ANALYTICAL REPORT 04

DIGITAL CAPABILITY READINESS IN EU LAW ENFORCEMENT: EVIDENCE FROM HORIZON FCT PROJECTS

An External Expert Report prepared for ENACT

Main Authors
Mara Mignone
Agnese Raimondi
Valentina Scioneri

August 2026

ENACT.
European Network Against Crime and Terrorism

ABOUT ENACT

ENACT is a knowledge network focused on the fight against crime and terrorism (FCT). The network is funded under the Horizon Europe Framework Programme in Cluster 3 – Civil Security for Society. The project addresses the call topic HORIZON-CL3-2022-SSRI-01-02 'Knowledge Networks for Security Research & Innovation', aiming to collect, aggregate, process, disseminate and make the most of the existing knowledge in the FCT area.

The project aims to satisfy two major ambitions,

- Provide evidence-based support to the decision-makers in the EU research and innovation (R&I) ecosystem in the FCT domain, targeted explicitly at enabling more effective and efficient programming of EU-funded R&I for the fight against crime and terrorism.

- Act as a catalyst for the uptake of innovation by enhancing the visibility and reliability of innovative FCT security solutions.

Funded by
the European Union

REPORT FEEDBACK

We're collecting feedback on this report through the EU Survey Platform, if you'd like to share your thoughts anonymously please click on the link below.

https://ec.europa.eu/eusurvey/runner/enact-report-feedback

COPYRIGHT

DISCLAIMER

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

This report was prepared by external experts outside of the ENACT consortium. The report does not represent the views or opinions of the ENACT project, and all content remains the sole responsibility of the authors.

USE OF AI

Following the ENACT policy for the use of AI, the authors disclose that a Generative AI tool (Claude, Anthropic) was used exclusively as a support to content development activities throughout the preparation of this report, including drafting, summarisation, and condensation of analytical text. No confidential, sensitive, or non-public information was processed by the tool at any stage. All AI-generated content, including references and data summaries, was curated, fact-checked, and verified against source materials by the authors under full human supervision. The authors remain fully responsible and accountable for the quality, accuracy, originality, and integrity of all content in this report, and confirm that the use of Generative AI did not replace expert judgement, critical analysis, or professional responsibility at any point in the report's development.

ACRONYMS

AI	Artificial Intelligence
BGA	Border Guard Authorities
CEPOL	European Union Agency for Law Enforcement Training
CORDIS	Community Research and Development Information Service
DOI	Diffusion of Innovation
EARTO	European Association of Research and Technology Organisations
ECTEG	European Cybercrime Training and Education Group
EU	European Union
EUCST	EU Civil Security Taxonomy
FCT	Fight against Crime and Terrorism
GDPR	General Data Protection Regulation
GIS	Geographic Information System
H2020	Horizon 2020
HE	Horizon Europe
IoT	Internet of Things
IS	Information System
ISF	Internal Security Fund
LEAs	Law Enforcement Agencies
LED	Law Enforcement Directive
OSINT	Open-Source Intelligence
R&I	Research and Innovation
SKB	Structured Knowledge Base
SOPs	Standard Operating Procedures
TAM	Technology Acceptance Model
TOE	Technology–Organization–Environment
WCO	World Customs Organisation

04

EXECUTIVE SUMMARY

This report investigates what "capability" means for European Law Enforcement Agencies (LEAs) adopting Artificial Intelligence (AI)-supported investigative tools, and puts forward a working hypothesis: that the operational value of these tools depends less on their technical sophistication than on agencies' capacity to absorb, govern and embed them into day-to-day practice.

The analysis draws on the following complementary strands of evidence: a review of the academic and policy literature on absorptive capacity, dynamic capabilities, and technology-adoption models; a mapping of thirteen Horizon 2020 (H2020) and Horizon Europe (HE) Fighting Crime and Terrorism (FCT) projects against an organisational readiness framework (Skills, Processes, Coordination, Culture); a primary empirical base of 894 questionnaire responses and 28 semi-structured interviews with LEA staff across several EU Member States, especially drawn from the ANITA, ARIEN, PARSEC and BORDERLINK H2020/HE projects; the authors' own professional experience, which directly informs the recommendations put forward.

Three findings stand out:

- **Workforce readiness does not simply track seniority**. Training needs peak among staff at an intermediate career stage, not among the most junior or the most experienced, and strongly co-occur with the need for explainable AI outputs, suggesting that comprehension, not mere exposure to a tool, is the precondition for trust.
- **Organisational fit, not technical performance, is the most frequently cited barrier to tool adoption**. Compatibility with existing systems, roles and procedures matters more to end users than any shortcoming of the tool itself, and different capability constraints concentrate at different levels of leadership.
- **Cross-border and inter-agency cooperation needs are a live concern for end users, even where they are not the object of inquiry**, pointing to a strategic need to capture these needs more systematically within FCT project design.

These findings carry direct implications for EU FCT Research and Innovation (R&I) governance, examined in relation to the AI Act's evolving compliance timeline and the practical demands of inter-agency data sharing in the customs and postal domain.

Building on this evidence, the report puts forward **twenty-two recommendations**, structured around the report's three guiding questions:

- (Q1) Which skills, processes and coordination capabilities determine whether LEAs can translate research outputs into operational practice?
- (Q2) How are training, pilot validation and end-user engagement currently designed and assessed in EU-funded FCT projects, and with what recurring strengths and weaknesses?
- (Q3) How can capability development be embedded more systematically in FCT R&I?

Recurring themes include differentiating measures by career stage, function and leadership tier; treating organisational fit and explainability on a par with technical specifications; strengthening coordination across training bodies, agencies and borders from the design stage; and ensuring training materials and capability-building outlive the funded project's own lifecycle.

1 - INTRODUCTION

08

This report explores the concept of "**capability**" in the context of the European Law Enforcement Agencies (LEAs), testing the working hypothesis that the operational value of AI-supported tools depends less on their technical sophistication than on the capacity of agencies and their personnel to absorb, govern, and embed them into everyday practice. As the European Union invests heavily in AI-driven investigative and intelligence capabilities across its security research programmes - particularly Horizon 2020 (H2020) and Horizon Europe (HE) - the critical question is not only whether such tools work in principle, but whether LEAs possess the organisational readiness in skills, processes, cross-agency coordination and organisational culture to translate them into operational results.

This question has grown more pressing as the volume of digital tools and data available to analysts and investigators increasingly outpaces individual officers' capacity to interpret, govern and act on them, making the human-machine relationship in policing a precondition for effective and accountable action rather than a secondary concern. This, in turn, calls for a critical reflection on how H2020 and HE-funded projects have typically approached end-user engagement, training and pilot validation, and whether these approaches genuinely contribute to capability building or merely to the adoption and use of individual AI-supported solutions without addressing the underlying organisational readiness gap. This tension between technical availability and individual/organisational readiness is what this report sets out to investigate, structured around **three guiding questions:**

- (Q1) Which skills, processes and coordination capabilities determine whether LEAs can translate research outputs into operational practice?
- (Q2) How are training, pilot validation and end-user engagement currently designed and assessed in EU-funded FCT projects, and with what recurring strengths and weaknesses?
- (Q3) On this basis, how can capability development be embedded more systematically in FCT research and innovation (R&I)?

These three questions are addressed, respectively, through: a review of the academic and policy literature on absorptive capacity, dynamic capabilities and technology adoption in policing; a mapping of publicly documented training, piloting and end-user validation practices across thirteen H2020 and Horizon Europe FCT projects; and a set of insights informed by primary survey and interview evidence, and by the authors' own professional experience, especially across the ANITA, ARIEN, PARSEC and BORDERLINK H2020/HE projects. These insights, in turn, ground the actionable recommendations presented in the report's concluding section.

On this basis, the report is expected to deliver three concrete **outputs**. The first is a typology of the capability gaps that most consistently hinder the uptake of research-based solutions by LEAs, distinguishing gaps rooted in individual skills from those rooted in organisational processes or cross-agency coordination. The second is an evidence-based assessment of the recurring strengths and weaknesses in how training, piloting and end-user engagement are currently designed and evaluated across FCT-funded projects, drawing on both the literature and the primary evidence gathered in this study. The third is a set of actionable recommendations for embedding workforce preparedness and capability development directly into the design of future FCT projects - from call conditions to consortium composition and governance requirements - rather than treating them as an ancillary activity layered on top of an already-finalised technical solution.

This need to translate technical capability into governed, accountable operational practice is not merely an organisational preference: the EU's dedicated regulatory framework for AI in law enforcement makes it a legal requirement as well. The Artificial Intelligence Act classifies most AI systems deployed by or on behalf of law-enforcement authorities as high-risk, imposing stringent requirements on risk management, transparency and human oversight (European Parliament & Council of the European Union, 2024), while the Law Enforcement Directive establishes a parallel data-protection regime specific to law-enforcement processing purposes (European Parliament & Council of the European Union, 2016). Legal and criminological analyses of AI in policing accordingly frame these systems as socio-technical assemblages whose effectiveness depends as much on agencies' capacity to absorb and govern them as on their technical design (Kafteranis et al., 2023).

Prior ENACT analyses of FCT research priorities and Internal Security Fund programmes have shown that EU funding increasingly concentrates on data-centric capabilities mapped against the EU Civil Security Taxonomy (Graikini & Ríos Morentin, 2024; Ríos Morentin & Alegria, 2024), suggesting that there is a need to extend this evidence base to the organisational and workforce dimensions of capability development that determine whether such funded capabilities are actually absorbed into operational practice.

Reflecting in particular Q1 above, the empirical analysis is organised around three capability-oriented dimensions that map skills, processes and coordination onto operational constructs: **workforce preparedness[1]; organisational capability maturity and operational readiness[2] and cross-border and inter-agency cooperation capacity[3].**

[1] Workforce preparedness is intended as the technical competences, training needs, digital skills and decision-making capacities that shape end-users' ability to pilot, understand and use AI-supported tools, examined through users' prior AI and data literacy, their reflexivity when interacting with AI outputs, and their operational role

[2] Organisational capability maturity and operational readiness is intended as how resource constraints, procedural bottlenecks, scalability challenges and leadership engagement shape the testing, further development and likely adoption of tools, examined through the allocation of suitably qualified testers, the presence of routines for knowledge acquisition (internal training, proactive engagement with technical partners), the involvement of senior decision-makers, and existing processes for integrating new tools into workflows

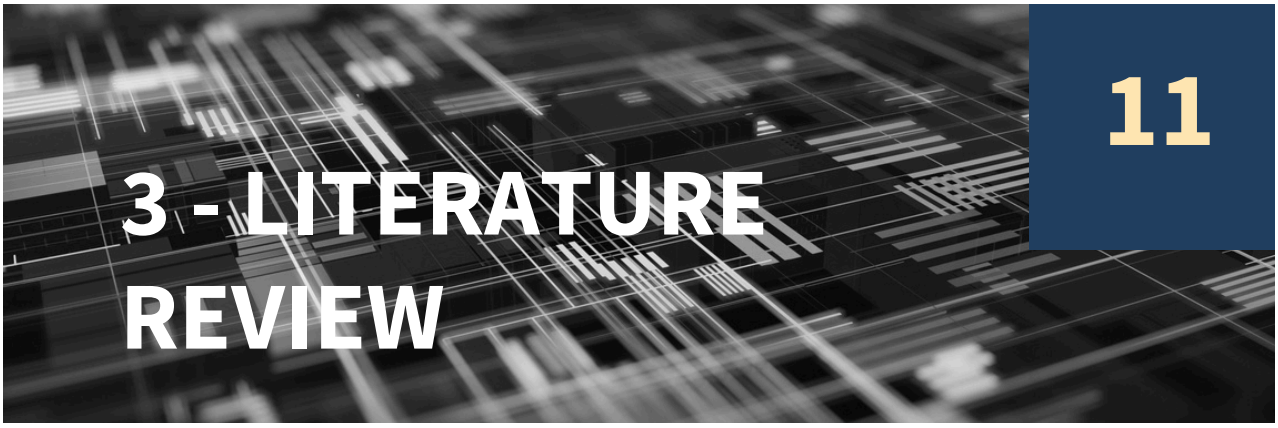
[3] Cross-border and inter-agency cooperation capacity is intended as how Horizon-funded projects' governance structures (general assemblies, work-package allocation) enable or constrain shared capacity-building across agencies and jurisdictions, as perceived by projects' own end users.

2 - METHODOLOGY

This report draws on three complementary strands of evidence, each addressing one of the guiding questions set out in the Introduction. The first is a **review of the academic and policy literature** on absorptive capacity, dynamic capabilities, established technology-adoption models, and the **EU** regulatory and policy architecture governing AI in law enforcement, undertaken to identify the organisational determinants of capability building at the centre of Question 1. The second maps the publicly documented training, piloting and end-user validation components of thirteen **Horizon 2020 and Horizon Europe projects funded under the Fighting Crime and Terrorism (FCT)** destination and its predecessor Secure Societies calls, selected because they target law-enforcement, customs or border-management end users and report such a component in their CORDIS fact sheets, results pages or project websites. Each project is read through the same organisational readiness dimensions used throughout this report (skills, processes, coordination and organisational culture, coded as explicitly, partially, or not addressed in public materials), in order to answer Question 2. The third strand provides the report's **primary empirical basis** and addresses Question 3. It derives mostly from the ANITA, ARIEN, PARSEC and BORDERLINK EU Horizon FCT projects, which support police and border forces, or, in the case of the now-concluded ANITA project, supported them in investigative and intelligence-led activities against illicit trafficking.

Data collection was carried out within the consortium of one of these four projects: for the sake of confidentiality, the specific project is not named or otherwise made identifiable, and questionnaire responses are reported only in aggregate form. The survey data are drawn from LEA partners of this project spanning several EU Member States, ensuring that the workforce and organisational capability findings presented in the Analysis Section reflect a cross-national perspective. A structured questionnaire was administered to multiple end-users in correlation with pilots testing a set of tools developed by technical partners at different stages of development, combining tool-specific questions with a core block common to all tools, which forms the basis for the transversal analysis presented below. In total, 894 questionnaire responses were collected. Two methodological caveats warrant attention. First, not all tools fell within the operational remit of every respondent, so several "not applicable" responses reflect genuine domain-specific irrelevance. Second, response patterns were heterogeneous, since not all respondents who addressed a given tool completed the full set of corresponding questions, resulting in uneven coverage across items.

This evidence base is further broadened through 28 semi-structured interviews with a wider set of police and border-authority practitioners, extending beyond the core project's consortium and capturing perspectives from stakeholders not directly bound to the pilot itself. This interview-based evidence is drawn upon throughout this report where it helps illustrate or substantiate patterns emerging from the survey data, particularly regarding how non-technical factors shape the uptake of AI tools within the transnational architecture of law-enforcement cooperation.



3 - LITERATURE REVIEW

This section synthesises academic and policy literature relevant to the report's central question: what determines the ability of Law Enforcement Agencies to translate research and innovation outputs, particularly AI-supported investigative tools, into sustained operational practice. The literature converges on a **capability-oriented** view: uptake depends on organisational learning, adaptive capacity, and an enabling policy environment.

Absorptive capacity, introduced by Cohen and Levinthal (1990) as a firm's ability to recognise, assimilate and apply external knowledge, is cumulative and cannot be improvised at the point of adoption. Butler and Ferlie (2020), examining two English public agencies, found that absorptive capacity in public-service organisations depends on skilled, embedded actors seizing episodic windows of opportunity to innovate, a risk for FCT projects if capacity depends on individuals who may not survive the pilot's end (see the Section 5). **Dynamic-capabilities** theory explains how organisations adapt over time: Teece, Pisano and Shuen (1997) define this as reconfiguring competences, and Teece (2007) identifies seizing as the weakest link, particularly under layered public-sector procurement rules. Recent work translates this into four public-sector pillars: interoperable data, infrastructure, workforce competencies, and leadership (Aarab, El Marzouki, Boubker & El Moutaqi, 2025), suggesting AI Act compliance and operational uptake need not compete.

Two adoption frameworks recur in this literature: the Technology–Organization–Environment (TOE) framework (Tornatzky & Fleischer, 1990) and Rogers's Diffusion of Innovation (DOI) theory. TOE-based studies in Finnish healthcare found organisational factors more decisive than technological ones (Pulkkinen, Huttu & Suhonen, 2025). A parallel JRC survey of 576 public managers across seven EU countries reached a similar conclusion: in-house expertise, innovative culture, strategy and leadership support were identified as the key internal drivers of AI adoption, more so than technology itself (Grimmelikhuijsen & Tangi, 2024). This pattern echoes the report's own project mapping. Rogers (2003) models adoption as shaped by an innovation's compatibility, complexity and observability. Bullock, Sidebottom, Laycock and Tilley (2022) applied this framework to problem-oriented policing in England and Wales, showing that these same factors explained why diffusion was uneven across police forces. Organisational culture is a further constraint. European frontrunner forces - notably in the Netherlands and the United Kingdom - overcame social-media adoption barriers only through sustained effort (Dekker, van den Brink & Meijer, 2020). More broadly, weak organisational capability can carry legal and reputational risk, as seen when data-protection or governance failures force an EU police force to discontinue a tool altogether (e.g. the Metropolitan Police's Gangs Violence Matrix, discontinued in 2024 following a 2018 ICO enforcement notice; Information Commissioner's Office, 2018). This "valley of death" between research and operational use is attributed to weak needs assessment, insufficient end-user involvement, and an underdeveloped exploitation strategy (EARTO, 2020).

EU policy increasingly treats capability building as a precondition for lawful AI deployment. The AI Act classifies most law-enforcement AI systems as high-risk, imposing obligations that include ensuring staff are adequately trained in the system's use and limitations.[4] These obligations are tracked through ENACT's own Structured Knowledge Base (which aggregates stakeholder observations across four thematic Observatories) and fed directly into the ENACT Flash Report on the AI Act (ENACT, 2025). The Law Enforcement Directive governs a parallel data-protection regime; Europol's Observatory Report (2024) links accountability and explainability to evidentiary validity in court. The High-Level Group (2024) diagnoses digital-forensics skills deficits, and CEPOL's EU-STNA 2026–2029 reframes training as a strategic investment. These obligations trigger at operational deployment, yet FCT projects typically end at the pilot stage.

Some FCT projects already build capability during the research cycle. INSPECTr's capacity-building programme was designed around CEPOL, ECTEG and Europol training standards (Whelan & Genoe, 2022). TENACITy's Living Labs combined tool testing with experiential learning. A study of twelve customs projects reportedly links durable uptake to early end-user involvement and sustained funding (Männistö, Wong-Chan & Doherty, 2025); a companion study proposes a three-tier training model that this report returns to in its recommendations (Männistö, 2025).

Three convergences emerge. Uptake is gated by prior organisational capacity, not tool quality, corroborated by TOE evidence. Adoption models transfer to policing only with qualification: hierarchical culture and fragmented coordination amplify Teece's seizing bottleneck. EU policy instruments encode this same logic but say little about how R&I project design itself could build this capacity as a deliverable. This is the review's principal gap, and addressing it is this report's contribution.

A final strand addresses how AI tools are received by those outside the deploying organisation. Citizen acceptance is not a simple approve/reject judgement: Q methodology[5] identifies five distinct perspectives where safety and privacy concerns coexist (Ezzeddine, Bayerl & Gibson, 2023), and a 670-respondent UNICRI/INTERPOL survey finds similarly multifaceted views, with police-affiliated respondents more favourable yet still strongly supportive of compulsory ethics training (UNICRI & INTERPOL, 2024). Public support for facial recognition depends more on trust in police than on technical characteristics (Bradford, Yesberg, Jackson & Dawson, 2020). On the staff side, local supervision and task fit matter more than a tool's intrinsic features (Lindsay, Jackson & Cooke, 2011). Technology acceptability, in short, is shaped less by sophistication than by institutional trust and organisational fit. This positions population preparedness as a distinct but related dimension of capability building.

[4] These obligations were originally due to apply from 2 August 2026. Following the Digital Omnibus on AI, proposed by the European Commission on 19 November 2025 and given final approval by the Council on 29 June 2026 (Council of the European Union, 2026), the application of high-risk obligations for stand-alone Annex III systems has been deferred to 2 December 2027. This extension widens the window agencies have to build readiness, but it does not remove the underlying obligation. FCT projects concluding before December 2027 will still need to anticipate requirements that apply once a tool moves into operational use.

[5] Q methodology is a research technique used to identify distinct, internally coherent viewpoints within a group, based on how participants rank a set of statements relative to one another, rather than measuring the prevalence of a single opinion across a large sample.

4 - MAPPING OF EU-FUNDED FCT PROJECTS

This section maps publicly documented outputs of Horizon 2020 and Horizon Europe projects funded under the Fighting Crime and Terrorism (FCT) destination and its predecessor Secure Societies calls, selecting projects that

- target law-enforcement, customs or border-management end users, and
- report a training, piloting, or end-user validation component in their CORDIS fact sheets, results pages, or project websites.

Thirteen such projects are analysed, spanning 2016 to the present and covering technology domains from AI-assisted investigation and augmented reality to postal security screening and IoT forensics. The full project-by-project mapping is provided in the Annex, in Table 4.

The mapping excludes coordination-and-support actions, whose primary output is a knowledge-sharing network rather than a deployable tool or curriculum, with one exception: ALIGNER, which is retained because its road mapping process is itself a capability-building mechanism. ENACT itself is not included, since its function is to aggregate knowledge about the wider FCT population rather than deliver a pilot or training product.

Each project is read through the same organisational readiness framework used throughout this report:

- **skills** (whether the project builds LEA staff competence to use, interpret or govern the technology),
- **processes** (whether it produces methodologies, Standard Operating Procedures (SOPs) or governance artefacts that can outlive the project),
- **coordination** (whether it establishes durable cross-agency, cross-border or multi-stakeholder mechanisms), and
- **organisational culture** (whether it engages end users as co-designers and owners of the outcome rather than as passive test subjects).

For each dimension, projects are coded as:

- explicitly addressed (E),
- partially or implicitly addressed (P), or
- not addressed in public materials (–).

The coding reflects what is documented in publicly available deliverables, not an assessment of the project's internal practice, which may be broader than what is disseminated externally.

A preliminary classification of these projects against the **EU Civil Security Taxonomy for FCT's** (EUCST) functional areas is already available in the ENACT Structured Knowledge Base (European Commission, 2022). This classification is based on the assessment submitted at the call proposal stage rather than on the project's actual execution. A systematic comparison between this preliminary classification and the practices observed in this report could therefore constitute a useful analytical development.[6]

Skills-building is the most consistently documented dimension, clustering into a bounded-deliverable model (INSPECTr, COPKIT, CREST) and a continuous model embedded in technical validation (TENACITy); projects with a narrower technology focus (ROXANNE, ANITA) report comparatively little on skills despite involving end users in testing. Process artefacts are strongest where a project's mandate is explicitly cross-agency or regulatory (ALIGNER, COPKIT), weakest where it centres on a single analytic capability (ROXANNE, ANITA). Coordination is most developed where a project builds a standing advisory structure (COPKIT, DARLENE) or recurring multi-stakeholder forum (ALIGNER, STARLIGHT), and only a few projects extend it across borders (ARIEN) rather than within a single Member State (CREST, ANITA). Organisational culture, end users as co-owners rather than test subjects, is the least consistently documented dimension, present mainly where projects name co-creation as an explicit design principle (CREST, STARLIGHT, TENACITy); elsewhere feedback is collected, but public materials rarely describe end users shaping a tool's design logic.

Projects funded more recently under Horizon Europe (PARSEC, BORDERLINK, SALUS, TENACITy, ARIEN) more frequently name training or capacity-building as an explicit objective than the earlier H2020 cohort. This suggests that call-level requirements, not only consortium choices, might drive which readiness dimensions are built in from the start. Public documentation alone, however, cannot establish which factors reliably convert pilot-stage engagement into durable capability. Coding reflects what projects choose, or are able, to disseminate. Some deliverables may also carry a restricted dissemination level given the security-sensitive nature of several FCT projects, a bias that could affect dimensions such as cross-border coordination more than others. This is a gap the primary survey and interview data examined next can help close.

[6] As an illustration of what this classification could look like, four of the thirteen projects lend themselves to a fairly straightforward assignment: PARSEC's non-intrusive detection technologies for postal and customs flows fall squarely under "detection of goods, substances, assets and people" (F07-Detection of goods, substances, assets and people, and incidents); BORDERLINK's checkpoint technologies span both detection (F07) and "identification and authentication of persons, assets and goods" (F06-Identification and authentication of persons, assets and goods); CREST's IoT-enabled platform for first-responder scenarios aligns with "personal and other equipment for prevention, response and recovery" (F01-Personal and other equipment for prevention, response and recovery); ANITA's investigation system for online illegal trafficking corresponds to "investigation and forensics" (F10-Investigation and forensics).
For the remaining projects, technology domains are more composite or span multiple functional areas, and a systematic application of the taxonomy to the full FCT project population would require a dedicated, focused effort that falls outside the scope of this report.

5 - ANALYSIS

Building on the theoretical framework set out in the literature review, this section turns to the report's primary empirical evidence to examine Q1 in practice, structured around the three dimensions introduced above: workforce preparedness; organisational capability maturity and operational readiness; and cross-border/inter-agency cooperation capacity. This evidence extends well beyond the technical functionalities of the tools under review: respondents' comments reveal training needs, documentation gaps, internal procedures and data-sharing practices that shape how **AI**-supported tools are actually used once deployed.[7]

WORKFORCE PREPAREDNESS

The analysis of workforce preparedness is based on the replies collected to the question:

"Are there any organisational or personal factors that could be improved to enhance the understanding and/or use of this tool? If yes, please specify which ones and explain why."[8]

It proceeds along two axes: a thematic coding scheme capturing recurring gaps in training and documentation, and a cross-tabulation of these themes with respondents' professional profiles (years of experience, function, leadership tier), to test whether preparedness gaps vary systematically across the workforce rather than being evenly distributed.

This is needed to move from an aggregate account of "what end users say" toward a more granular understanding of who says it, under what conditions of prior exposure to digital tools and institutional roles, and with what degree of reflexivity regarding their own training and capacity needs. Of the 894 questionnaires received, four response patterns emerge, as summarised in Table 1.

[7] It consists of 894 questionnaire responses collected within one of the four Horizon FCT projects introduced above (ANITA, ARIEN, PARSEC and BORDERLINK), whose identities are kept anonymous for confidentiality, complemented by 28 semi-structured interviews with police and border officers connected to the same projects.

[8] Open and not mandatory question.

Table 1 - Distribution of responses on workforce preparedness factors

RESPONSE CATEGORY	N	% OF TOTAL
Factors identified (YES – respondent specified one or more factors)	400	44.70%
No factors identified (respondent explicitly stated that none applied)	174	19.50%
No response (question left blank)	223	24.90%
N/A (respondent explicitly wrote "N/A")	97	10.90%
GRAND TOTAL	**894**	**100%**

Of these four categories, only “No response” reflects an unanswered question. The other three all correspond to an explicit answer: a specific factor, an explicit statement that none applied, or an explicit “N/A”. In particular, N/A answers mean that the respondent did not feel the tool was within his/her remit of expertise and/or operational activity. This suggests that some participants, while professionally competent for the evaluation process, may simply not need this tool for their day-to-day work, raising a broader question about how LEAs select staff to take part in European FCT projects, especially in the context of pilots. Disaggregating the response pattern by years of experience (Table 2) shows that engagement with the question is uneven.

Table 2 - Workforce preparedness factors: response distribution by years of experience

YEARS OF EXPERIENCE	YES (FACTORS IDENTIFIED)	NO FACTORS	NO RESPONSE	N/A	TOTAL RESPONDENTS (BUCKET)
1-3	65	43	61	12	181
% of 1-3 bucket	35.90%	23.80%	33.70%	6.60%	100.00%
4-6	47	31	37	36	151
% of 4-6 bucket	31.10%	20.50%	24.50%	23.80%	100.00%
7-10	72	30	15	6	123
% of 7-10 bucket	58.50%	24.40%	12.20%	4.90%	100.00%
10+	216	70	110	43	439
% of 10+ bucket	49.20%	15.90%	25.10%	9.80%	100.00%
GRAND TOTAL	**400**	**174**	**223**	**97**	**894**
% OF GRAND TOTAL (894)	**44.70%**	**19.50%**	**24.90%**	**10.90%**	**100.00%**

Respondents with 7-10 years of experience were the most likely to identify a factor (58.50%) and the least likely to leave the question unanswered (12.20%), while the 4-6 years band accounts for a disproportionate share of “Not applicable” responses (36 of 97 cases, against an expected 17 if evenly distributed).

Of the 400 respondents who identified at least one factor that could be improved to enhance the understanding and/or use of the tool under evaluation, 265 cited training- or documentation-related needs. Respondents' comments were coded into three categories. As these categories are not mutually exclusive, some respondents appear in more than one. “Tool-specific Training”: requests for further training on the specific tool under evaluation; “Other Training”: requests for training not tied to the specific tool under evaluation but covering a broad range of digital skills; and “Additional Documents”: requests for supporting documentation, such as a guide or tutorials.

Table 3 shows the breakdown of related answers, again disaggregated by years of experience. Overall, 234 respondents (26.20% of the full sample and 58.50% of those who indicated at least one factor) requested further tool-specific training, 146 (16.30% and 36.50%) flagged the need for additional documentation, and 32 (3.60% and 8.00%) requested further training of a more general nature.

Table 3 - Workforce preparedness improvement factors: breakdown by years of experience

YEARS OF EXPERIENCE	TOOL-SPECIFIC TRAINING	OTHER TRAINING	ADDITIONAL DOCUMENTS	N/A	TOTAL RESPONDENTS (BUCKET)
1-3	39	3	28	12	181
% of 1-3 bucket	21.50%	1.70%	15.50%	6.60%	100.00%
4-6	36	1	19	36	151
% of 4-6 bucket	23.80%	0.70%	12.60%	23.80%	100.00%
7-10	48	6	31	6	123
% of 7-10 bucket	39.00%	4.90%	25.20%	4.90%	100.00%
10+	111	22	68	43	439
% of 10+ bucket	25.30%	5.00%	15.50%	9.80%	100.00%
GRAND TOTAL	**234**	**32**	**146**	**97**	**894**
% OF 400*	**58.50%**	**8.00%**	**36.50%**	**-**	
% OF GRAND TOTAL (894)	**26.20%**	**3.60%**	**16.30%**	**10.90%**	**100.00%**

* Percentages do not sum to 100% because categories are not mutually exclusive.

Considering the distribution by years of experience (Figure 1), the most senior cohort (10+ years) accounts for the largest share of mentions in every category, but this is mostly a size effect: it is the largest group in the sample, and Figure 1's percentages reflect total mentions, not band size. Normalised by group size, the 7-10 years band shows the highest per-capita demand for “Tool-specific Training” (39.00%) and “Additional documents” (25.20%), consistent with this band also being the most likely to identify at least one enabling factor (58.50%): respondents with 7-10 years of experience are proportionally the most engaged with the question.

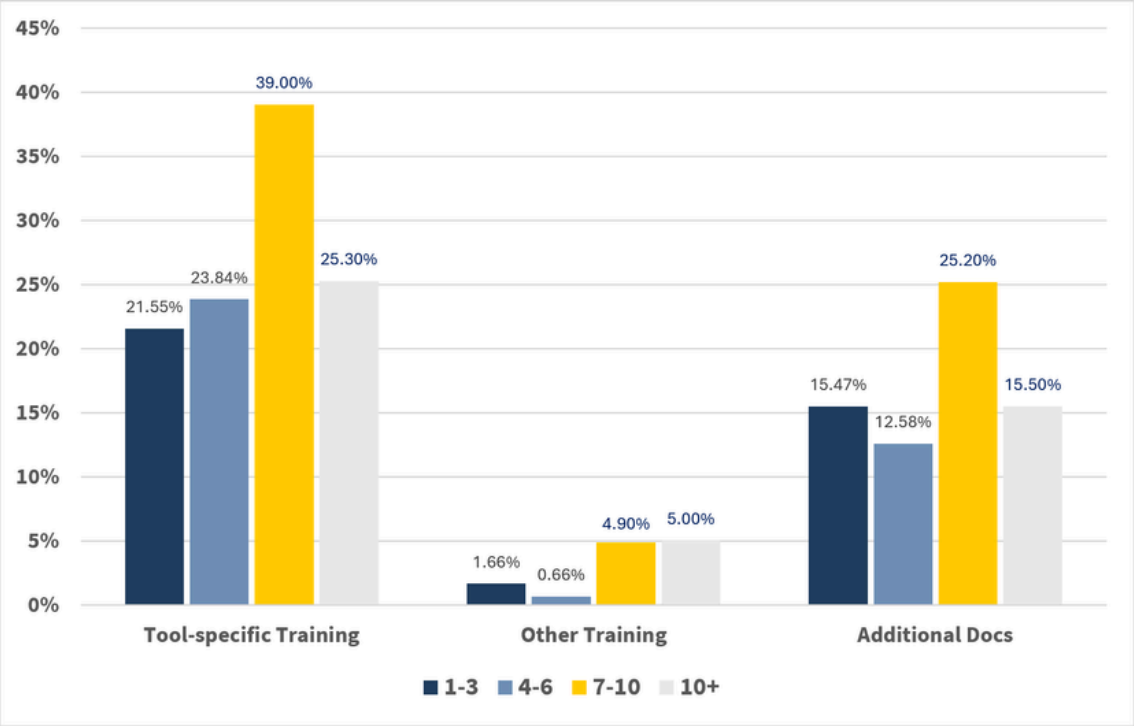


Figure 1 - Workforce preparedness: need for supporting personal capabilities by years of experience

When disaggregated by functional role (Figure 2),[9] technical and operational staff show similar shares in absolute terms. This is partly a size effect, as operational staff constitute the larger group (520 respondents compared with 374 technical staff). Normalised, technical staff report a higher per-capita demand across all three categories. This is not a function-composition artefact of the seniority effect above: the 7-10- and 1-3-year bands have similar shares of technical staff (56.10% and 57.50%), yet very different demand rates, suggesting that seniority itself drives the earlier pattern. It cannot be distinguished whether respondents describe their own gaps or their team's, an ambiguity that may matter more for leadership positions, discussed next.

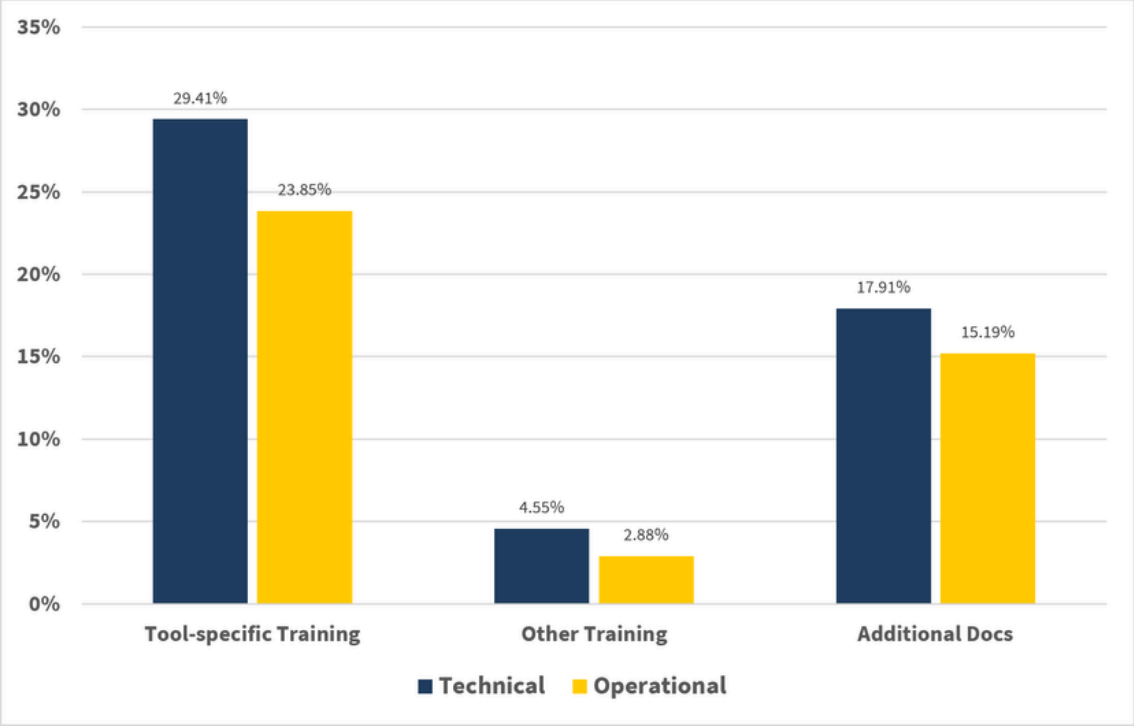


Figure 2 - Workforce preparedness: need for supporting personal capabilities by functional role

Turning to leadership tiers (Figure 3)[10], leaders account for a slight majority of “Tool-specific Training” flags in absolute terms (55.10%). This partly reflects group size: Individual Contributors form the largest group (582 respondents), against 220 Decision Makers and 92 Directors. Normalised by group size, the picture changes. Individual Contributors report the lowest per-capita demand across all three categories (18.00% “Tool-specific Training”, 2.90% “Other Training”, 12.50% “Additional Documents”). Decision Makers report a higher demand (40.00%, 3.60%, 27.70%). Directors report the highest demand for “Tool-specific” and “Other Training” (44.60%, 7.60%), but “Additional Documents” peaks among Decision Makers (27.70%) rather than Directors (13.00%), echoing the non-monotonic pattern already seen for years of experience. This pattern is consistent with either leaders feeling these gaps themselves or reporting on behalf of their team.

[9] Function distinguishes professional roles by orientation rather than hierarchy: "technical" refers to roles focused on developing, deploying or managing tools (e.g., Software Engineer, DevOps Engineer, Information Security Administrator, Innovation Manager), while "operational" refers to roles focused on using them for investigative or law-enforcement activity (e.g., Investigator, Analyst, criminal inspector). The two categories are independent of leadership tier.

[10] Leadership tiers were derived from a separate self-reported field on respondents' decision-making or managerial status, distinct from their free-text job title, and grouped into three categories: Individual Contributor (e.g., Investigator, Analyst, Software Engineer), Decision Maker (e.g., Innovation Manager, senior investigative officer), and Director (e.g., Head of Section, Chief Officer, CISO). For the purposes of this analysis, "leadership positions" combines Decision Makers and Directors, against Individual Contributors.

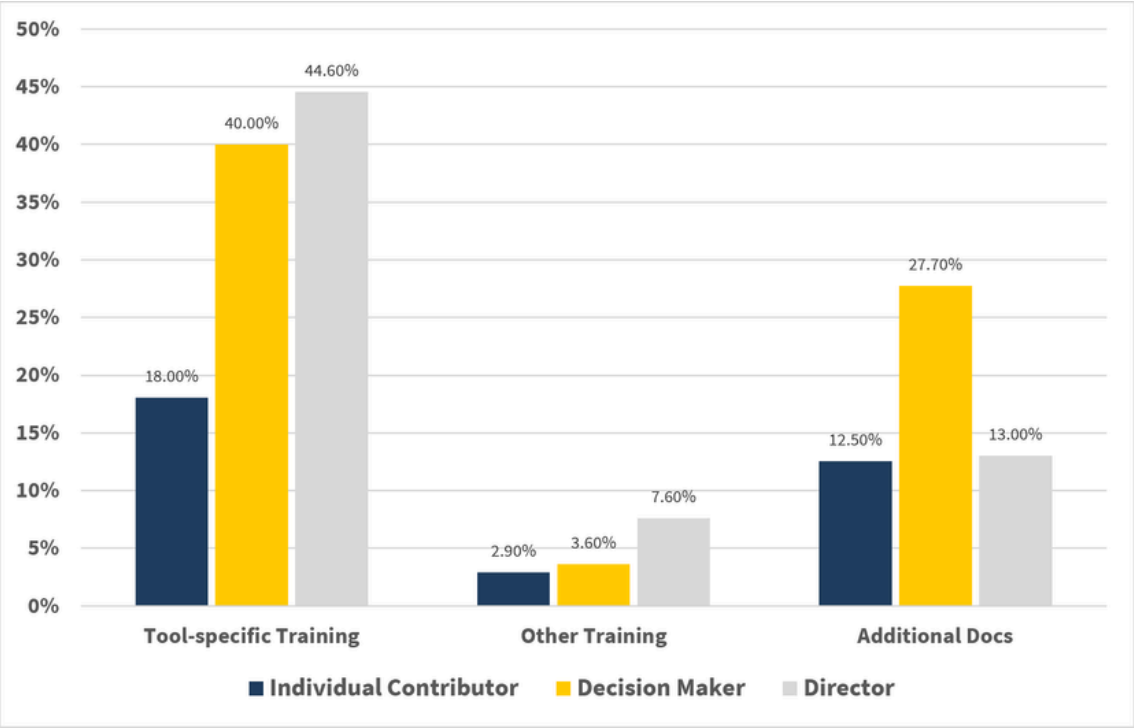


Figure 3 - Workforce preparedness: need for supporting personal capabilities by leadership role

Taken together, seniority and hierarchical position shape who articulates a need, but not in the same direction: experience peaks at an intermediate level (7-10 years), leadership shows a more consistent rise from Individual Contributors to Directors, and function operates as a largely separate axis. Among "Other, non-tool-specific" training, digital skills dominate (13 of 39 mentions), ahead of graph/network analysis (7), analytical skills and train-the-trainer (6 each), OSINT (5), and GIS (2); digital skills and train-the-trainer requests come mostly from operational staff and individual contributors, while graph/network and GIS requests skew toward decision makers and directors.

Finally, we observed a strong positive correlation between the flagged **need for training** and the flagged need for **explainability**, that is, respondents' explicit request for the tool to show how it produces specific results or alerts ($r = 0.59$, $n = 894$).

This suggests that these two capability gaps tend to co-occur in the same individuals. This pairing may point to a broader mechanism: trust in an AI-supported tool does not appear to be granted by default, but to depend on the user's ability to understand how the tool arrives at its outputs. Where that understanding is lacking, the same respondents are also more likely to flag a need for training, suggesting that comprehension, rather than mere exposure to the tool, may be the precondition for trust and, in turn, for sustained use in operational environments.

WORKFORCE PREPAREDNESS: KEY FINDINGS

Age and seniority may be a misleading lens for targeting support. Capability gaps do not track seniority. The respondents most vocal about these gaps are neither the newest cohort, who might be expected to need onboarding, nor the most senior, who might be expected to need the least support, but those in an intermediate career stage. Capability-building efforts that target only new hires, or assume that experience is self-sufficient, risk missing where the need is actually concentrated.

A single training offer is unlikely to fit every profile. Technical staff and senior decision-makers each show a distinct pattern of engagement with the question, independent of seniority. This suggests that capability-building measures designed around one generic profile risk underserving the range of technical and hierarchical roles involved in piloting and using these tools.

Training and explainability needs are not separate problems — they are the same problem seen from two angles. Respondents who ask for more training are, to a significant degree, the same respondents who ask for the tool to show its reasoning. This suggests that investment in explainable, interpretable AI outputs may serve a dual function as a capability-building measure, rather than being a purely technical add-on.

Demand for capability support extends beyond the specific tool being piloted. A meaningful share of respondents asked for training unrelated to any single tool — general digital skills, network/graph analysis and OSINT — pointing to a baseline digital-literacy gap that may fall outside the scope of any single FCT project, each of which is typically designed to deliver training on technical tools rather than a general training curriculum.

ORGANISATIONAL CAPABILITY AND OPERATIONAL READINESS

Beyond the training-related gaps examined above, respondents' free-text comments also point to a further layer of capacity constraints: organisational and personal factors[11] affecting the effective testing and deployment of AI-centred tools.

Among the 400 respondents who identified at least one such factor, the need to align internal operations — system integration, roles and internal rules — with the tool's functionalities emerged as the single most frequently cited constraint (88 mentions, 22.00%). This is not a shortcoming of the tool's technical performance, but a question of organisational fit, resonating with the TOE framework discussed in the literature review, where organisational characteristics, rather than technological ones, were found to be the more decisive barrier to AI adoption.

This was followed by the need for more time to test and become familiar with the tool (66 mentions, 16.50%), more stable support from technical partners (60 mentions, 15.00%), and additional internal resources (24 mentions, 6.00%). As a share of the full corpus of 894 factors, the ranking is broadly maintained: internal SOP alignment accounts for 9.80%, more time for 7.40%, technical support for 6.70%, and resourcing for 2.70%. These proportions may understate the reality, since needs may remain tacit or under-reported when derived from voluntary comments to a single open-ended question.

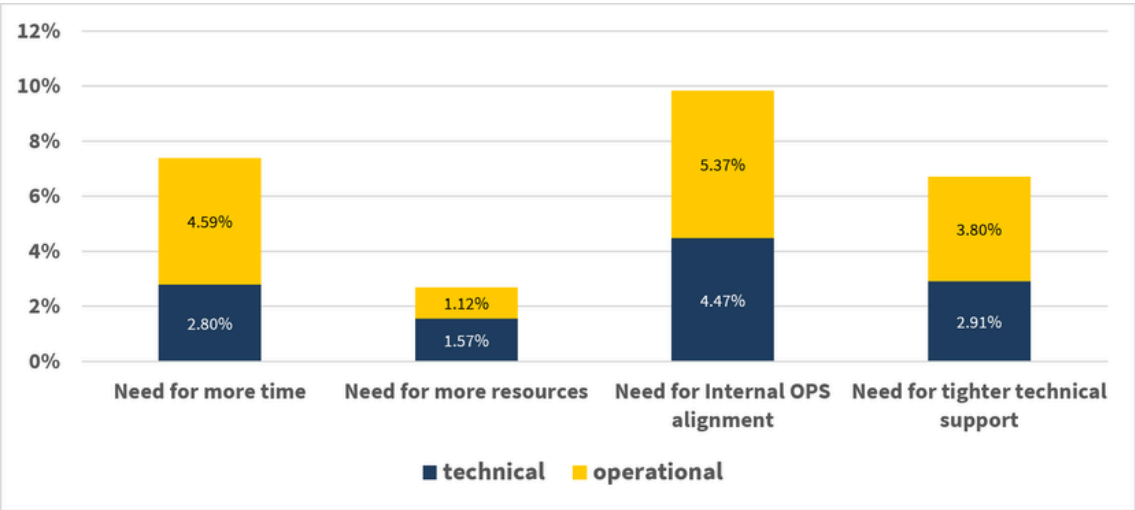


Figure 4 – Organisational capability and operational readiness: distribution of capacity needs by respondent function (% of total coded improvement factors, n=894)

[11] Personal factors concern individual capacity constraints such as time, rather than the skill and training gaps examined in the workforce preparedness.

A parallel breakdown by leadership position (Figure 5) shows a similar concentration among **Individual Contributors** in absolute terms. They account for the largest shares across the three leadership tiers — 4.40%, 5.90% and 3.90%, respectively — largely reflecting group size (582 **Individual Contributors**, compared with 220 **Decision Makers** and 92 **Directors**). When the figures are normalised by group size, however, **Decision Makers** show the highest rate for internal-operations alignment (13.20%, compared with 9.10% and 6.50%), while **Directors** show the highest rates for resourcing (7.60%) and time (12.00%).

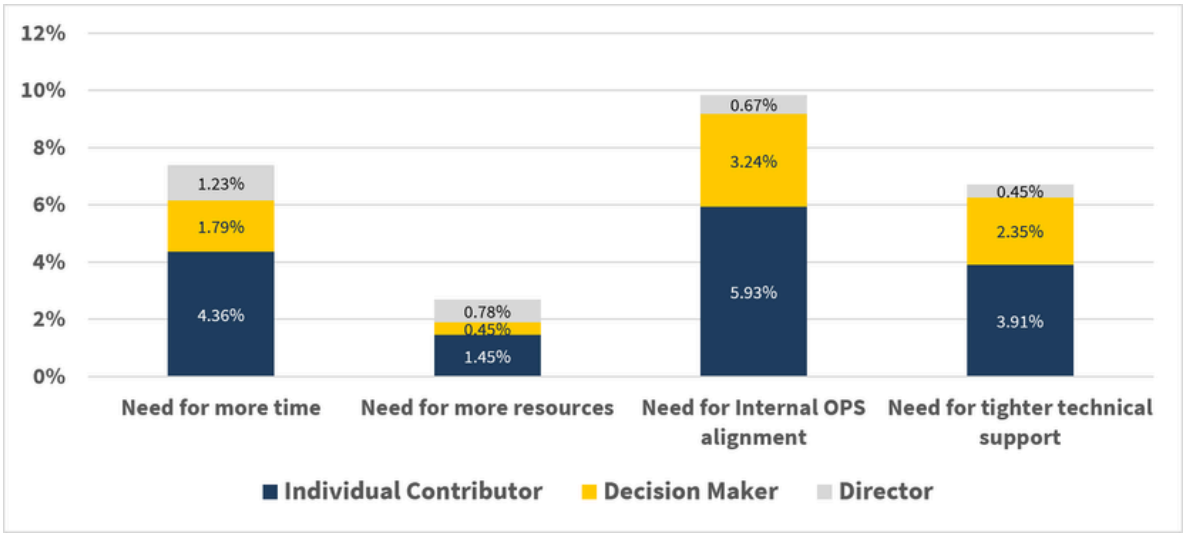


Figure 5 – Organisational capability and operational readiness: distribution of capacity needs by respondent leadership position (% of total coded improvement factors, n=894)

Taken together, these findings suggest that organisational-level preparedness constraints, distinct from individual skill gaps, cluster particularly around **SOP** alignment. This points to organisational integration, rather than individual skill acquisition alone, as a distinct axis of workforce preparedness. They also suggest that different constraints concentrate at different seniority levels: procedural alignment among **Decision Makers**, and time and resourcing among **Directors**. This is a pattern that project design should account for. Assumptions embedded in project design, both around tool transferability and training design, should therefore be built around the different professional profiles involved, with particular attention to seniority and leadership tier.

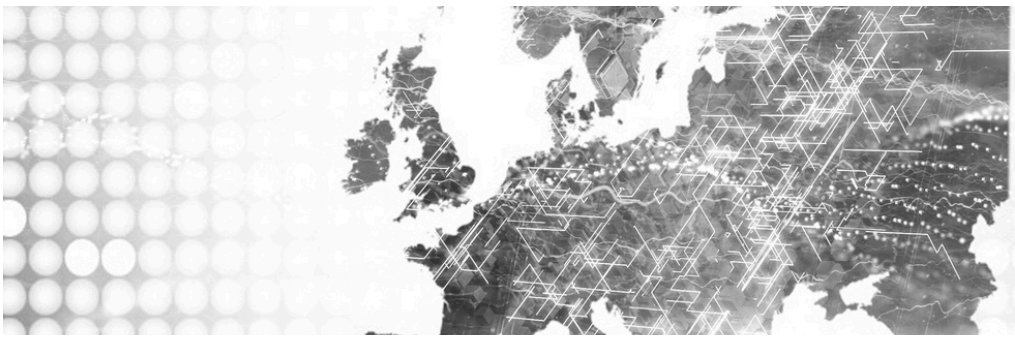
ORGANISATIONAL CAPABILITY AND OPERATIONAL READINESS: KEY FINDINGS

Organisational fit, not technical performance, is the leading constraint. The most frequently cited barrier to using AI-supported tools is not a shortcoming of the tool's technical performance, but whether it aligns with existing systems, roles and internal rules. This is consistent with the TOE framework discussed in the literature review, where organisational factors outweigh technological ones as barriers to adoption.

Understanding organisational capability requires an in-depth assessment of users, particularly with regard to their specific function and seniority level. How AI-supported tools interact with existing systems, roles and procedures cannot be understood by treating end users as a single, undifferentiated group. The organisational constraints at play — from procedural alignment to resourcing — vary systematically with respondents' function and seniority tier, and capability-building measures need to be designed with this variation in mind.

Different organisational and capability constraints concentrate at different levels of seniority. Procedural alignment concerns cluster around Decision Makers, while time and resourcing constraints concentrate among Directors. No single professional profile captures the full range of organisational readiness gaps. This suggests that capacity-building measures need to be differentiated by seniority and functional tier, rather than designed as a single, one-size-fits-all intervention.

Operational readiness depends more on procedural fit than on tool functionality. Because compatibility with existing systems and internal rules is the most frequently cited constraint, FCT projects should treat this compatibility as a design consideration from the outset, rather than a late-stage integration task. This would help avoid the risk of building tools that are technically sound but operationally difficult to absorb.



CROSS-BORDER OR INTER-AGENCY COOPERATION CAPABILITIES

Although the questionnaire was not designed to examine cross-border or inter-agency cooperation dynamics, a small subset of respondents' free-text comments on data governance and data-sharing protocols spontaneously raised such concerns. This suggests that these considerations remain salient to end users, even in the absence of a dedicated survey item.

Across the sample, 17 such comments were recorded, spanning four LEAs. These were split almost evenly by theme — data governance, with 9 mentions (52.94%), and data-sharing protocols, with 8 mentions (47.06%) — and by function: operational respondents accounted for 9 mentions (52.94%), while technical respondents accounted for 8 mentions (47.06%). Operational respondents mainly raised data protection and security concerns (2 mentions) and the need to test tools with real rather than synthetic data (3 mentions), feedback that was also recorded across tool-specific questions. Technical respondents instead emphasised shared infrastructure across partner agencies, including a common translation server (2 mentions) and a centralised OSINT graph repository (1 mention). These comments were predominantly voiced by technical-function Directors (8 of 17, 47.06%).

Taken together, these voluntary but thematically consistent references point to an emergent dimension of organisational preparedness: the capacity to operate within the broader inter-agency and transnational data-sharing architecture. Existing FCT mechanisms, such as the mid-term practitioner assessment required under recent Horizon Europe calls, focus on evaluating overall project outcomes rather than specifically surfacing cross-border cooperation needs. A dedicated mechanism could help capture such needs more systematically, addressing shared infrastructure and data-protection protocols before they surface as obstacles during piloting.

CROSS-BORDER AND INTER-AGENCY COOPERATION CAPABILITIES: KEY FINDINGS

Inter-agency cooperation is an active concern for end users, even where it is not the object of inquiry. The fact that these concerns emerged unprompted, through voluntary comments on an unrelated question, suggests that cross-border and inter-agency cooperation should be treated as a first-order dimension of capability building, as well as an enabling factor for the adoption of AI-assisted tools.

Different professional profiles are likely to value different aspects of cross-agency cooperation. Concerns ranged from shared technical infrastructure to data-protection safeguards. Echoing the same lesson already drawn for workforce and organisational capability, cooperation mechanisms should be designed around this diversity of professional profiles and their distinct priorities, so that both technical and operational needs are addressed from the outset.

A dedicated space for surfacing cross-border and inter-agency needs would strengthen the adoption of AI-assisted tools in FCT project design. Practitioner-assessment requirements already built into FCT projects offer a natural point of entry for this purpose. Extending them to explicitly cover cross-border and inter-agency cooperation, alongside overall project outcomes, would allow these needs to be captured systematically from the outset, so that shared infrastructure and data-governance arrangements can be planned for rather than discovered during implementation.

6 - IMPLICATIONS FOR EU FCT R&I GOVERNANCE

Based on the preceding analysis and on 28 semi-structured interviews conducted to date with officers from border and police forces across multiple EU countries, many of whom are either partners in or advisers to the aforementioned EU Horizon projects, organisational capabilities have consistently emerged as a critical concern. This applies both at the level of the organisation as a whole and at the level of individual operators. The growing volume of data to analyse and items to inspect, combined with limited time to respond to alerts, makes it increasingly difficult to maintain comprehensive oversight of enforcement activities. This qualitative evidence reflects, in particular, interviews with stakeholders in the customs, border and postal domain. The challenges discussed below should therefore be read as illustrative of this domain, rather than representative of the full range of FCT contexts covered elsewhere in this report. Three main considerations emerge.

First, insufficient organisational and individual capabilities undermine the feedback loops required for AI systems to operate effectively and generate accurate signals.

Interview evidence illustrates the scale of the issue. One border force representative described how only a minority of postal-hub volume is flagged through risk profiling, while the share actually physically inspected remains well below 10% due to limited manual-inspection resources. Another noted that even a substantial increase in staff would still leave most of the flow unchecked. Survey data corroborate this: 10.90% of all responses were marked N/A, often accompanied by comments such as “I am not the target user for this tool”. This suggests that resource constraints may also result in the misallocation of personnel to testing activities, limiting the effectiveness of validation.

Limited organisational capacity therefore constrains human operators’ ability to remain meaningfully “in the loop”. This challenge extends beyond resources. As shown in the section on workforce preparedness, training needs peak not among the most junior or most experienced staff, but at an intermediate career stage and among senior decision-makers. This suggests that officers with the deepest domain expertise may not always receive training at a pace that matches advances in AI, even though their expertise is critical to refining these systems. If so, this would both diminish human-in-the-loop effectiveness and represent a loss of expert input that is indispensable for distinguishing true positives and embedding professional judgement into adaptive learning.

Second, robust inter-agency data sharing is especially critical given rising digital illicit trade flows.

The 2025 Illicit Trade Report (WCO, 2025) shows that e-commerce now accounts for close to 50% of all reported cases globally, with over 60% of cases involving counterfeit goods, medical products and cannabis detected through postal channels. This represents an enforcement challenge intrinsically linked to digital transactions. These flows generate structured data which, if integrated into AI systems, could enhance risk profiling and interdiction. Timely and secure data exchange, including with private actors such as postal and courier operators, is therefore a precondition for effective AI-supported enforcement.

Interview evidence illustrates both the potential and the structural barriers. Public-private data exchange with couriers was seen as valuable for updating risk profiles, although intercontinental data-governance agreements remain slow, multi-year processes. Postal volumes are also growing faster than the quality of data available for risk assessment, with some administrations dependent on external actors for information that is not systematically shared. Resource constraints compound this challenge. Respondents called for greater investment in real-time analytics, while also recognising that frontline postal workers provide valuable indications of suspicious parcels. They also noted that postal operators, while not enforcement agencies, hold data that could help identify illicit goods if rights holders shared findings back with them.

Institutional fragmentation adds a further layer of complexity. In some administrations, only the police, rather than customs authorities, can request data from postal or courier companies. Access to data on goods transiting non-EU territory is particularly limited. Respondents pointed to closer public-private cooperation as a possible mitigation, while emphasising that solutions must remain flexible enough to serve agencies at different levels of digital maturity.

Third, cross-border and institutionalised cooperation mechanisms are a *condicio sine qua non* for AI effectiveness in this domain.

Sustained inter-agency and cross-border data sharing is essential for training and continuously improving AI systems. However, respondents described current exchange practices as insufficiently timely. One respondent, operating outside EU information-sharing frameworks, reported delays of up to two weeks in receiving seizure data from EU counterparts. They attributed this partly to data-protection constraints, which, within the EU law-enforcement context, are governed primarily by the Law Enforcement Directive (Directive (EU) 2016/680) rather than by the GDPR.

Beyond timeliness, data quality and diversity also matter. The effectiveness of AI tools depends on sustained input from multiple agencies, because their value lies not only in the volume of data available but in its quality, relevance and diversity. Cooperation among postal operators, government bodies, police and customs authorities across borders was therefore seen as key to learning from cross-border flows.

Taken together, these insights reinforce that AI effectiveness in this domain is contingent upon institutionalised cooperation mechanisms that enable continuous, high-quality data exchange across agencies and borders.

28

7 - RECOMMENDATIONS AND FUTURE DIRECTIONS

The recommendations that follow are grounded in three sources of evidence: the wider literature reviewed throughout this report; the primary survey, interview and mapping evidence presented above; and the authors' professional experience across different Horizon 2020 and Horizon Europe projects.

The analysis presented in Section 4 has shown that FCT projects address the Skills, Processes, Coordination and Culture dimensions of capability readiness unevenly. Sections 5 and 6 extend this picture with empirical evidence on workforce, organisational and cross-border capability gaps. Together, these findings have direct implications for EU FCT R&I governance. The recommendations below translate these findings into actionable proposals, structured around the three guiding questions introduced in the Introduction. For ease of reference, the same recommendations are also presented in tabular form in the Annex.

Where the authors' own experience is drawn from projects that have already concluded, it reflects completed training design, delivery and evaluation activity. Where it is drawn from projects still ongoing, it reflects direct involvement in project design, coordination and planning practice, rather than completed training outcomes or evaluated results.

Q1 – SKILLS, PROCESSES AND COORDINATION CAPABILITIES

Training and piloting are consistently funded and documented as separate deliverables rather than as one interdependent strategy (Section 4). FCT projects should therefore be required to design training and operational testing as a single, integrated capability-building work package. Relatedly, procedural artefacts (Processes) exist without a corresponding mechanism to verify staff competence, indicating the need for a defined validation or certification pathway for operational staff.

Organisational constraints beyond training — including procedural alignment, time and resourcing — concentrate differently across leadership tiers (Organisational Capability and Operational Readiness). This suggests that capacity-building and change-management measures should be differentiated by leadership tier, distinguishing procedural and coordination measures aimed at Decision Makers from resourcing and time-allocation measures aimed at Directors or senior management. More broadly, compatibility with existing internal systems, roles and rules is the most frequently cited constraint on tool understanding and use, ahead of any technical shortcoming (Organisational Capability and Operational Readiness). FCT projects should therefore be required to assess and document this alignment as an explicit design criterion, alongside technical specifications, rather than treating it as a late-stage integration task.

Coordination of safety-critical, multi-agency field testing can depend on a single internal role, with no identified backup capacity if that person becomes unavailable. This points to the need for **FCT** projects handling hazardous or operationally sensitive activities to identify backup coordination capacity, whether internal or specialist external, in advance.

At EU level, the train-the-trainer offer remains comparatively limited relative to other EU Justice and Home Affairs agencies, constraining the scale at which internally cascaded training can reach LEA staff. Expanding train-the-trainer capacity and funding at EU level would reduce reliance on centrally delivered sessions alone. Externally delivered or outsourced training activities are also not consistently quality-assured against a common standard, suggesting that FCT projects delivering training through third parties or subcontractors should apply a defined quality-assurance framework aligned with existing EU training quality standards.

Finally, technology requirements are sometimes defined by a single stakeholder group in isolation, without a structured process for reconciling the differing priorities of postal/customs, technical and policy-level actors before specifications are finalised. FCT projects should therefore apply a structured, documented multi-stakeholder requirements framework, capturing operator, technical and policy perspectives, rather than defaulting to the perspective of whichever partner leads procurement. Relatedly, training and pilot sessions are sometimes delegated entirely to LEA-internal trainers, without technical partners present, limiting the real-time clarification that would otherwise benefit the whole cohort. Structuring at least part of training and pilot delivery as joint sessions with technical partners present would help address this gap.

Q2 – RECURRING STRENGTHS AND WEAKNESSES IN TRAINING, PILOTING AND END-USER ENGAGEMENT

Training needs cluster around documentation and explainability and do not increase steadily with seniority, peaking instead at an intermediate career stage (Workforce preparedness). Training design should therefore be differentiated explicitly by career stage and functional or leadership profile, rather than assuming that needs increase uniformly with seniority. Relatedly, the need for training and the need for explainable AI outputs strongly co-occur among the same respondents (Workforce preparedness), suggesting that investment in explainable, interpretable AI outputs should be treated as a capability-building measure in its own right, complementing rather than substituting for training.

Differentiated audiences, for example LEAs versus BGAs, require distinct curricula rather than a single generic training offer. Training curricula, and the materials that accompany them, should therefore be explicitly differentiated by end-user function and institutional context from the design stage, distinguishing operational reference materials from full technical documentation.

Training built around a single delivery modality is also fragile to project disruption. Projects should therefore budget for an alternative delivery modality from the outset and build a structured, iterative feedback mechanism between sessions. Training sessions for first-time users of complex, multi-module tools can similarly front-load comprehensive platform functionality, overwhelming trainees rather than building confidence progressively. Sequencing initial training around a single concrete use-case walkthrough, before introducing the full breadth of platform functionality, would help address this.

Finally, organisational culture — understood here as positioning end users as co-owners rather than passive subjects — is the least consistently documented readiness dimension (Section 4). FCT projects should therefore require documented evidence of end-user involvement from the proposal-preparation stage onward.

Q3 – EMBEDDING CAPABILITY DEVELOPMENT SYSTEMATICALLY IN FCT R&I

Training materials lose relevance once no actor owns their post-project upkeep. FCT projects should therefore require an explicit post-project maintenance plan for training and coordination artefacts, naming a responsible organisation as a funding condition.

Field demonstrations and multi-agency trials build practical and procedural competence, including for the operational staff who take part in them. However, they are rarely recognised or funded as capability-building activities in their own right, and the operational and logistical burden they place on participating staff is frequently underestimated relative to the technology costs of the exercise. Formally recognising and funding such trials as capability-building activities, with dedicated logistical support for end users, would address this gap.

Multiple EU-level and project-level actors deliver LEA training with limited coordination among them, risking duplication and inconsistent quality. Coordination mechanisms between FCT projects and existing EU training bodies, such as CEPOL, ECTEG and Europol, should therefore be strengthened at the design stage, rather than allowing training to develop in parallel with limited mutual awareness.

Relatedly, a meaningful share of training needs concerns baseline digital literacy, such as general digital skills, OSINT and graph/network analysis, rather than any single piloted tool (Workforce preparedness). This points to the value of a cross-project or EU-level digital-literacy offer for FCT-involved staff, addressing needs that fall outside the remit of any individual project.

Training curricula, test protocols and demonstration outcomes developed within individual FCT projects are also rarely shared systematically across the wider project population, limiting how much later projects can learn from what earlier ones have already attempted, tested or discarded. A dissemination tier for training and testing materials across FCT projects, short of full public release, could account for the legitimate security sensitivity of much of this material, rather than assuming it away.

Cross-border and inter-agency cooperation needs to surface only incidentally, through voluntary free-text comments, rather than through a dedicated assessment mechanism (Cross-border or inter-agency cooperation). Existing practitioner-assessment requirements in FCT projects should therefore be extended to explicitly cover such needs alongside overall project outcomes.

Finally, the regulatory deferral of AI Act high-risk obligations to December 2027 should not be treated as a reason to defer capability-building. The applicable timeline for high-risk obligations has already shifted, with current official EU guidance indicating that obligations for high-risk systems listed in Annex III apply from 2 December 2027, while obligations for high-risk AI systems embedded in regulated products listed in Annex I apply from 2 August 2028. FCT projects should therefore build compliance-readiness training and documentation practices around a flexible timeline rather than a single fixed deadline, so that tools reaching operational use are not left without trained personnel, regardless of which specific deadline applies.

8 - CONCLUSION

This report set out to test a working hypothesis: that the operational value of AI-supported tools at the level of law enforcement depends less on their technical sophistication than on the organisational capacity of the agencies that adopt them. The evidence gathered across the literature, the mapping of thirteen FCT projects, and the primary survey and interview data consistently points in the same direction. Capability gaps do not cluster where intuition might suggest — around the newest staff, or around the most technically complex tools — but around organisational fit, career-stage-specific needs, and coordination mechanisms. This points to a set of priorities for FCT project design that this report's recommendations aim to make more explicit.

The evidence gathered across this report supports and corroborates this hypothesis: technical sophistication is necessary but not sufficient, and absorptive capacity — skills, processes, coordination and culture — is what ultimately determines whether an EU-funded tool is absorbed into sustained operational practice, or remains confined to the lifecycle of the project that developed it. Taken together, the report's recommendations point towards a shift in how capability building is treated within FCT R&I: not as a downstream consequence of a successfully completed pilot, but as a deliverable to be designed, resourced and evaluated in its own right, differentiated by who is expected to absorb the tool — by career stage, function and leadership tier — rather than treated as a uniform, one-size-fits-all outcome.

This shift has different implications depending on one's position within the FCT ecosystem.

For the **European Commission**, the most direct point of leverage is the design of calls for proposals. The evidence in this report suggests that capability-building requirements are more likely to be delivered when they are built into the conditions of funding, rather than left to individual consortia to prioritise voluntarily. The same attention should extend to how participation requirements are designed within calls for proposals, which points to a broader question of how LEAs select and structure the staff who take part in FCT projects. This is not simply a matter of specifying how many LEAs or countries a consortium should include. It is a matter of establishing a meaningful, substantiated connection between the call topic, the range of competences represented in the consortium, and the outcomes and impact the project is expected to achieve. The composition of the working team should follow a clear causal and logical link to the specific phenomenon the project sets out to address, rather than a generic participation requirement. Call requirements that explicitly encourage this kind of substantiated fit would allow projects to benefit from LEA input in a more continuous and effective way throughout the project lifecycle and to develop technologies with clear impact. One of the central challenges this report identifies is how to reconcile the demands of FCT project participation with the day-to-day operational workload each LEA must manage, compounded by its own organisational complexity.

Addressing this challenge is itself something FCT projects could contribute to, but doing so requires a cultural and organisational shift. Senior figures within LEAs have a pivotal role to play in this shift: their growing awareness, sensitivity and understanding of what these projects can offer is what allows this relationship to change, with FCT projects becoming a genuine resource for European LEAs, rather than an additional demand on their time.

For **FCT consortium coordinators**, there is an equally crucial role. They are the primary point of reference for all parties and need to be able to engage constructively with the different components of the consortium — operational, technical, research and policy alike. An approach that genuinely integrates competences across these different knowledge domains is of fundamental value, supporting a model of shared learning and growth among strategic partners at European level and with police forces. Building on this role, the recommendations point to the value of treating training, piloting and organisational-fit assessment as a single, integrated work package from the proposal stage, rather than as parallel or sequential activities. Building in a structured, documented process for reconciling the differing priorities of operational, technical and policy partners before specifications are finalised, and identifying backup coordination capacity for safety-critical field activities in advance, are both low-cost measures relative to the risks they mitigate. Value should not be placed solely on acquiring competence in operating the tool, but, more importantly, on its potential day-to-day use, the level of innovation it can bring, and how it integrates into the overall capabilities of the individual police officer and, more broadly, into the organisational model of the LEA for which they work.

For **technical and research partners**, the report's findings on the strong co-occurrence between training needs and explainability needs suggest that investment in explainable, interpretable AI outputs should be planned as a capability-building measure in its own right, not solely as a technical or compliance requirement. Similarly, treating cross-border and inter-agency data-sharing arrangements as a design consideration from a project's outset, rather than a matter to be resolved once a tool nears deployment, would address a need that end users in this report raised unprompted and considered strategically important.

For **LEAs participating in FCT projects**, the findings suggest that internal capability-building efforts should not assume that need is evenly distributed across staff. Deliberately involving mid-career staff and decision-makers alongside more junior colleagues, and documenting end-user involvement from the earliest possible stage of a project, are both practices that this report's evidence associates with stronger organisational readiness outcomes. Beyond internal capability building, the literature reviewed in this report also points to a further dimension that LEAs may wish to consider: public trust in the use of AI by police forces depends less on the sophistication of a given tool than on citizens' broader trust in law enforcement itself. Internal capability-building efforts and external communication with the public may therefore be worth treating as connected, rather than separate, priorities.

A final consideration cuts across all four of these levels. Some of the most consequential factors shaping whether an AI-supported technological tool and its associated training are actually absorbed into daily practice are also among the simplest, yet they are rarely discussed explicitly. These include, for example, whether English can be assumed as a shared working language; physical distance and time-zone differences between partners; internal rules on device use; an agency's organisational model and related contingencies; the geographic scale over which it operates; and its varying degrees of direct experience with the criminal phenomena that a tool is meant to address.

The point is that LEAs and BGAs differ from one another in experience, operational capacity and existing technological tools, and consequently in their requirements and needs. They also operate across geographic areas marked by different criminal patterns, trends, threats and challenges, which shape end users' approach to project activities and to the complexity of the criminal landscape each project sets out to explore. The existing technological baseline across partner agencies can itself vary considerably, from very limited equipment to advanced tools. This, in turn, shapes not only what a given LEA asks of a project, but also its capacity to think beyond its current tools and articulate what would genuinely improve its working methods. The geographic and jurisdictional scope of a given technology also matters directly to end users, who are primarily concerned with strengthening their capacity to act within their own jurisdiction. Together, these factors point to a broader heterogeneity of end users' requirements and expectations that is easy to overlook in a careful evaluation of a tool's technical merits, yet that often determines, in practice, how readily a technology enters an operational context, or the extent to which it struggles to do so. Among the central challenges for FCT projects, then, is designing technological solutions capable of being tailored to police forces with very different needs and expectations, while still identifying and building on the key elements they hold in common. This means elaborating strategies that strengthen the capacity to investigate and classify available information, sustain a continuous knowledge-management process, and improve intelligence, monitoring and operations against the phenomena each project addresses.

A related and often underestimated point concerns what "training" is assumed to mean. End users frequently expect training to focus solely on how a technological tool functions, rather than on the criminal phenomenon it is meant to help address — its modus operandi, its evolving trends and its underlying dynamics. This is an understandable but often mistaken assumption, particularly for criminal phenomena that evolve rapidly or take on new forms; a tool's technical functioning cannot be meaningfully understood in isolation from the reality it is built to respond to. Relatedly, AI-based tools in particular can attract a degree of misplaced expectation, with some end users assuming that they might substitute for human judgement altogether rather than support it. This underscores, once more, the need for greater digital literacy, so that the respective roles of technology and human expertise are clearly understood from the outset. Meeting this challenge is not only a matter of training design: it requires making the substantive, research-based knowledge produced within FCT projects genuinely accessible and operationally useful to end users, by selecting what is necessary and presenting it in a clear, usable form.

None of these shifts requires abandoning the technical ambitions of FCT R&I; the case made throughout this report is that they are a precondition for those ambitions to be realised in sustained operational practice, rather than an alternative to them.

Aarab, A., El Marzouki, A., Boubker, O., & El Moutaqi, B. (2025). Integrating AI in public governance: A systematic review. *Digital, 5*(4), 59. https://doi.org/10.3390/digital5040059

ALIGNER - Artificial Intelligence Roadmap for Policing and Law Enforcement. CORDIS Project 101020574. https://cordis.europa.eu/project/id/101020574

ANITA - Advanced tools for fighting oNline Illegal TrAfficking. CORDIS Project 787061. https://cordis.europa.eu/project/id/787061

ARIEN - ARtificial IntelligencE in fighting illicit drugs production and traffickiNg. CORDIS Project 101121329. https://cordis.europa.eu/project/id/101121329

BORDERLINK - Border Control Agencies for Interlinked and Interoperable Future. CORDIS Project 101167589. https://cordis.europa.eu/project/id/101167589

Bradford, B., Yesberg, J. A., Jackson, J., & Dawson, P. (2020). Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. *The British Journal of Criminology, 60*(6), 1502–1522. https://doi.org/10.1093/bjc/azaa032

Bullock, K., Sidebottom, A., Laycock, G., & Tilley, N. (2022). The diffusion of police innovation: A case study of problem-oriented policing in England and Wales. *International Journal of Police Science & Management*. https://doi.org/10.1177/14613557221106084

Butler, M. J. R., & Ferlie, E. (2020). Developing absorptive capacity theory for public service organizations: Emerging UK empirical evidence. *British Journal of Management, 31*(2), 344–364. https://doi.org/10.1111/1467-8551.12342

CEPOL. (2026). *EU Strategic Training Needs Assessment 2026–2029*

Cohen, W.M., & Levinthal, D.A. (1990). Absorptive Capacity: A New Perspective on Learning and Innovation. Administrative Science Quarterly, 35(1), 128–152

COPKIT - Technology, training and knowledge for Early-Warning/Early-Action led policing in fighting Organised Crime and Terrorism. CORDIS Project 786687. https://cordis.europa.eu/project/id/786687

Council of the European Union (2026, 29 June). *Artificial intelligence: Council gives final green light to simplify and streamline rules* [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/

CREST - Fighting Crime and TerroRism with an IoT-enabled Autonomous Platform. CORDIS Project 833464. https://cordis.europa.eu/project/id/833464/results

DARLENE - Deep AR Law Enforcement Ecosystem. CORDIS Project 883297. https://cordis.europa.eu/project/id/883297

Dekker, R., van den Brink, P., & Meijer, A. (2020). Social media adoption in the police: Barriers and strategies. *Government Information Quarterly, 37*(2), 101441. https://doi.org/10.1016/j.giq.2019.101441

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive), (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680

EARTO (European Association of Research and Technology Organisations) (2020). Towards Horizon Europe: Bridging the Valley of Death in Security Research. Working Group Security & Defence Position Paper. https://www.earto.eu/earto-working-group-security-defence-paper-towards-horizon-europe-bridging-the-valley-of-death-in-security-research/

ENACT (2025). *AI Act and Law Enforcement*. Flash Report 09. European Network Against Crime and Terrorism. https://enact-eu.net/wp-content/uploads/2026/02/ENACT-FLASH-REPORT-09-AI-ACT-AND-LAW-ENFORCEMENT-FINAL.pdf

European Commission (2022). *EU Civil Security Taxonomy and Taxonomy Explorer*. Directorate-General for Migration and Home Affairs. https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study/eu-civil-security-taxonomy-and-taxonomy-explorer_en

European Commission (2026). *Digital Omnibus on AI: amendments to the Artificial Intelligence Act*. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Europol. (2024). *AI and policing: The benefits and challenges of artificial intelligence for law enforcement* (Europol Innovation Lab Observatory Report, Issue. https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing

Ezzeddine, Y., Bayerl, P. S., & Gibson, H. (2023). Safety, privacy, or both: Evaluating citizens' perspectives around artificial intelligence use by police forces. *Policing and Society, 33*(7), 861–876. https://doi.org/10.1080/10439463.2023.2211813

Graikini, D., & Ríos Morentin, D. (2024). *Internal Security Fund: Analysis of EU Member State Priorities (Analytical Report 03)* (ENACT – European Network Against Crime and Terrorism)

Grimmelikhuijsen, S., & Tangi, L. (2024). *What factors influence perceived artificial intelligence adoption by public managers? A survey among public managers in seven EU countries.* Publications Office of the European Union. https://data.europa.eu/doi/10.2760/0179285

High-Level Group (EU Commission). (2024). *Concluding report of the High-Level Group on access to data for effective law enforcement*

Information Commissioner's Office. (2018). *ICO finds Metropolitan Police Service's Gangs Matrix breached data protection laws*. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-finds-metropolitan-police-service-s-gangs-matrix-breached-data-protection-laws/

Kafteranis, D., Sachoulidou, A., & Turksen, U. (2023). Artificial Intelligence in Law Enforcement Settings: AI Solutions for Disrupting Illicit Money Flows. *eucrim – The European Criminal Law Associations' Forum, 18*(1), 60-66. https://doi.org/10.30709/eucrim-2023-006

Lindsay, R., Jackson, T. W., & Cooke, L. (2011). Adapted technology acceptance model for mobile policing. *Journal of Systems and Information Technology, 13*(4), 389–407. https://doi.org/10.1108/13287261111183988

Männistö, T. (2025). AI-Ready Customs Enforcement: Building Capabilities for the Future. PEN-CP Annual Study, Cross-border Research Association (CBRA). www.cross-border.org

Männistö, T., Wong-Chan, S., & Doherty, M. (2025). Customs Innovations Resulting from EU Projects: Game Changers or Forgotten Ideas? PEN-CP Annual Study, Cross-border Research Association (CBRA). www.cross-border.org

Mignone, M., & Scioneri, V. (2022). Training and Education During the Pandemic Crisis: The H2020 ANITA project experience. *European Law Enforcement Research Bulletin*, Special Conference Edition Nr. 5, 221–230. European Union Agency for Law Enforcement Training (CEPOL). https://www.cepol.europa.eu/api/assets/European_Law_Enforcement_Research_Bulletin_Special_Conference_Edition_Nr5.pdf

PARSEC - Parcel and Letter Security for Postal and Express Courier Flows. https://www.parsec-project.eu/

Pulkkinen, J., Huttu, K., & Suhonen, M. (2025). Systemic challenges in AI adoption in public social and health organizations in Finland: a technology-organisation-environment perspective. *Journal of Health Organization and Management, 39*(9), 435–456. https://doi.org/10.1108/JHOM-06-2025-0309

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 certain Union legislative acts (Artificial Intelligence Act), (2024). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

Ríos Morentin, D., & Alegria, A. (2024). *FCT R&I: An Analysis of EU Priorities 2014–2024 (Analytical Report 01)* (ENACT – European Network Against Crime and Terrorism)

Rogers, E.M. (2003). *Diffusion of Innovations* (5th ed.). Free Press.

ROXANNE - Real time network, text, and speaker analytics for combating organized crime. CORDIS Project 833635. https://cordis.europa.eu/project/id/833635

SALUS - Strengthening law enforcement with advanced IoT forensic tools. CORDIS Project 101225719. https://cordis.europa.eu/project/id/101225719

STARLIGHT - Sustainable Autonomy and Resilience for LEAs using AI against High priority Threats. CORDIS Project 101021797. https://cordis.europa.eu/project/id/101021797

Teece, D.J. (2007). Explicating Dynamic Capabilities: The Nature and Microfoundations of (Sustainable) Enterprise Performance. *Strategic Management Journal, 28*(13), 1319–1350

Teece, D.J., Pisano, G., & Shuen, A. (1997). Dynamic Capabilities and Strategic Management. *Strategic Management Journal, 18*(7), 509–533

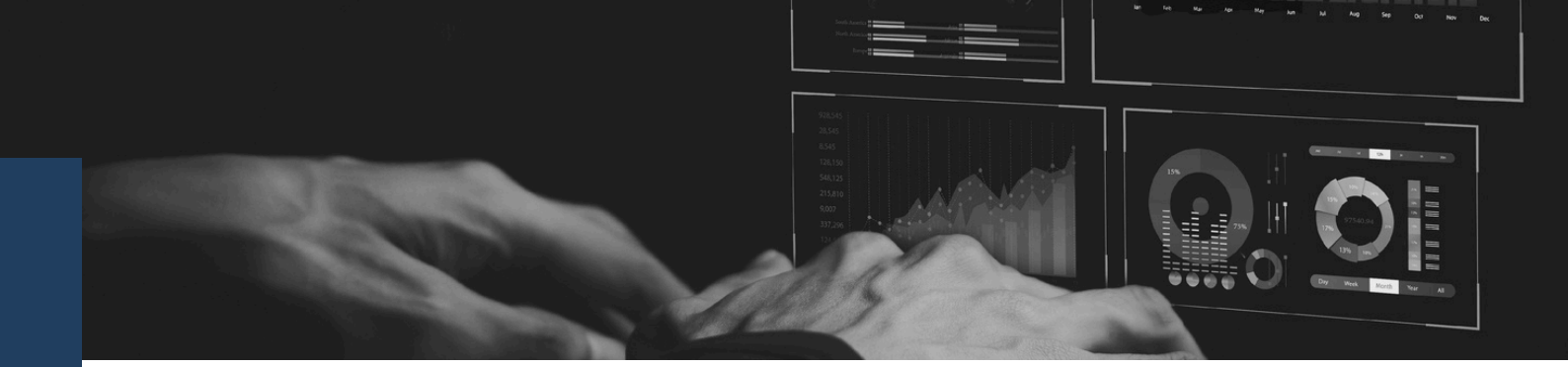
TENACITy - Living Labs as catalysts for experiential learning in law enforcement training: Insights from the TENACITy project. PMC. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC12828252/

Tornatzky, L.G., & Fleischer, M. (1990). The Processes of Technological Innovation. Lexington Books

UNICRI & INTERPOL (2024). *Not Just Another Tool: Public Perceptions of Police Use of Artificial Intelligence.* United Nations Interregional Crime and Justice Research Institute. https://unicri.org/sites/default/files/2024-11/Public-Perceptions-Police-Use-Artificial-Intelligence.pdf

WCO. (2025). *Illicit Trade Report.* https://www.wcoomd.org/en/topics/enforcement-and-compliance/resources/publications.aspx

Whelan, M., & Genoe, R. (2022). Law Enforcement Agency Capacity Building as a Driver for the Adoption of European Research. European Law Enforcement Research Bulletin, (6), 75–85.



ANNEX A: PROJECT MAPPING AND ORGANISATIONAL READINESS CODING

Table 4 - Organisational readiness mapping of thirteen H2020 and Horizon Europe FCT projects

PROJECT	CALL / PERIOD	TRAINING COMPONENT	PILOTING COMPONENT	END-USER VALIDATION COMPONENT	READINESS DIMENSIONS ADDRESSED*
INSPECTr (H2020)	SU-FCT01-2018 2019–2022	Dedicated capacity-building programme; training-needs analyses referencing CEPOL EU-STNA, ECTEG standards and Europol's Training Competency Framework.	AI-assisted cybercrime intelligence-sharing platform tested with LEA partners.	Continuous stakeholder consultation feeding curriculum design.	Skills (E); Processes (P); Coordination (P); Culture (–)
COPKIT (H2020)	SU-FCT03-2017 2018–2021	Innovative curricula covering the full Early Warning/Early Action (EW/EA) methodology, explicitly designed to facilitate LEA uptake.	EW/EA toolkit tested by LEAs in their own premises across use cases.	End User and Stakeholder Advisory Board (EUSAB), chaired by Europol, steering direction and outputs.	Skills (E); Processes (E); Coordination (E); Culture (P)
ROXANNE (H2020)	SU-FCT02-2018 2019–2022	No dedicated curriculum documented; uptake relies on demonstrated platform performance.	Speech/video/network-analysis platform tested on real case data in 9 EU Member States.	Early-version releases used explicitly to collect end-user feedback before finalisation.	Skills (–); Processes (P); Coordination (P); Culture (–)
DARLENE (H2020)	SU-FCT01-2019 2020–2023	"Extensive demonstration and training activities for LEAs" built into the workplan.	Augmented-reality ecosystem piloted in realistic scenarios ahead of field deployment.	Standing community of LEA organisations guiding development throughout.	Skills (E); Processes (P); Coordination (E); Culture (P)
ALIGNER (H2020, CSA)	SU-AI-2020 2021–2023	No technology-specific training; instead builds a recurring workshop series among LEAs, policymakers, industry and civil society.	No prototype piloting (Coordination and Support Action); focus on assessment methodology instead.	Structured technology-watch and risk/impact assessment process, plus a Fundamental Rights Impact Assessment tool co-designed with practitioners.	Skills (P); Processes (E); Coordination (E); Culture (P)

STARLIGHT (H2020)	SU-AI-2020 2021–2024	Needs largely still at diagnostic stage in public reporting; training plans tied to later use-case maturity.	Six use cases / twelve scenarios under joint development with LEA partners.	First 30 months dedicated to collecting needs and analysing current LEA practices via a co-creation approach.	Skills (P); Processes (E); Coordination (E); Culture (E)
CREST (H2020)	SEC-12-FCT-2016 ended 2021	Citizen training material produced and formally validated through a dedicated validation report.	IoT-enabled platform trialled with first-responder and citizen scenarios.	Guidance handbook explicitly built around "organisational and human factors variables" for implementation.	Skills (E); Processes (E); Coordination (P); Culture (E)
ANITA (H2020)	SEC-12-FCT-2016 2018–2021	No distinct training work package documented in public materials.	User-centred investigation system for online illegal trafficking, tested against real-world content.	"User-centred" design methodology embedding end-user input from early design stages.	Skills (–); Processes (P); Coordination (P); Culture (P)
PARSEC (Horizon Europe)	HORIZON-CL3-2022 ongoing	Training activities bundled with tool customisation for operational staff (per project work plan).	Explicit piloting of non-intrusive detection technologies across three use cases.	Customs authorities, police agencies and postal/express operators jointly define use cases and requirements.	Skills (P); Processes (E); Coordination (E); Culture (P)
BORDERLINK (Horizon Europe)	HORIZON-CL3-2023 ongoing	Explicit objective to reinforce training alongside detection capability.	Field validation of detection/identification technologies at customs checkpoints.	Communication and data-sharing mechanisms built in as a distinct capacity-building strand.	Skills (E); Processes (E); Coordination (E); Culture (P)
SALUS (Horizon Europe)	HORIZON-CL3-2024 ongoing	Training and standards development named as one of three delivery mechanisms alongside technology and ecosystem building.	Five pilot use cases with five police authorities and two critical-infrastructure operators.	Cross-sector pilot design spanning law enforcement and critical-infrastructure end users.	Skills (P); Processes (E); Coordination (E); Culture (P)
TENACITY (Horizon Europe)	HORIZON-CL3-2022 ongoing	Living Lab sessions explicitly designed as experiential-learning environments, not only technology tests.	Passenger Information Unit officers pilot data-driven tools within the same Living Lab sessions.	Dual-purpose Living Lab model merges validation and professional development in a single mechanism.	Skills (E); Processes (P); Coordination (P); Culture (E)
ARIEN (Horizon Europe)	HORIZON-CL3-2022 ongoing	Explainable-AI (XAI) outputs designed partly to build analyst interpretive competence, not only detection accuracy.	Co-creation approach across criminological, societal and legislative strands ahead of tool finalisation.	International-cooperation strategies engaging EU and non-EU LEAs, Customs and Border Guard Authorities and policymakers.	Skills (P); Processes (P); Coordination (E); Culture (P)

* E = explicitly addressed in public deliverables; P = partially or implicitly addressed; – = not addressed in publicly available materials. Coding reflects disseminated documentation, not necessarily internal project practice.

ANNEX B: RECOMMENDATIONS AND FUTURE DIRECTIONS

Q1 - SKILLS, PROCESSES AND COORDINATION CAPABILITIES

Table 5 - Recommendations by guiding question 1 about skills, processes and coordination capabilities

NR	THEME	GAP IDENTIFIED	RECOMMENDATION
R1	Integration	Training and piloting are consistently funded and documented as separate deliverables rather than as one interdependent strategy	Require projects to design training and operational testing as a single, integrated capability-building work package
R2	Competence validation	Procedural artefacts (Processes) exist without a corresponding mechanism to verify staff competence	Require a defined validation or certification pathway for operational staff
R3	Leadership differentiation	Organisational constraints beyond training - procedural alignment, time, resourcing - concentrate differently across leadership tiers (Organisational Capability and Operational Readiness)	Differentiate capacity-building and change-management measures by leadership tier, distinguishing procedural/coordination measures aimed at decision-makers from resourcing and time-allocation measures aimed at senior management
R4	Organisational fit	Compatibility with existing internal systems, roles and rules is the most frequently cited constraint on tool understanding and use, ahead of any technical shortcoming (5.2 Organisational Capability and Operational Readiness)	Require FCT projects to assess and document alignment with target agencies' existing systems and standard operating procedures as an explicit design criterion, alongside technical specifications, rather than treating it as a late-stage integration task
R5	Coordination resilience	Coordination of safety-critical, multi-agency field testing can depend on a single internal role, with no identified backup capacity if that person becomes unavailable	Require FCT projects handling hazardous or operationally sensitive test activities to identify backup coordination capacity (internal or specialist external) in advance, rather than only after an internal gap emerges
R6	EU training capacity	Train-the-trainer offer at EU level remains comparatively limited relative to other EU Justice and Home Affairs agencies, constraining the scale at which internally cascaded training can reach LEA staff	Expand train-the-trainer capacity and funding at EU level, rather than relying primarily on centrally delivered sessions to reach a growing target population
R7	Quality assurance	Externally delivered or outsourced training activities are not consistently quality-assured against a common standard	Require FCT projects delivering training through third parties or subcontractors to apply a defined quality-assurance framework, aligned with existing EU training quality standards
R8	Multi-stakeholder design	Technology requirements are sometimes defined by a single stakeholder group in isolation, without a structured process for reconciling the differing priorities of postal/customs, technical, and policy-level actors before specifications are finalised	Require FCT projects to apply a structured, documented multi-stakeholder requirements framework (capturing operator, technical, and policy perspectives) before finalising technical specifications, rather than defaulting to the perspective of whichever partner leads procurement
R9	Joint delivery	Training and pilot sessions delegated entirely to LEA-internal trainers, without technical partners present, limit the real-time clarification that would otherwise benefit the whole cohort rather than only the individual who asks	Require FCT projects to structure at least part of training and pilot delivery as joint sessions with technical partners present, rather than delegating delivery entirely to LEA-internal trainers post-handover

Q2 - RECURRING STRENGTHS AND WEAKNESSES IN TRAINING, PILOTING AND END-USER ENGAGEMENT

Table 6 - Recommendations by guiding question 2 about strengths and weaknesses in training, piloting and end-user engagement

NR	THEME	GAP IDENTIFIED	RECOMMENDATION
R10	Seniority differentiation	Training needs cluster around documentation and explainability and do not increase steadily with seniority, peaking instead at an intermediate career stage (Workforce preparedness)	Differentiate training design explicitly by career stage and functional/leadership profile, rather than assuming that training needs increase uniformly with seniority
R11	Explainability	The need for training and the need for explainable AI outputs strongly co-occur in the same respondents (Workforce preparedness)	Treat investment in explainable, interpretable AI outputs as a capability-building measure in its own right, complementing rather than substituting for training
R12	Delivery resilience	Training built around a single delivery modality is fragile to project disruption	Require projects to budget for an alternative delivery modality from the outset, and build a structured, iterative feedback mechanism between sessions
R13	Audience differentiation	Differentiated audiences (e.g., LEA vs. BGA) require distinct curricula rather than a single generic training offer	Require training curricula, and the materials that accompany them, to be explicitly differentiated by end-user function and institutional context from the design stage, distinguishing operational reference materials from full technical documentation
R14	Co-ownership	Organisational culture (end users as co-owners) is the least consistently documented readiness dimension (Section 4)	Require documented evidence of end-user involvement from the proposal-preparation stage
R15	Progressive onboarding	Training sessions for first-time users of complex, multi-module tools can front-load comprehensive platform functionality, overwhelming trainees rather than building confidence progressively	Sequence initial training around a single concrete use-case walkthrough before introducing full platform breadth, rather than covering comprehensive functionality in first-exposure sessions

Q3 - EMBEDDING CAPABILITY DEVELOPMENT SYSTEMATICALLY IN FCT R&I

Table 7 - Recommendations by guiding question 3 about embedding capability development systematically in FCT R&I

NR	THEME	GAP IDENTIFIED	RECOMMENDATION
R16	Post-project sustainability	Training materials lose relevance once no actor owns their post-project upkeep	Require an explicit post-project maintenance plan for training and coordination artefacts, naming a responsible organisation, as a funding condition
R17	Field-trial recognition	Field demonstrations and multi-agency trials build practical, procedural competence, including for the operational staff who take part in them, but are rarely recognised or funded as capability-building activities in their own right, and the operational/logistical burden they place on participating staff is frequently underestimated relative to the technology costs of the exercise	Formally recognise and fund field demonstrations/multi-agency operational trials as capability-building activities, with dedicated logistical support for end-users
R18	Training coordination	Multiple EU-level and project-level actors deliver LEA training with limited coordination among them, risking duplication and inconsistent quality	Strengthen coordination mechanisms between FCT projects and existing EU training bodies (CEPOL, ECTEG, Europol) at the design stage, rather than developing training in parallel with limited mutual awareness
R19	Digital literacy	A meaningful share of training needs concern baseline digital literacy (e.g., general digital skills, OSINT, graph/network analysis) rather than any single piloted tool (Workforce preparedness)	Consider a cross-project or EU-level digital-literacy offer for FCT-involved staff, addressing needs that fall outside the remit of any individual project
R20	Cross-border mechanism	Cross-border and inter-agency cooperation needs surface only incidentally, through voluntary free-text comments, rather than through a dedicated assessment mechanism (Cross-border or inter-agency cooperation)	Extend existing practitioner-assessment requirements in FCT projects to explicitly cover cross-border and inter-agency cooperation needs, alongside overall project outcomes
R21	Knowledge sharing	Training curricula, test protocols and demonstration outcomes developed within individual FCT projects are rarely shared systematically across the wider project population, limiting the extent to which later projects can learn from what earlier ones have already attempted, tested, or discarded	Consider a dissemination tier for training and testing materials across FCT projects, short of full public release, that accounts for the legitimate security-sensitivity of much of this material rather than assuming it away
R22	Compliance timeline	The regulatory deferral of AI Act high-risk obligations to December 2027 is not an isolated event: the applicable timeline for high-risk obligations has already shifted multiple times since the Act's adoption, as reflected in ENACT's own Structured Knowledge Base (ENACT, 2025), and may continue to evolve	Require FCT projects to build compliance-readiness training and documentation practices around a flexible timeline rather than a single fixed deadline, given the AI Act's demonstrated pattern of schedule revisions, so that tools reaching operational use are not left without trained personnel regardless of which specific deadline eventually applies

ENACT.
European Network Against Crime and Terrorism

@enact-network

enact-eu.net

Scan the QR code to visit ENACT online and read this report in digital format.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.