and cybersecurity, and to perform consistently throughout their lifecycle. For digital forensic procurement, Article 15 raises practical questions: what accuracy level is appropriate for a forensic task, what validation evidence is required, how robustness should be tested, and how cybersecurity controls should protect models, prompts, logs, evidence data, and outputs.

The EU Model Contractual Clauses for AI procurement provide a bridge between AI Act obligations and procurement practice by expressing legal and technical requirements as contract clauses and annexes [6]. However, procurement teams still require structured methods for checking whether supplier documentation contains explicit evidence of these requirements. Recent AI procurement standardisation is also relevant. IEEE 3119-2025 defines a procurement standard for artificial intelligence and automated decision systems, covering problem definition, solicitation preparation, vendor and solution evaluation, contract negotiation, contract monitoring, and AI-specific risk management across the procurement lifecycle [7]. TAF complements this state of the art by focusing on rights-sensitive digital forensic procurement and by representing evidence requests, review gaps, and risk outputs in a machine-readable semantic model.

Ontologies and semantic web technologies provide a promising foundation for such assessment. Standardised knowledge graph formats and graph processing languages including RDF, OWL, SPARQL, and SHACL enable machine-readable representation, querying, and validation of domain knowledge [8, 9, 10, 11]. In AI governance, ontologies can link legal provisions, technical controls, organisational responsibilities, evidence artefacts, and risk categories. For procurement, this enables a reusable vocabulary and traceability model that connects legal obligations to operational safeguards and documentary evidence.

3. Research Problem and Aim

The research problem addressed in this paper is the lack of a structured, traceable, and machine-readable method to assess whether procurement documentation for AI-based digital forensic tools explicitly operationalises Article 15 safeguards and related fundamental rights requirements.

Current AI procurement assessments often depend on supplier claims, generic security questionnaires, informal expert judgement, or broad contractual statements. These approaches may be insufficient for AI-based forensic tools because they do not consistently connect legal obligations to specific evidence requirements. A supplier may state that a tool is accurate, robust, secure, or explainable without providing task-specific accuracy metrics, robustness testing, cybersecurity controls, audit logging, human oversight mechanisms, or evidence of its impact on rights.

This creates four linked gaps. The first is a legal-to-technical translation gap: Article 15 is expressed at a regulatory level, whereas procurement teams require operational requirements and supplier evidence. The second is a forensic reliability gap: digital forensic practice depends on evidence integrity, traceability, repeatability, and expert review [4, 5]. The third is a fundamental rights gap: in-house investigations may process sensitive personal data and influence serious employment or legal outcomes, but must do so while protecting the rights of individuals affected by those outcomes [2, 3]. The fourth is a standardisation gap: without a reusable semantic structure, different procurement teams may ask

inconsistent questions and interpret safeguards inconsistently.

The research question is:

> How can semantic web technologies support the structured assessment of Article 15 and fundamental rights safeguards in the procurement of AI-based digital forensic tools?

The aim is to develop and evaluate a semantic governance framework that supports structured assessment of AI-based digital forensic tool procurement documentation against Article 15 accuracy, robustness, and cybersecurity requirements, while also identifying related fundamental rights and forensic governance risks.

4. Methodology

The research follows a design-oriented methodology. The purpose is to construct and evaluate a governance artefact that prototypes semantic-driven procurement assessment. The framework is not designed to perform model benchmarking, legal certification, or automated compliance determination. Instead, it supports structured decision-making by making legal and forensic safeguards explicit and traceable within procurement documentation.

The design process has five stages. First, relevant legal and governance sources are identified, including the EU AI Act, EU Model Contractual Clauses for AI procurement, IEEE 3119-2025 on AI procurement, public procurement principles, GDPR, the Charter of Fundamental Rights, and digital forensic principles [12, 3, 1, 6, 7]. Second, these requirements are translated into procurement-level safeguards. Third, the safeguards are represented in a semantic model. Fourth, a deterministic screening layer evaluates procurement artefacts for explicit textual evidence of safeguards. Fifth, results are presented through coverage reports, traceability tables, risk summaries, and HTML reporting.

The ontology development follows the Linked Open Terms methodology, which supports requirements specification, implementation, publication, and maintenance of ontology artefacts [13]. The ontology links legal provisions, granular sub-provisions, competency questions, governance safeguards, evidence indicators, risk dimensions, and structural procurement-risk outputs. In the RDF implementation these are semantic model concepts with explicit relation types; the paper uses camel-case names only where it refers to implementation identifiers.

The left-to-right arrows in Figure 1 are a reader-oriented traceability order rather than an assertion that each class is a `prov:wasDerivedFrom` derivation of the previous class. In the implementation, provenance is represented separately using PROV-O-style links from generated artefacts back to source material and script runs, for example `prov:wasDerivedFrom` for output provenance [14]. Domain links in MTALO are expressed as named traceability relations between requirements, questions, safeguards, evidence indicators, and risk outputs.

The prototype evaluation assesses whether these semantic links can be represented, validated, and used to produce procurement risk outputs. The evaluation does not determine legal compliance or model-level statistical performance. It evaluates whether the framework can represent legal obligations, map them to safeguards, detect evidence indicators in procurement artefacts, and produce reproducible procurement governance outputs.

The screening layer uses deterministic HIT/MISS evidence detection. A HIT means that explicit textual evidence was detected for a GovernanceSafeguard. A MISS means that expected evidence was not detected in the analysed procurement material. Coverage is calculated as:

$$\textit{Coverage} = \text{evidenced GovernanceSafeguards} \,/\, \text{expected GovernanceSafeguards}$$

This coverage score indicates alignment with documentary evidence only. It is not a legal compliance score, a conformity assessment, or a model performance score.

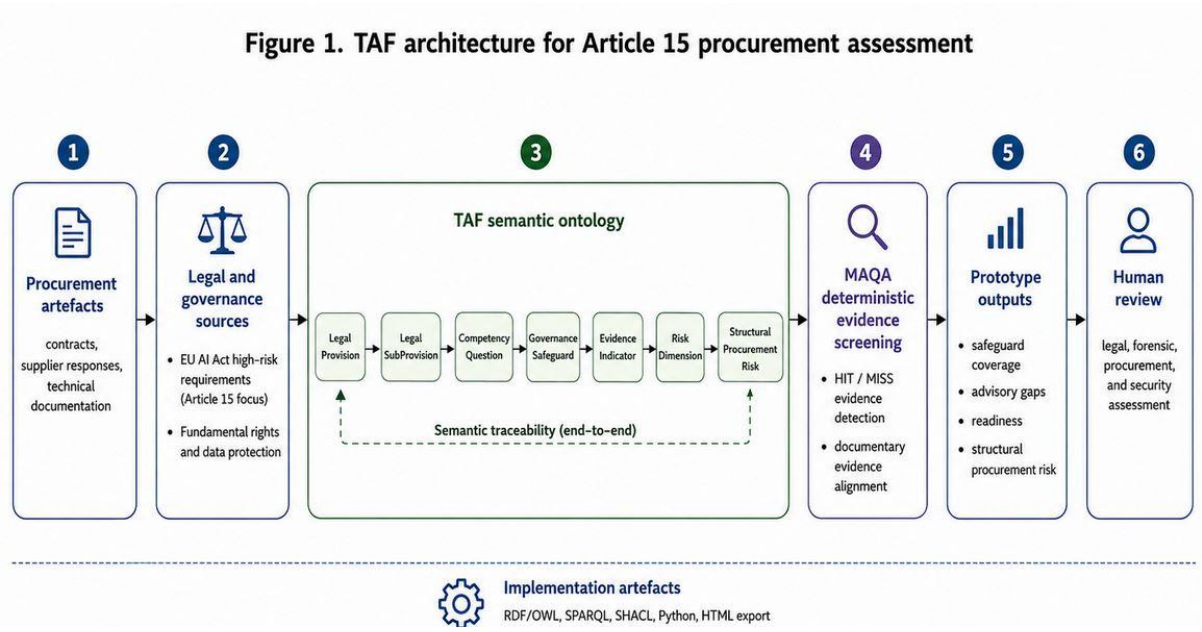

Figure 1: TAF architecture for Article 15 procurement assessment. The diagram shows the flow from procurement artefacts and legal-governance sources into the TAF semantic ontology, where semantic model concepts for legal provisions, legal sub-provisions, competency questions, governance safeguards, evidence indicators, risk dimensions, and structural procurement-risk outputs are linked through an end-to-end traceability model. The arrows show traceability and order-of-assessment links; provenance/derivation of generated artefacts is modelled separately using PROV-O. The ontology output is then screened by MAQA to produce safeguard coverage, advisory gaps, readiness, and structural procurement-risk outputs for human legal, forensic, procurement, and security review.

5. The TAF Framework

5.1. Framework Overview

TAF has three main layers: a semantic governance layer, a deterministic screening layer, and a reporting layer. The semantic governance layer represents legal provisions, sub-provisions, competency questions, governance safeguards, evidence indicators, risk dimensions, and structural procurement risks. The deterministic screening layer evaluates procurement artefacts, including supplier questionnaires, tender responses, contract clauses, model cards, validation reports, technical documentation, cybersecurity documentation, data processing agreements, and AI governance statements. The reporting layer produces safeguard coverage reports, Article 15 mappings, legal traceability tables, risk summaries, and procurement follow-up recommendations.

5.2. Core Semantic Model

Table 1 summarises the core semantic model.

The implemented ontology validation confirms these semantic links and reports 12 legal provisions, 33 legal sub-provisions, 31 competency questions, 12 governance safeguards, 3 evidence indicator categories, 4 risk dimensions, 7 structural procurement risk classes, 3 active contract instances, and 12 full-chain rows.

5.3. Mapping Article 15 to Procurement Safeguards

Article 15 is operationalised in TAF through procurement evidence requirements. The framework treats Article 15 as a legal source that must be translated into supplier obligations and reviewable evidence.

Accuracy is mapped to declared task-specific metrics. For example, if a tool classifies documents as

Table 1
Core TAF ontology classes.

Semantic model concept	Role in TAF
Legal provision (`LegalProvision`)	Represents a legal or governance source, such as the EU AI Act Article 15.
Legal sub-provision (`LegalSubProvision`)	Represents a granular requirement within a legal provision.
Competency question (`CompetencyQuestion`)	Defines the assessment question that scopes a safeguard.
Governance safeguard (`GovernanceSafeguard`)	Represents an operational procurement safeguard.
Evidence indicator (`EvidenceIndicator`)	Represents documentary or textual evidence of a safeguard.
Risk dimension (`RiskDimension`)	Aggregates safeguard evidence into a procurement risk dimension.
Structural procurement risk (`StructuralProcurementRisk`)	Represents the final risk-oriented procurement output.

Table 2
Article 15 mapping to procurement safeguards.

Article 15 requirement	Procurement interpretation	Example evidence indicators	Forensic risk if absent
Accuracy	Supplier defines task-specific accuracy and performance levels.	Accuracy metric, precision, recall, error rate, validation report.	Unsupported reliance on inaccurate outputs.
Robustness	The tool performs reliably under foreseeable forensic conditions.	Robustness test, stress test, adversarial input, failure mode.	Weak performance under noisy or adversarial evidence conditions.
Cybersecurity	The tool protects models, evidence data, logs, prompts, and outputs.	Vulnerability, hardening, penetration test, access control, encryption.	Compromised evidence integrity or exposure of sensitive data.
Lifecycle consistency	Supplier maintains performance and security over time.	Monitoring, versioning, update, retraining, change control.	Degradation after deployment or an unreviewed model change.
Limitations	Supplier discloses known limitations and unsuitable uses.	Limitation, intended purpose, failure condition, instructions for use.	Over-trust in outputs beyond the validated forensic context.

relevant or irrelevant, procurement documentation should specify the metric, benchmark data, validation method, false-positive and false-negative thresholds, and limitations. Robustness is assessed by testing under foreseeable forensic conditions, such as noisy data, incomplete logs, corrupted files, multilingual communications, adversarial prompts, and changing operational environments. Cybersecurity is mapped to controls protecting the AI system, model, evidence data, logs, prompts, and outputs.

5.4. Mapping Fundamental Rights to Procurement Requirements

The framework links fundamental rights to procurement safeguards because rights risks arise from technical and organisational design choices. Privacy and data protection are operationalised through safeguards for data minimisation, purpose limitation, retention, access control, logging, and secure processing [3]. Non-discrimination is operationalised through bias testing, representative validation data, human review, and disparate impact analysis [2]. Fair procedures and effective remedies are operationalised through transparency, documentation, explainability, evidence traceability, and reviewability.

In in-house investigations, these safeguards are particularly important. Employees and contractors may not fully understand how AI tools analyse their data. Procurement documentation should therefore

Table 3
Prototype procurement use-case results.

Use case	Scenario and contract	Evidence and readiness	Risk and main review gap
Use Case 1	AI provider to AI deployer using GPAI. Contract 1: 709560452, Provision of CRIMES HQ Cellebrite Licence and Support.	Core safeguards: 8/8 (100.0%). Advisory gaps: 2. Readiness: 100/100.	Moderate. Gap: fundamental rights impact assessment.
Use Case 2	AI provider to AI deployer without GPAI. Contract 2: 708269450, Service Police Cybercrime Centre.	Core safeguards: 7/8 (87.5%). Advisory gaps: 2. Readiness: 88/100.	High. Gap: forensic chain of custody and data integrity.
Use Case 3	AI deployer procures GPAI directly. Contract 3: York Global Initiative for Safe Autonomy Building.	Core safeguards: 8/8 (100.0%). Advisory gaps: 1. Readiness: 100/100.	Moderate. Gap: law-enforcement specific compliance, Annex III.

require tools to support auditability, human review, and proportional use.

6. Prototype Evaluation

6.1. Evaluation Material

The prototype evaluation uses a static exported prototype report generated by the TAF/MAQA checker. The paper does not rely on a password-protected or mutable frontend as a cited source. Instead, the reported figures are treated as outputs from a frozen evaluation export.

The exported report contains three relevant components. The coverage interpretation component defines HIT/MISS and coverage. The use-case demonstration component provides the three procurement use-case results. The validation component provides the active-run and ontology-validation summaries. This separation prevents the paper from mixing method explanations, contract-level outputs, validation checks, and legal interpretation into a single results section.

The online prototype demonstration provides the static exported checker output used to derive the reported use-case summaries, while the WIDOCO documentation provides an inspectable HTML view of the ontology terms and structure. The prototype was implemented as a Python 3 command-line pipeline using `download.py` for public procurement dataset retrieval and filtering and `mcc_ai_checker.py` for TAF/MAQA screening. The implementation uses JSON/JSONL and CSV/XLSX intermediates, RDFLib for RDF/OWL serialisation to RDF/XML, SHACL shapes, SPARQL query files, WIDOCO/WebVOWL ontology documentation, and static HTML reporting. Source code, ontology files, shapes, queries, and release artefacts are made available through the persistent project URI in Table 5.

Figure 2 summarises the evaluation workflow used to move from the frozen prototype export to the workshop-paper results. Figure 3 then gives a fuller end-to-end view of the implemented TAF artefact pipeline, including dataset preparation, semantic assessment, checker outputs, ontology export, and provenance.

6.2. Procurement Use Cases

The prototype uses three AI procurement value-chain configurations: an AI provider supplying a forensic system to an AI deployer with GPAI involvement; an AI provider supplying a forensic system without GPAI; and an AI deployer procuring GPAI directly. These configurations allow the framework to test different positions in the AI value chain. This matters because Article 15 responsibilities and procurement risks may differ depending on whether the organisation buys a complete AI-enabled forensic system, buys a non-GPAI forensic system, or directly procures GPAI capability for forensic use.

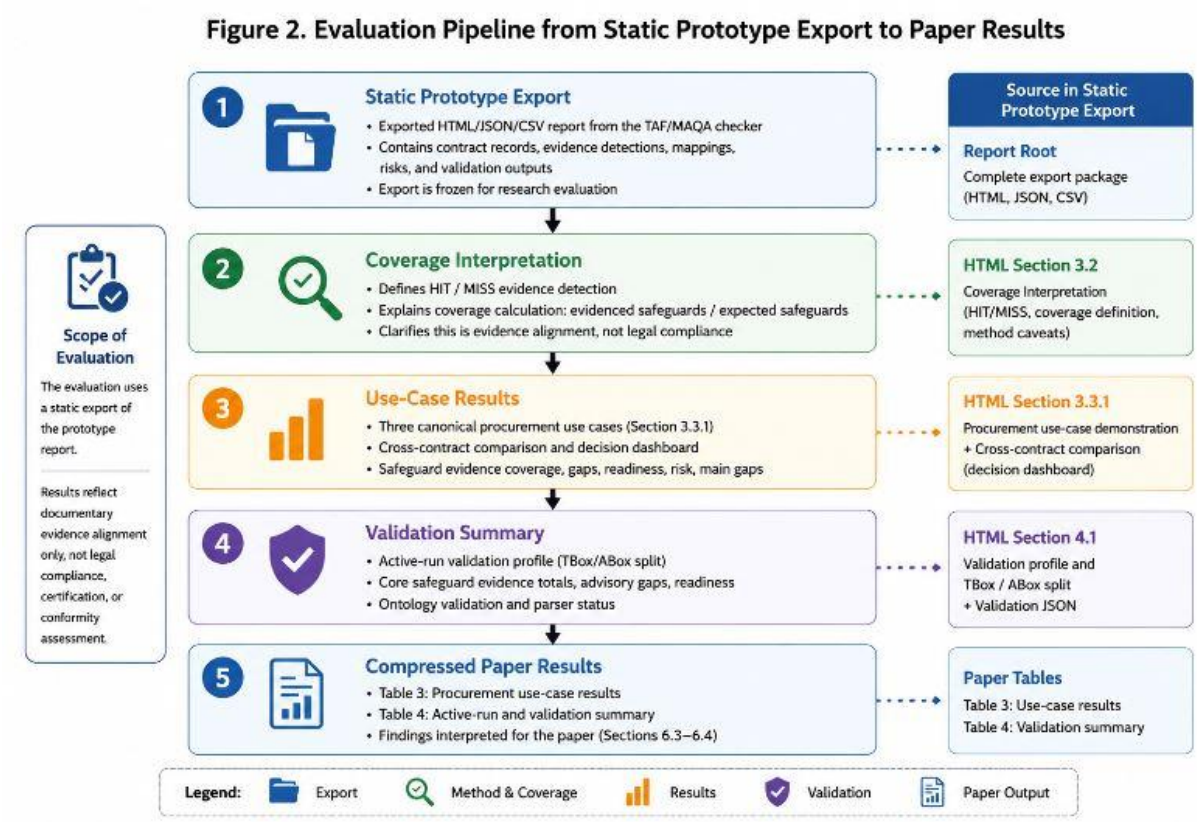

Figure 2: Evaluation pipeline process used to move from the frozen prototype export to use-case summaries, ontology validation checks, and workshop-paper results. The pipeline separates coverage interpretation, use-case extraction, active-run validation, ontology-validation outputs, and results synthesis so that contract-level evidence, semantic validation, and legal interpretation remain distinct.

6.3. Use-Case Results

The results show that the framework can distinguish between procurement records with full core safeguard evidence coverage and a record with a specific missing core safeguard. Use Case 2 is particularly important because it demonstrates that high coverage does not necessarily imply low structural risk. Although 7 of 8 core safeguards were evidenced, the missing safeguard concerns forensic chain of custody and data integrity, both of which are central to digital forensic reliability. The framework, therefore, assigns a higher StructuralProcurementRisk output.

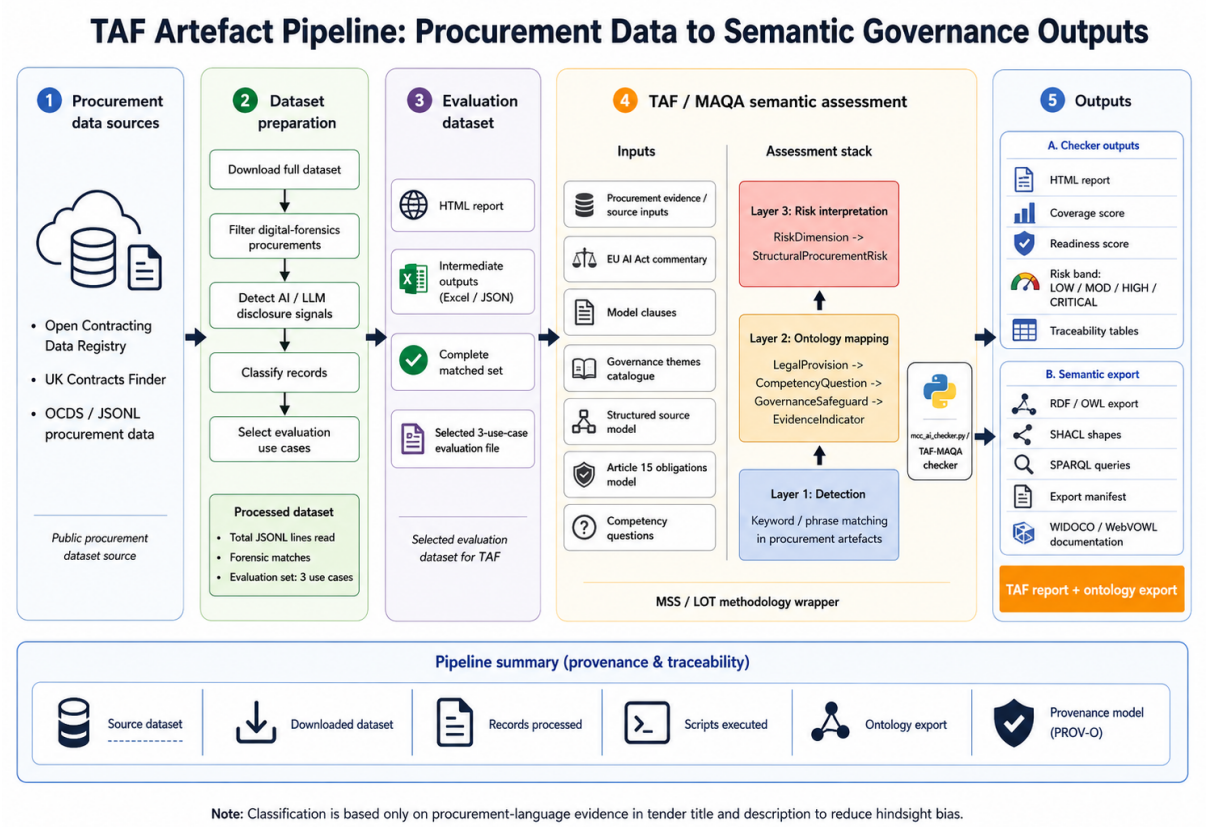

Figure 3: End-to-end TAF artefact pipeline from procurement data to semantic governance outputs. The figure shows how public procurement data from the Open Contracting Data Registry and UK Contracts Finder are downloaded and filtered for digital forensic procurements, screened for AI/LLM disclosure signals, organised into an evaluation dataset, and processed by the TAF/MAQA checker. The checker combines procurement evidence, legal and governance sources, ontology inputs, and Article 15 competency mappings to produce coverage and readiness scores, risk bands, traceability tables, and semantic exports including RDF/OWL, SHACL, SPARQL, WIDOCO, and provenance artefacts.

6.4. Active-Run and Artefact Validation Summary

Table 4 is generated from `mtalo_complete_protege_ready_validation.json`.

Table 4: Active-run and semantic validation summary.

Metric	Result
Active procurement contract groups	3
Core safeguards evidenced	23/24
Core safeguard evidence coverage	95.8%
Advisory review gaps	5
Average readiness	96.0/100
High-risk cases	1
Moderate-risk cases	2
Low-risk cases	0
Ontology validation status	PASS
RDF/XML parser status	PASS
Full-chain rows	12

The active-run result should be read as evidence coverage, not empirical classification accuracy. The framework has not yet been evaluated against independently reviewed `expected_status` labels. Therefore, precision, recall, F1, false positives, false negatives, and classification accuracy remain the evaluation metrics for future work.

6.5. Structural Procurement Risk Interpretation

StructuralProcurementRisk is the framework's final risk-oriented output. It is derived from evidence coverage, safeguard strength, advisory gaps, and aggregated RiskDimension results. It should not be treated as a legal conclusion.

The full traceability tables are useful for audit and debugging, but they are too large for a workshop paper. The paper therefore presents `StructuralProcurementRisk` as a compact output column and refers to Figure 1 and Table 1 for the semantic traceability model rather than repeating the same class sequence inline. This is sufficient to show the semantic contribution without overwhelming the reader.

7. Discussion

TAF contributes to trustworthy AI procurement by operationalising legal and governance obligations into procurement-level safeguards. Article 15 requires appropriate levels of accuracy, robustness, and cybersecurity, but procurement teams need practical ways to ask for and review supplier evidence [1]. TAF provides a structured vocabulary and traceability model for doing so.

The framework is standards-oriented in three respects. First, it translates legal obligations into reusable procurement controls. Second, it creates machine-readable assessment artefacts using RDF/XML, SHACL, SPARQL, JSON, Python outputs, and HTML reporting [8, 10, 11]. Third, it supports standardised evidence requests, allowing buyers to ask suppliers for accuracy metrics, robustness testing, cybersecurity controls, logging capabilities, data governance documentation, human oversight controls, and evidence of the impact on fundamental rights, using a consistent vocabulary. This complements IEEE 3119-2025 by providing a semantic representation of evidence requests and review gaps for the specific case of rights-sensitive AI-based digital forensic procurement [7].

For in-house digital forensic teams, the framework supports earlier identification of tool risks. It helps teams ask whether an AI tool is suitable for a specific forensic purpose, rather than relying on generic AI performance claims. Missing audit logs affect the chain of custody and the reviewability

Table 5
Online resources and artefact availability.

Resource	Availability
Prototype demo	http://trinners.com/TAF_NXDG2026_Artefact_v1/mcc_ai_checker_output.html. Static exported TAF/MAQA checker output showing coverage, advisory gaps, readiness, and StructuralProcurementRisk outputs.
Ontology documentation	http://trinners.com/TAF_NXDG2026_Artefact_v1/Widoco/. WIDOCO-generated documentation for the TAF ontology, including human-readable ontology documentation and term-level inspection.
Project repository / persistent URI	https://w3id.org/taf. Persistent landing page for the open-source repository and release artefacts, including source code, ontology files, SHACL shapes, SPARQL queries, documentation, and versioned exports.

of records. Missing accuracy metrics affect reliability. Missing oversight controls increase the risk of automation bias. Missing data governance controls increase privacy and data protection risk.

The framework also supports collaboration between legal, procurement, forensic, security, and risk teams. Legal teams can examine source provisions. Forensic teams can examine the integrity and traceability of evidence. Procurement teams can examine supplier evidence. Security teams can examine cybersecurity controls. Risk teams can examine `StructuralProcurementRisk` outputs. Because MTALO concepts, SHACL constraints, SPARQL queries, JSON taxonomies, and MAQA screening rules are represented as declarative artefacts, they can be revised as legal requirements, standards, regulatory guidance, or local organisational policies change. This is important for AI procurement governance because the assessment model can evolve without rewriting the whole prototype pipeline.

8. Limitations and Future Work

The framework has five main limitations. First, it evaluates procurement documentation rather than the behaviour of deployed systems. A procurement artefact may contain a safeguard claim even if the safeguard is not technically implemented. Second, it does not perform model-level statistical validation. Article 15 accuracy ultimately requires a technical assessment of performance in context. Third, it does not determine legal compliance. Compliance depends on legal interpretation, organisational context, contractual terms, data processing conditions, deployment facts, and regulatory guidance. Fourth, deterministic lexical screening may miss semantically equivalent wording or detect weak keyword evidence. Fifth, the current evaluation uses a limited prototype scenario and selected procurement artefacts.

Future work should extend the ontology to include additional legal, procurement, and forensic standards, expand the evidence indicator taxonomy, strengthen SHACL validation, refine SPARQL queries, and test the framework against larger procurement datasets. A specific future-work task is to demonstrate maintainability by applying a controlled change to the declarative model, for example updating requirements in response to EU Digital Omnibus changes to the AI Act, new European Commission guidance, CEN/CENELEC JTC 21 or ISO/IEC JTC 1/SC 42 standards, ENISA guidance, or sector-specific rules [15]. Further work should also add independently reviewed `expected_status` labels to enable measurement of precision, recall, F1, and false-positive behaviour. This would shift the evaluation from prototype-evidence alignment to empirical validation.

9. Online Resources and Artefact Availability

To support review, transparency, and reuse of the semantic artefacts, the project provides online resources for the prototype outputs, ontology documentation, and public repository landing page.

These resources make the framework inspectable beyond the static paper and support open-access expectations in semantic web venues.

Where access to live or sensitive prototype material cannot be fully open during review, the paper links to static documentation and exported demonstration outputs so reviewers can inspect the semantic model, mappings, and reporting structure without relying on a mutable or private system.

10. Conclusion

This paper proposes TAF, a semantic governance framework for assessing Article 15 safeguards in the procurement of AI-based digital forensic tools. The framework addresses a practical gap between high-level legal obligations and procurement-level evidence. It operationalises legal provisions into competency questions, governance safeguards, evidence indicators, risk dimensions, and structural procurement-risk outputs.

The framework is paired with MAQA, a deterministic screening method that checks procurement artefacts for explicit evidence of safeguards. The implemented artefact includes RDF/XML, SHACL, SPARQL, JSON taxonomy files, a Python screening pipeline, and HTML reporting. Validation confirms the presence of the semantic traceability links and demonstrates that procurement artefacts can be assessed for evidence coverage in a reproducible way.

TAF does not certify compliance, replace legal judgment, or benchmark model performance. Its contribution is to make AI forensic procurement safeguards explicit, traceable, queryable, and reviewable. In high-risk, rights-sensitive forensic contexts, procurement should not rely on generic claims of accuracy, security, or compliance. It should require structured evidence. TAF provides a standards-oriented semantic approach for doing so.

References

[1] European Parliament and Council, Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence, Official Journal of the European Union, 2024.

[2] European Union, Charter of Fundamental Rights of the European Union, Official Journal of the European Union, 2012.

[3] European Parliament and Council, Regulation (EU) 2016/679: General Data Protection Regulation, Official Journal of the European Union, 2016.

[4] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3 ed., Academic Press, London, 2011.

[5] ISO/IEC, ISO/IEC 27037:2012: Information technology – Security techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, International Organization for Standardization, 2012.

[6] Public Buyers Community, Procurement of AI, Updated EU AI Model Contractual Clauses, Public Buyers Community, 2025.

[7] IEEE Standards Association, IEEE 3119-2025: IEEE Standard for the Procurement of Artificial Intelligence and Automated Decision Systems, IEEE Standards Association, 2025. URL: https://standards.ieee.org/ieee/3119/10729/.

[8] R. Cyganiak, D. Wood, M. Lanthaler, RDF 1.1 Concepts and Abstract Syntax, W3C Recommendation, 2014.

[9] P. Hitzler, M. Krötzsch, B. Parsia, P. F. Patel-Schneider, S. Rudolph, OWL 2 Web Ontology Language Primer, W3C Recommendation, 2012.

[10] S. Harris, A. Seaborne, SPARQL 1.1 Query Language, W3C Recommendation, 2013.

[11] H. Knublauch, D. Kontokostas, Shapes Constraint Language (SHACL), W3C Recommendation, 2017.

[12] European Parliament and Council, Directive 2014/24/EU on Public Procurement, Official Journal of the European Union, 2014.

[13] M. Poveda-Villalón, A. Fernández-Izquierdo, M. Fernández-López, R. García-Castro, LOT: An Industrial Oriented Ontology Engineering Framework, Engineering Applications of Artificial Intelligence 111 (2022) 104755.
[14] T. Lebo, S. Sahoo, D. McGuinness, et al., PROV-O: The PROV Ontology, W3C Recommendation, 2013. URL: https://www.w3.org/TR/prov-o/.
[15] European Commission, Digital Omnibus on AI Regulation Proposal, European Commission, Shaping Europe's digital future, 2025. URL: https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal.