OSINT + KYC

DUE DILIGENCE REPORT

Illustrative Investigation Report

SUBJECT IDENTIFIER

AB-01

Pseudonymized public-report copy

Report ID	INFRA-KYC-DEMO-2026-001
Report date	4 September 2026
Classification	CONFIDENTIAL - DEMONSTRATION
Provisional decision	**CONDITIONAL PASS - EDD REQUIRED**

This document is a methodological and product-demonstration sample based on public-source material. It is not a substitute for authoritative identity verification, licensed sanctions screening, legal advice or a final AML/KYC decision.

Document Control and Confidentiality

Controlled report metadata, use restrictions and privacy treatment

Control field	Value
Document title	INFRA OSINT + KYC Due Diligence Report
Report identifier	INFRA-KYC-DEMO-2026-001
Version	1.0
Report date	4 September 2026
Prepared by	INFRA AI - OSINT and KYC Intelligence
Subject reference	AB-01
Classification	Confidential - Illustrative Sample
Purpose	Demonstrative pre-engagement due diligence and platform-report design
Status	Provisional - Enhanced Due Diligence outstanding
Review trigger	New authoritative evidence, material corporate change, sanctions/PEP alert or adverse-media development

Confidentiality notice

This report contains personal, corporate and reputational information. It may be used only for the stated due-diligence purpose, by authorised personnel with a demonstrable need to know. Redistribution, publication, secondary profiling or operational use outside the approved purpose is prohibited unless separately authorised and legally justified.

Pseudonymization and direct identifiers

The subject is represented as AB-01. The complete legal identity, date of birth, contact details, document numbers and source locators that reveal direct identifiers are excluded from this copy. A production platform would store the identity mapping in a separate encrypted vault with stricter access controls and independent audit logging.

Important use limitation
An OSINT report is an analytical input, not a verdict. Public-source absence does not prove that an event never occurred, and public-source association does not prove misconduct. Final decisions must rely on proportionate, lawful and subject-specific evidence.

Data-protection principles

- Purpose limitation: collect and use information only for the defined decision or investigation. [S02]
- Data minimization: exclude private-life details that do not affect the stated risk question. [S02]
- Accuracy and correction: retain contradictions and permit correction or challenge of material facts. [S02]
- Security and accountability: control access, preserve audit logs and document automated processing. [S02]
- Retention control: delete or archive data according to legal, contractual and evidential requirements. [S02]

Contents

Major report sections and appendices

Navigation note
Page numbers refer to this generated PDF version. Source locators that expose direct identifiers are suppressed from the visible report and retained only in the restricted evidence store.

Executive Summary

Provisional decision, principal findings and unresolved checks

IDENTITY RESOLUTION	OVERALL RISK	EVIDENCE CONFIDENCE	DECISION
HIGH	MODERATE	MEDIUM	CONDITIONAL PASS

Assessment

AB-01 was resolved with high confidence as a cybersecurity and artificial-intelligence professional associated with two Estonian technology companies. The professional identity is coherent across historical profiles, company information, institutional event listings, an international technology programme and current edited media. [S03-S08]

Both associated companies are publicly listed as consortium partners in the EU-supported VANTAGE cybersecurity project. An institutional SI-CERT source identifies the project grant, consortium, duration, eligible costs and EU contribution. Edited media separately describes AB-01 as the project technical leader, although that exact personal role was not verified from the grant agreement itself. [S04, S08, S12]

One associated company was reported with a minor tax debt of approximately EUR 122 and outstanding turnover or VAT declarations as at the report date. The annual report was shown as submitted. This is a corporate-compliance review flag, but the amount and apparent nature do not independently indicate serious financial misconduct. [S09, S10]

A 2007 edited-media article associates AB-01, through a historical online handle, with the Telecom Italia Tiger Team and related organisations discussed in a broader investigation. The accessible article identifies another person as arrested. It does not report that AB-01 was arrested, charged or convicted, and it does not establish a specific unlawful act by AB-01. The item is therefore historical adverse-media association, not proof of criminal conduct. [S13, S14]

Decision rationale

Conditional pass - Enhanced Due Diligence required
No verified disqualifying evidence was identified in the reviewed public sources. Final approval remains conditional on authoritative identity verification, sanctions and PEP screening, direct corporate-tax confirmation, and resolution of the historical legal context through subject-specific primary evidence.

Decision component	Summary
Positive / mitigating	Coherent identity; sustained cybersecurity profile; institutional conference participation; transparent reported ownership; active EU-project associations.
Material review flags	Historical adverse-media association; minor corporate tax/declaration issue; extensive public identity exposure.
Unassessed areas	Identity-document authenticity; liveness; authoritative sanctions/PEP; criminal record; source of funds/wealth; Dark Web and credential exposure.
Decision threshold	Pass only after completion of the mandatory authoritative checks and adjudication of false positives or unresolved findings.

1 Report Purpose and Required Characteristics

A defensible OSINT and KYC report is a controlled decision record supported by traceable evidence. It must explain who was investigated, why the investigation was lawful and necessary, how records were attributed, what remains uncertain, and how the evidence supports the decision. It should not become an unstructured collection of search results or an automated accusation mechanism.

Core report characteristics

Component	Required content	Operational purpose
Report control	Case ID, report ID, version, date, analyst, requester, classification, jurisdiction, retention and approval status.	Prevents uncontrolled or obsolete copies from being treated as current.
Purpose and legal basis	Defined decision, lawful basis, permitted use, necessity and proportionality.	Limits mission creep and irrelevant collection.
Scope	Countries, languages, time range, source classes, search depth, exclusions and limitations.	Makes absence-of-evidence conclusions interpretable.
Subject identification	Pseudonym, protected identity mapping, known variants, nationality, date of birth and document-verification status.	Separates identity proof from analytical profiling.
Entity resolution	Matching attributes, confidence, namesakes, exclusions and contradictory records.	Reduces false positives and inappropriate record merging.
KYC screening	Identity, address, sanctions, PEP, watchlists, enforcement and periodic review status.	Supports regulated onboarding and monitoring.
Professional verification	Roles, employers, dates, education, qualifications, publications, events and discrepancies.	Tests declared history against independent evidence.
KYB and ownership	Registrations, directors, shareholders, UBOs, group structure, filings, insolvency and tax indicators.	Exposes corporate-control and shell-company risk.
Financial context	Source of funds, source of wealth, revenue, assets and inconsistencies when legally relevant.	Avoids confusing company turnover with personal wealth.
Adverse media and legal matters	Allegation, investigation, charge, trial, conviction, acquittal or dismissal, kept explicitly separate.	Prevents guilt by headline.
Digital and cyber footprint	Domains, accounts, infrastructure, impersonation, breach exposure and Dark Web findings where authorised.	Captures modern identity and operational risk.
Relationship analysis	Links among people, companies, addresses, domains, wallets, projects and events.	Shows networks without treating association as proof.
Timeline and geography	Chronology, role transitions, location consistency and impossible overlaps.	Reveals fabricated histories and temporal conflicts.
Contradiction register	Competing dates, amounts, ownership claims, source disagreements and resolution status.	Preserves uncertainty instead of deleting inconvenient facts.
Risk assessment	Separate dimensions for severity, confidence, evidence quality, recency and mitigating factors.	Produces explainable, reviewable decisions.
Decision and actions	Pass, conditional pass, EDD, reject or insufficient information; required documents and monitoring.	Turns analysis into a reviewable operational outcome.
Evidence appendix	Source, retrieval time, extract, translation, screenshot, archive reference and hash.	Supports reproducibility and evidential integrity.
Privacy and audit	Redactions, access, retention, correction, analyst actions and automated-processing logs.	Demonstrates lawful and accountable processing.

Required analytical separation

- Identity-match confidence must be independent from the seriousness of a finding.
- Evidence confidence must be independent from risk severity.

- Observed facts, subject declarations, third-party reporting and analyst inference must be labelled separately.
- Association must not be converted into responsibility without subject-specific evidence.
- No-result screening must be described as unconfirmed absence unless authoritative coverage is known.

2 Scope and Limitations

Defined purpose

This illustrative investigation supports a pre-engagement due-diligence decision concerning AB-01 and associated corporate entities. It demonstrates the structure and analytical behaviour expected from an INFRA OSINT + KYC platform. It does not constitute a completed regulated KYC file.

Public-source coverage

Scope dimension	Coverage
Languages	English, Italian, Estonian and Slovenian source material
Time horizon	Historical records through 4 September 2026
Source classes	Corporate-information services, institutional project sites, conference programmes, professional profiles, edited media and public search results
Entity classes	Individual, corporate entities, EU project, institutions, event appearances and historical media references
Collection mode	Public-source review; no covert interaction, credential use or intrusive system access

Checks not performed

- Government identity-document authentication and biometric liveness verification
- Authoritative address verification
- Licensed sanctions, PEP, close-associate and watchlist screening
- Official criminal-record retrieval or direct court-file access
- Bank-account, transaction, source-of-funds or source-of-wealth analysis
- Dark Web, compromised-credential or breach-corpus investigation
- Facial recognition or biometric comparison
- Intrusive infrastructure scanning
- Direct contact with employers, authorities, project coordinators or the subject

Interpretation of scope
The report can support triage and determine what must be verified next. It cannot provide authoritative clearance in areas that were not searched using the required primary or licensed sources.

Redaction scope

The visible report excludes complete legal name, birth date, personal identifiers, private contact details, exact residential information, family data, photographs, live travel information and direct source locators that themselves reveal the identity. These fields belong in a restricted evidence layer, not in every analyst export.

3 Methodology and Evidence Governance

The INFRA platform should implement an auditable sequence from intake to decision. Multi-agent AI may accelerate collection, extraction, correlation and drafting, but every material claim must remain linked to inspectable evidence and a human adjudication state.

Investigation workflow

1	**Intake:** Define purpose, legal basis, identifiers, jurisdictions, required source classes and decision threshold.
2	**Collection:** Query authorised public, institutional, licensed and internal sources; preserve raw captures and timestamps.
3	**Normalization:** Extract names, dates, companies, roles, locations, accounts and source metadata into a common schema.
4	**Entity resolution:** Cluster records, compare attributes, identify namesakes, score matches and preserve contradictory evidence.
5	**Analysis:** Build timelines and relationship graphs; identify KYC, KYB, legal, reputational, financial and cyber indicators.
6	**Verification:** Challenge unsupported findings, require corroboration, classify event stage and check source authority.
7	**Decision:** Apply transparent policy rules, document residual uncertainty and assign required EDD or monitoring actions.
8	**Monitoring:** Re-run dynamic checks and alert only on material, novel and sufficiently confident changes.

Evidence classification

Class	Meaning
Verified	Supported by an authoritative primary source with a strong subject match.
Corroborated	Supported by multiple independent sources that materially agree.
Declared	Stated by the subject or a subject-controlled organisation; not independently proven.
Reported	Published by an edited third-party source; content may still require primary verification.

Class	Meaning
Inferred	Derived analytically from evidence; reasoning and uncertainty must be stated.
Unresolved	Evidence is conflicting, incomplete or insufficient for a conclusion.
Excluded	Confirmed namesake, false positive, duplicated record or irrelevant result.

Source-tier model

Tier	Type	Typical use
Tier 1	Authoritative	Government registry, court record, sanctions authority, signed agreement or identity-document result.
Tier 2	Institutional / primary-adjacent	National CERT, official project site, university, conference organiser, regulated entity.
Tier 3	Edited independent source	Established media, professional database or industry publication.
Tier 4	Subject-controlled	Company site, personal profile, social account or self-declared biography.
Tier 5	Unverified / lead only	Forum, anonymous post, scraped data or uncorroborated leak reference.

AI control rule
No AI-generated statement should enter the final report without an evidence reference, a confidence classification and explicit separation between observed fact and inference.

4 Subject Identification and Entity Resolution

Identity cluster

The target cluster was resolved using the combined continuity of a cybersecurity and AI professional history, association with INFRA AI and HAXORAI, founder or management roles, participation in current cybersecurity events, historical telecommunications-security references, and involvement in the VANTAGE project. [S03-S08, S12]

Resolution attribute	Assessment	Confidence
Displayed name variants	Multiple public variants were identified; direct variants are retained only in the restricted identity vault.	High
Professional domain	Cybersecurity, vulnerability assessment, penetration testing, OSINT and artificial intelligence.	High
Corporate associations	INFRA AI OÜ and HAXORAI OÜ.	High
Institutional continuity	Conference, programme and EU-project references align with the corporate and professional profile.	High
Historical continuity	Older professional and media records are consistent with the same technical field.	Medium-high
Namesake exclusion	At least one unrelated public record showed incompatible biographical and professional attributes.	High

Namesake and false-positive handling

Public searches produced multiple records sharing the displayed legal name. A clearly unrelated sports profile presented an incompatible birth year and professional context and was excluded. Name-only matching is therefore insufficient. The platform should require at least two strong identifiers or a larger set of mutually consistent weak identifiers before merging records. [S15]

Assessment dimension	Result
Name-only reliability	Insufficient
Cross-source identity coherence	High
Documentary identity verification	Not performed
Residual false-positive risk	Low after contextual resolution
Final entity-resolution confidence	High
	Identity conclusion The public-source cluster is highly likely to refer to the same subject, but legal identity remains formally unverified until document and liveness checks are completed.

5 Professional Profile

Corroborated professional context

A legacy professional profile states that AB-01 has worked in IT security since 1998, including assessment, investigations, forensics, data recovery and penetration testing, and describes a former leadership role in a telecommunications security team. As a subject-authored or subject-controlled source, these claims are classified as declared rather than independently verified. [S03]

An institutional CyberTECH page independently lists AB-01 as chief executive and founder of an INFRA vulnerability-assessment initiative and describes INFRA as an intelligence framework for computer and network security. [S05]

In 2026, HEK.SI and INFOSEK listed AB-01 as an INFRA AI lecturer on artificial intelligence, hacking, cybersecurity, forensic activity and OSINT. Fortune Italia separately described AB-01 as technical leader of VANTAGE and chief executive of the associated INFRA organisation. [S06-S08]

Claim	Evidence basis	Status	Confidence
Long-term cybersecurity experience	Declared in legacy profile; consistent with later sources.	Declared / corroborated context	Medium-high
Founder / executive role at INFRA	Institutional programme and edited media.	Corroborated	High
Current public speaking	Two 2026 institutional conference listings.	Verified as event listing	High
VANTAGE technical leadership	Edited media description; not checked against contractual project documents.	Reported	Medium
Exact employment history	No employer confirmations or contracts reviewed.	Unresolved	Low
Formal academic qualifications	No diplomas or authoritative education records reviewed.	Unresolved	Low
Work with police / authorities	No contracts or official confirmations reviewed in this sample.	Unresolved	Low

Professional assessment

Assessment
The professional identity is coherent and partly independently corroborated. The strongest verified facts concern public corporate roles, event participation and institutional project associations. Claims about exact employment periods, qualifications and sensitive public-sector engagements require primary documentation.

6 Corporate and Beneficial-Ownership Findings

Entity C-01 - INFRA AI OÜ

Field	Public-source finding
Registration	Reported registered on 29 August 2024
Principal activity	Information technology and computer services
Share capital	EUR 300
Management / ownership	AB-01 reported as board member and sole shareholder
VAT status	Registration reported from January 2026
Annual report	2025 annual report shown as submitted
Tax position	Approximately EUR 121-122 reported outstanding
Declaration status	Sources differed between one outstanding VAT declaration and three overdue turnover declarations
Court / enforcement indicators	No company court orders, hearings, decisions or bailiff-enforcement entries shown by the reviewed aggregator

Assessment: low-to-moderate corporate-compliance risk. The monetary amount is minor, but missing declarations and inconsistent source data require direct verification with the Estonian authorities. [S09, S10]

Entity C-02 - HAXORAI OÜ

Field	Public-source finding
Registration	Reported incorporated on 27 August 2024
Share capital	EUR 900
Management / ownership	AB-01 reported as one of three managers and owners
2025 sales revenue	EUR 27,285
2025 operating result	EUR 1,961 operating loss
Tax position	No tax debt reported on the review date
Declaration status	Shown as correctly filed on the review date

Assessment: no material corporate-compliance indicator was identified in the reviewed data. The financial values describe the company and must not be treated as evidence of AB-01's personal income or wealth. [S11]

Ownership transparency assessment

Dimension	Assessment
Reported direct ownership	Transparent in the reviewed registry-derived sources
Reported management roles	Consistent with professional and project sources
Complex offshore structure	Not identified in the reviewed scope
Nominee / shared-director indicators	Not identified in the reviewed scope
Authoritative UBO verification	Not performed
Corporate risk level	Low to moderate, driven principally by the C-01 filing/tax flag

7 EU Project and Institutional Associations

The official VANTAGE project website and SI-CERT both list INFRA AI OÜ and HAXORAI OÜ among the consortium partners. The project concerns multi-agent AI, automated vulnerability assessment, penetration testing and cyber investigation. [S04, S12]

Project attribute	Reported value
Grant agreement	101249800
Start date	1 January 2026
End date	31 December 2028
Duration	36 months
Total eligible costs	EUR 7,837,116.56
EU contribution	EUR 4,988,530.73
Associated subject companies	INFRA AI OÜ and HAXORAI OÜ listed in the consortium
	Financial interpretation The project figures concern the entire consortium. They must not be represented as funds personally received by AB-01 or as amounts allocated entirely to the two associated companies.

Subject role

Fortune Italia identifies AB-01 as the project technical leader. This is credible edited-media evidence but not definitive contractual proof. Final verification would require the consortium agreement, Description of Action, appointment record or confirmation from the coordinator. [S08]

Finding	Status	Confidence
Company participation	Verified through official project and institutional sources	High
Project scope	Consistent across official project and SI-CERT descriptions	High
Personal technical-leader role	Reported by edited media	Medium
Personal financial benefit	Not established from consortium-level budget figures	Not assessed

8 Adverse Media and Legal Matters

Finding AM-01 - historical telecommunications-security article

Field	Assessment
Publication date	8 February 2007
Source type	Established edited media
Subject match	High
Context	Telecommunications security team and related organisations discussed in a broader investigation
Event stage	Association and allegation context
Subject-specific illegal conduct established	No
Subject arrest reported	No
Subject charge or conviction reported	No
Current evidential status	Unresolved historical adverse-media association
Materiality	Moderate
Confidence in article-subject association	High
Confidence in personal wrongdoing	Low

The article maps a historical handle to AB-01 and places the subject within the relevant professional group. Its broader narrative discusses alleged illegal activity involving the surrounding security ecosystem. In the accessible passage, however, the person expressly identified as arrested is another team member. The article does not establish a specific offence by AB-01. [S13]

Negative-news methodology must distinguish allegation, investigation, charge, trial, conviction, acquittal and dismissal. Source credibility, subject match, recency and event maturity affect materiality. [S14]

Analytical conclusion
AM-01 is a legitimate review flag but not evidence of guilt. The correct status is unresolved historical association. It must not be reported as an arrest, charge or conviction.

Required resolution path

- Obtain an official criminal-record certificate where lawful and proportionate.
- Search authoritative judicial records using verified identifiers.
- Collect any relevant dismissal, acquittal, limitation or case-disposition documentation.
- Request a written subject explanation and supporting evidence.
- Reassess using subject-specific primary evidence, not association alone.

No-result treatment

No primary judicial disposition concerning AB-01 was located during the limited public-source review. That result is not a legal clearance. It is recorded as unresolved because the relevant authoritative sources were not comprehensively searched.

9 Sanctions, PEP and Enforcement Screening

Status: incomplete
No obvious exact-match sanctions or PEP signal emerged from the general open-web review. This is not an authoritative clearance. Ordinary search engines are not complete financial-crime databases, and adverse-media screening is separate from sanctions and PEP list screening.

Production requirements

Requirement	Expected implementation
Identity inputs	Verified legal name and variants, date of birth, nationality, residence and relevant jurisdictions
Sanctions sources	Official national, EU, UN and other applicable authorities plus licensed consolidated datasets
PEP sources	Current and former PEPs, family members and close associates where legally permitted
Enforcement sources	Regulators, debarment lists, law-enforcement notices and sector-specific restrictions
Adjudication	Exact identifier comparison, false-positive analysis, source capture, reviewer approval and rationale
Ongoing monitoring	Event-driven rescreening and periodic refresh according to risk tier

Screening disposition

Control	Status	Next action
Sanctions	Not completed	Authoritative and licensed list screening required
PEP / RCA	Not completed	Verified identity and appropriate datasets required
Regulatory enforcement	Partially reviewed in public sources	Direct authority checks required
Criminal-record check	Not completed	Official certificate or lawful authoritative access required
Overall clearance	Cannot be issued	Mandatory screening components remain outstanding

The appropriate status is therefore not completed; an open-web no-result cannot be treated as authoritative clearance. [S14]

10 Digital and Cyber Exposure

AB-01 has a substantial public professional footprint across company pages, social networks, conferences, institutional sites and edited media. This improves professional verifiability but also lowers the effort required to reconstruct the subject identity and business relationships. [S05-S08]

Corporate-information services publicly index direct contact and identity-related fields. Those values are deliberately redacted from this copy. The exposure is relevant to executive impersonation, spear phishing and business-email-compromise risk; it is not evidence of misconduct. [S09]

Indicator	Level	Basis
Public professional visibility	High	Multiple current institutional and media references
Identity reconstruction difficulty	Low	Cross-source corporate and professional links are easy to correlate
Spear-phishing exposure	High	Public role, technical interests and event participation provide targeting context
Executive impersonation exposure	High	Public executive role and company relationships
Business-email-compromise exposure	High	Executive and project context can support credible pretexts
Evidence of actual compromise	Not assessed	No breach or credential-corpus search performed
Dark Web exposure	Not assessed	Outside current scope
Credential exposure	Not assessed	Outside current scope

Recommended defensive monitoring

- Monitor domain registrations, certificate issuance and social profiles that imitate the subject or associated companies.
- Track exposed corporate credentials and breach notifications through lawful licensed sources.
- Detect typosquatted domains, phishing infrastructure and fraudulent recruitment or investment profiles.
- Alert on material Dark Web references only after source reliability and subject match have been assessed.
- Separate cyber-victimisation indicators from integrity or compliance risk in the scoring model.

Cyber-risk interpretation
High exposure means high susceptibility to targeting, not high likelihood of wrongdoing. The platform must preserve that distinction.

11 Contradictions and Uncertainty Register

Contradictions are retained as first-class analytical objects. The platform should never silently choose the most convenient source, average incompatible values or erase a discrepancy because the report looks tidier without it.

ID	Issue	Treatment	Status	Confidence
CR-01	One corporate source reports one outstanding VAT declaration; another lists three overdue turnover declarations.	Retain both values and query the authoritative Estonian tax source.	Open	Medium
CR-02	Institutional sources show inconsistent project end-date information in one secondary summary.	Prefer the detailed SI-CERT funding page provisionally; verify against the grant agreement.	Open	Medium
CR-03	Several people share the displayed legal name.	Resolve using date, profession, companies, geography and historical continuity; exclude incompatible records.	Controlled	High
CR-04	Professional titles vary between founder, chief executive, technical leader, ethical hacker and researcher.	Treat as potentially simultaneous roles; verify formal titles and dates separately.	Open	Medium-high
CR-05	Historical adverse media establishes association but no subject-specific offence or legal outcome.	Do not infer guilt; obtain primary legal disposition and subject response.	Open	High

Uncertainty rules

- A higher-quality source may outweigh a lower-quality source, but the displaced claim remains visible in the audit trail.
- Confidence increases through independent corroboration, exact identifiers and primary evidence; repetition by copied sources does not count as independence.
- Unresolved contradictions must influence the decision or create a specific EDD action.
- The platform should maintain a contradiction group ID linking every competing claim and resolution decision.

12 Risk Assessment

Risk dimensions are scored separately. Severity describes potential impact; confidence describes how strongly the evidence supports the finding. Unassessed controls are not treated as low risk. The overall decision is policy-driven and should not be produced by averaging unrelated risk dimensions into a single unsupported score.

Risk dimension	Provisional level	Confidence	Basis
Identity mismatch	Low	High	Strong cross-source coherence after namesake exclusion
Professional credibility	Low risk / positive evidence	Medium-high	Institutional, corporate, conference and media corroboration
Ownership transparency	Low	Medium-high	Ownership and management consistently reported
Corporate filing and tax compliance	Low-moderate	Medium	Minor debt and outstanding declarations require authoritative verification
Adverse media and legal exposure	Moderate review flag	Medium	Historical association; no subject-specific offence or disposition established
Sanctions and PEP	Unassessed	Low	Authoritative list screening not performed
Fraud / financial crime	No substantiated indicator found	Medium-low	Limited public-source scope
Source of funds and wealth	Unassessed	None	No relevant financial evidence collected
Cyber and impersonation exposure	High	High	Extensive public identity and business exposure
Reputational exposure	Moderate	Medium	Historical article remains discoverable
Overall provisional risk	Moderate	Medium	Driven by unresolved checks, not verified serious misconduct

Decision drivers

Driver class	Assessment
Positive drivers	High-confidence identity resolution; coherent technical career; transparent reported corporate associations; institutional and EU-project participation.
Negative drivers	Historical unresolved adverse-media association; minor corporate compliance discrepancy; high executive-targeting exposure.
Uncertainty drivers	Incomplete sanctions/PEP screening; no official criminal-record check; no identity-document verification; no source-of-funds/wealth review.
Residual-risk treatment	Conditional approval subject to EDD, documentary verification and monitoring.
	Overall risk Moderate provisional risk with medium confidence. The level reflects unresolved mandatory checks and historical context, not a substantiated finding of serious misconduct.

13 Required Enhanced Due Diligence

The following actions are required before final onboarding, high-trust engagement or reliance on the subject for a regulated role.

ID	Action	Domain	Priority	Status
EDD-01	Verify government identity documents, date of birth, nationality and liveness.	Identity/KYC	Mandatory	Open
EDD-02	Perform authoritative sanctions, PEP, close-associate, enforcement and watchlist screening.	AML/KYC	Mandatory	Open
EDD-03	Obtain current official Estonian registry and tax extracts for both associated companies.	KYB	Mandatory	Open
EDD-04	Resolve the historical adverse-media item through official judicial documentation and a subject statement.	Legal/reputational	Mandatory	Open
EDD-05	Confirm the VANTAGE role through consortium, grant or coordinator documentation.	Professional/project	Required for role reliance	Open
EDD-06	Verify source of funds and source of wealth where required by the intended transaction.	Financial crime	Conditional	Not started
EDD-07	Review public exposure of personal contact data and implement impersonation monitoring.	Cyber protection	Recommended	Not started
EDD-08	Refresh all dynamic findings immediately before the final decision.	Quality control	Mandatory	Open

Decision gates

- Hard gate: unresolved sanctions or confirmed disqualifying watchlist match.
- Hard gate: identity-document failure, impersonation or material identity contradiction.
- Escalation gate: primary evidence of charge, conviction, fraud, corruption or deliberate misrepresentation.
- Remediation gate: minor filing or tax issue confirmed and promptly corrected with evidence.
- Monitoring gate: material new adverse media, corporate-control change or cyber-impersonation event.

Required reviewer behaviour
Every closed action must contain the document or source reviewed, retrieval date, reviewer, outcome, false-positive rationale and impact on the final decision.

14 Final Disposition

PROVISIONAL DECISION

CONDITIONAL PASS - ENHANCED DUE DILIGENCE REQUIRED

Decision statement

The reviewed public evidence supports a coherent professional and corporate identity. No verified sanctions match, conviction, serious corporate misconduct or other disqualifying fact was established within the reviewed source set. Authoritative screening is nevertheless incomplete and must be completed before final approval.

The 2007 article creates a legitimate historical review requirement but does not justify describing AB-01 as arrested, charged or convicted. The approximately EUR 122 corporate-tax issue and reported outstanding declarations require confirmation or remediation, not disproportionate escalation.

Conditions for final pass

Condition	Pass requirement
Identity	Successful document, liveness and identifier verification
AML/KYC	No unresolved sanctions, PEP or enforcement match
Corporate	Authoritative confirmation of company status, ownership and filing/tax position
Legal	Subject-specific resolution of the historical adverse-media context
Professional	Primary verification of any role or qualification material to the engagement

Final analytical note

Evidence-based conclusion
The report maintains evidential discipline: it records the historical article, limits the claim to what the source supports, identifies missing authoritative evidence and makes final approval conditional on resolving those gaps.

Approved decision statuses for the production platform should be limited to: Pass; Conditional Pass; Enhanced Due Diligence; Reject; or Insufficient Information. Each status must include explicit rationale, reviewer identity, approval date and expiry or review trigger.

Appendix A Source Register

This visible register identifies source classes and domains without displaying direct source locators that contain the subject's complete legal name. Exact URLs, archived copies, screenshots and hashes belong in the restricted evidence store.

ID	Source	Type	Domain / locator	Reliability
S01	FATF Recommendations	International standard / guidance	fatf-gafi.org	High
S02	European Commission - GDPR principles	Official EU guidance	commission.europa.eu	High
S03	Legacy professional networking profile	Subject-controlled / historical profile	Restricted locator	Medium-low
S04	Official VANTAGE project website	Project primary source	vantageproject.eu	High
S05	CyberTECH Network programme profile	Institutional profile	cybertechnetwork.org	Medium-high
S06	HEK.SI lecturer page	Institutional event listing	hek.si	High for event listing
S07	INFOSEK programme and lecturer page	Institutional event listing	infosek.net	High for event listing
S08	Fortune Italia article on VANTAGE	Edited media	Restricted locator	Medium-high
S09	INFRA AI OÜ company profile	Registry-derived business information	inforegister.ee	Medium-high
S10	INFRA AI OÜ company profile	Business-information service	radar.aripaev.ee	Medium-high
S11	HAXORAI OÜ company profile	Business-information service	radar.aripaev.ee	Medium-high
S12	SI-CERT VANTAGE project page	National CERT / institutional	cert.si	High
S13	Historical telecommunications-security article	Established edited media	lespresso.it	Medium-high for publication content
S14	Negative News Screening FAQs	Industry guidance	wolfsberg-group.org	High
S15	Public namesake profile	False-positive exclusion source	Restricted locator	Medium

Source-record requirements

- Exact source URL or dataset identifier
- Publication date and retrieval timestamp in UTC
- Raw capture, rendered screenshot and relevant extract
- Language, translation method and translated text where applicable
- Source tier, author or issuing authority and independence assessment
- Subject-match evidence, claim IDs and contradiction group
- SHA-256 hash and immutable storage reference
- Access restrictions, retention date and legal-basis tag

Appendix B Evidence Field Schema

Every claim should be machine-readable, reviewable and exportable without losing provenance. The following minimum schema supports reproducibility, graph analysis, human review and continuous monitoring.

Field	Purpose
claim_id	Unique immutable identifier for the analytical claim
entity_id	Resolved subject, company, account, asset or event identifier
claim_text	Precisely bounded factual statement or inference
claim_type	Identity, role, ownership, sanctions, legal, adverse media, cyber, financial or other defined category
evidence_class	Verified, corroborated, declared, reported, inferred, unresolved or excluded
source_id	Reference to the preserved source record
source_tier	Authority and reliability classification
publication_date	Date the source content was issued
retrieval_timestamp	UTC time the evidence was collected
subject_match_confidence	Confidence that the record concerns the resolved subject
claim_confidence	Confidence that the claim is factually supported
risk_severity	Potential impact if the claim is true
event_stage	Allegation, investigation, charge, trial, conviction, acquittal, dismissal or not applicable
corroboration_state	Independent sources supporting or contradicting the claim
contradiction_group	Identifier linking mutually inconsistent claims
analyst_inference	Reasoning that goes beyond source text, explicitly marked
review_status	Unreviewed, analyst reviewed, second-line approved, rejected or superseded
reviewer_and_date	Reviewer identity and approval timestamp
monitoring_rule	Condition that should trigger re-evaluation
evidence_hash	Cryptographic hash of preserved evidence

Risk-model constraints

- Do not convert unassessed controls to zero risk.
- Do not raise confidence because multiple websites copied the same original source.
- Do not infer misconduct from network proximity without an independent behavioural indicator.
- Do not let a single overall score hide high-severity low-confidence allegations.
- Retain the evidence and policy rule that produced every decision.

Appendix C Analytical, Legal and Privacy Notes

Analytical limitations

- Public records may be incomplete, delayed, mistranslated, outdated or indexed under variant names.
- Corporate-information aggregators may lag behind authoritative registries and may interpret filing status differently.
- Adverse-media reporting may contain allegations, editorial framing and copied errors; primary legal documents are preferred.
- The absence of a public result does not establish the absence of the underlying fact.
- Automated entity resolution can amplify false positives when common names, shared addresses or copied biographies are present.

Privacy controls for an INFRA production platform

Control	Implementation requirement
Access separation	Identity vault, evidence store and analytical workspace use separate roles and permissions.
Purpose tagging	Every case and claim records the lawful purpose and permitted downstream uses.
Sensitive-data minimization	Private-life, biometric, health, political and family data are excluded unless strictly necessary and lawful.
Export controls	Public, client and law-enforcement exports apply different redaction templates.
Correction workflow	Material subject challenges create a review task without deleting the original audit history.
Retention	Case, evidence and identity data have independent retention and legal-hold rules.
Automated decision control	Human review is mandatory for adverse decisions and material risk escalation.
Security	Encryption, immutable logging, least privilege, anomaly monitoring and secure on-premises deployment options.

Report disclaimer

This illustrative report is not legal advice, a criminal-record certificate, a sanctions clearance, a credit report or a final compliance determination. It demonstrates how INFRA can structure evidence, confidence, risk and action in a combined OSINT + KYC platform. Any operational deployment must be configured for the customer jurisdiction, sector, lawful basis, risk policy and data-source licences.

End of report
Report INFRA-KYC-DEMO-2026-001 - Version 1.0 - 4 September 2026