



**A project of the European Anti-Cybercrime Technology Development
Association (EACTDA)**



EACTDA National Nodes

D5.2 Report on the MVP PoC and on the validation in
the non-operational environments of the National
Nodes



**Co-funded by
the European Union**

Version:	1.0	
Delivery date:	November 2024	
Dissemination level:	Public	
Status	Final	
Nature:	Report	
Main author(s):	Evaldas Bruze	Seconded to EACTDA
Contributor(s):	Juan Arraiza	EACTDA
	Amaya Iglesias	EACTDA

DOCUMENT CONTROL

Version	Date	Author(s)	Change(s)
0.1	30/09/2024	Evaldas Bruze (L3CE, seconded to EACTDA)	TOC and initial text. Distributed for review.
0.2	30/10/2024	Evaldas Bruze seconded to EACTDA) Amaya Iglesias (EACTDA) Juan Arraiza (EACTDA)	Version for review
1.0	14/11/2024	Juan Arraiza (EACTDA)	Version reviewed and approved. Version distributed within partners.

TABLE OF CONTENTS

1. Executive Summary.....	4
2. Introduction	5
2.1. Overview of the Tools4LEAs project	5
2.2. Objectives of T5.2 Validation Task	6
2.3. Background on EACTDA National Nodes	6
2.4. Relation to other deliverables	6
2.5. Structure of the deliverable	7
3. Deliverable Scope and Goals.....	7
3.1. Description of MVP and NNs.....	7
3.2. Key Involved Actors and Stakeholders.....	8
4. Validation in Non-Operational Environments.....	8
4.1. Intra-Node Validation	8
4.1.1. NN Conceptual Structures and Operational Models.....	9
4.1.2. NN validation.....	10
4.2. Inter-Node Validation	11
4.2.1. Implementation of Inter-Node validation	11
4.2.2. Next Steps and Future Collaboration	12
4.3. Feedback Loop and Iterative Improvements.....	12
4.3.1. Structure of the Feedback Instrument	13
4.3.2. Feedback instrument Goals and Objectives	13
4.3.3. Feedback Loops	14
4.3.4. Operational Importance	14
4.3.5. Role of the National Nodes in the Feedback Process	14
4.3.6. Importance of the Feedback Instrument for end-users	15
5. Governance Framework for NNs	17
5.1. Governance and Procedures Validation.....	17
5.2. Regulatory and Soft Law Aspects.....	17
5.3. Role of Innovative Products from External Sources.....	18
5.4. Piloting the LT NN innovation management process with FusionSec	18
5.4.1. FusionSec Solution Overview.....	21
5.4.2. LT NN process structure	21
5.4.3. Role of LT NN in Innovation Development Path	21
5.4.4. Challenges in Transitioning the Innovation to EACTDA.....	22
5.4.5. Advancing Development of FusionSec with the LEAD-Pro project.....	22

5.4.6. Lessons Learned from the Pilot Process	22
6. Feedback Loop and Lessons Learned.....	23
6.1. National Nodes Feedback	23
6.1.1. Early NN Feedback loop results	23
6.2. Evaluation of Results from MVP and Inter-NN Validation	25
7. Conclusions and Next Steps	27
7.1. Conclusions.....	27
7.2. Next Steps	27
Annexes.....	28
List of Acronyms.....	28
Reference Documents	28
List of References:	28

1. Executive Summary

The *Tools4LEAs National Nodes (NNs) Report* (D5.2) outlines the validation of the Tools nationally and governance frameworks NNs established under the European Anti-Cybercrime Technology Development Association (EACTDA). The document provides an overview of the Pilot National NNs evaluation, conducted in non-operational settings across the NNs, which

are composed of national networks of public security practitioners fighting cybercrime (referenced through this document as targeted end users) (, researchers, and industry partners.

The project, in its second phase, seeks to enhance targeted end-users' capabilities in combating cybercrime by delivering and validating tools and fostering a sustainable framework. The National Tools Uptake validation focused on technical performance, usability, regulatory compliance, and iterative improvement mechanisms, while also refining the governance structure to support targeted end-users collaboration and effective deployment in their operational environments.

Key outcomes include national feedback on Tools functionalities with recommendations for enhancements, as well national feedback on NN establishments and the need for stronger stakeholder engagement to optimize governance frameworks. Future steps involve operational validation, improving stakeholder engagement within NNs, integrating additional services for tools operationalization, and continued development based on structured feedback mechanisms.

2. Introduction

2.1. Overview of the Tools4LEAs project

EACTDA is the acronym of the European Anti-Cybercrime Technology Development Association, which is a private non-profit association, established in San Sebastian, Spain. The members of the Association include European Union (EU) public entities fighting cybercrime, universities and research technology organisations, for-profit private companies, and other relevant actors in the field of the EU security research and innovation.

The Tools4LEAs projects are a series of projects that receive a Direct Award under the ISFP programme, and which main goal is to facilitate and promote the uptake of innovative technologies by EU public entities fighting cybercrime. EACTDA, via the Tools4LEAs projects, aims at further developing pre-existing assets, mainly from EU-funded security research and development projects, so that they are offered with no license cost and with access to the source code to EU public entities fighting cybercrime.

In the first Tools4LEAs project (v1; Jul'21 to Jun'23), the focus was on designing and setting up the infrastructures, processes, and governance / decision-making mechanisms, whilst delivering the first set of "fully-tested and operational-ready" tools via Europol's Tool Repository. Though 11 tools were further developed in the v1 project, 3 of them will not be released to their targeted audience as they did not pass the pre-established quality threshold of "operational-ready". Also, an End-User Advisory Board (EUAB) composed as of Oct'24 by 21 members from 14 EU member states and co-chaired by two Europol units (EC3 and Innovation Lab) was established and it is the body responsible for identifying and prioritising end-user needs and which has veto right over the decisions done by EACTDA/Tools4LEAs with regard to the tool development roadmap.

In the second Tools4LEAs project (v2; Jul'23 to Jun'25), it is proposed to double the number of tools delivered. Also, the repository of tools implemented in v1, and currently used to host the results of the Tools4LEAs projects, will be enhanced and reused to host the results of EU-funded security research projects (when relevant in the field of cybercrime). EACTDA will play the role of custodian of these results, and the technical, IPR, and administrative aspects needed to create this new repository of security research results will be put in place. In addition, the v2 project will include a pilot to proof the concept of initial and limited support & maintenance periods for a selection of tools.

Besides, a pilot of the concept of EACTDA NN will be included, with nodes planned in Lithuania, France, Spain, and maybe one or two additional ones. Also, a platform for end-users to evaluate online tools will be implemented. Finally, the v2 project will include activities to further build the community of Tools4LEAs stakeholders and to promote the creation and/or adoption of technical blueprints, and in general, of commonly accepted best practices.

2.2. Objectives of T5.2 Validation Task

Task T5.2 is a critical component of the Tools4LEAs v2 project, focusing on the validation of the MVPs developed within the NNs. This task aims to ensure that the governance frameworks, procedures, and innovative solutions are fully functional and aligned with the operational needs of target end-users. The validation is conducted in non-operational environments, allowing stakeholders to rigorously evaluate the products and governance mechanisms without the constraints of real-world deployment.

The objectives of this task are threefold:

1. To evaluate the governance and procedural frameworks at both intra-node and inter-node levels;
2. To validate the integration of innovative products, including those sourced externally;
3. To establish a feedback loop that facilitates iterative improvements in both governance and product design.

The outcome of this validation process is a comprehensive report that will inform future iterations of the MVPs and guide the transition to operational environments.

2.3. Background on EACTDA National Nodes

The concept of NNs was introduced as part of the Tools4LEAs project to enhance the local adoption of innovative solutions for the targeted end-users across EU member states. Each NN represents a national-level consortium of stakeholders, including targeted end-users, research institutions, and industry partners, working in concert to promote the operationalization of innovative tools.

NNs are designed to serve as local ecosystems that facilitate the validation, piloting, and eventual deployment of these tools. Each NN operates under the governance framework established by EACTDA, ensuring coordination and alignment with EU-wide law enforcement fighting cybercrime objectives. NNs are also tasked with tailoring the solutions to their national contexts, ensuring that the tools meet the specific needs of local law enforcement agencies.

The pilot phase of NNs, which is part of Tools4LEAs v2, includes nodes in Lithuania, France, Spain, and possibly other countries. This network of NNs is expected to play a pivotal role in ensuring that innovative tools are tested, validated, and refined before being rolled out in national operational environments.

2.4. Relation to other deliverables

This deliverable is closely related to the following deliverables:

- **D5.1 Design of the NNs overall solution:** Deliverable D5.1 presents the NNs maturity model approach, which is used in this self-assessment form.
- **D5.3 Report on the validation in operational environments and on the adoption, roll-out, and use of the NNs:** Deliverable D5.3 will elaborate on what is reported in D5.2 by presenting the work done in operational environments and during the initial phases of the adoption, roll-out, and use of the concept of NNs.

2.5. Structure of the deliverable

Overall deliverable is structured into seven sections:

1. Summary

2. Introduction - The introduction establishes the context for the deliverable by introducing the Tools4LEAs project and the specific objectives of Task T5.2. It provides background information on the NNs, their purpose, and their role in the broader project framework. The structure of the introduction follows a funnel approach: it starts with a general overview and progressively narrows down to the specific objectives of the task. The principle is to ensure that the reader has a strong foundation of understanding before diving into the technical details of the validation.

3. Deliverable Scope and Goals - This section details the scope of the deliverable and outlines its specific goals, which are centered around validating the MVPs and NNs. The principle here is to clearly define what the document covers and what it aims to achieve, ensuring that the reader knows what to expect from the rest of the report.

4. Validation in Non-Operational Environments - This is the core of the deliverable, where the validation process is described in detail. It is divided into sub-sections that cover both intra-node and inter-node validation, with a special focus on the feedback loops and iterative improvements.

- Intra-Node Validation: Discusses the testing and validation activities that take place within each individual NN.
- Inter-Node Validation: Highlights the collaborations between nodes, including specific examples like the cooperation between the Lithuanian and French nodes.
- Feedback Loop: Focuses on how feedback is gathered, analyzed, and used to improve both the tools and governance structures.

The principle guiding this section is completeness and transparency. It documents the validation activities comprehensively, ensuring that each step is clearly explained and backed by examples or results from the NNs.

5. Governance Framework for NNs - This section provides an analysis of the governance structures in place within the NNs and how they support the implementation and validation of the MVPs. It also assesses the legal and regulatory compliance of the NNs, ensuring alignment with relevant EU laws and regulations. The principle here is accountability: the section ensures that the governance frameworks are robust and provide the necessary support for operational success.

6. Feedback Loop and Lessons Learned - This section reflects on the lessons learned from the feedback mechanisms in place. It emphasizes the importance of continuous improvement and documents how stakeholder feedback has been used to refine the tools and governance frameworks. The principle behind this section is learning and adaptability, showing how iterative improvements are critical to the project's success.

7. Conclusions and Next Steps - The conclusions summarize the key findings from the validation process and set the stage for future work, particularly the transition to operational validation in real-world environments. The principle here is forward-thinking: while the document reports on completed tasks, it also provides a roadmap for the next phases of the project.

3. Deliverable Scope and Goals

3.1. Description of MVP and NNs

The Minimum Viable Product (MVP) developed within each National Node represents the first iteration of the innovative tools designed for targeted end-users per national end-users. Each

MVP is tailored to address specific challenges that targeted end-users face, incorporating technologies such as advanced data analytics, machine learning, and digital forensics. These tools aim to improve the operational capacity of national targeted end-users in areas such as cybercrime detection, investigation, and prevention.

The scope of Task T5.2 involves the validation of these MVPs within non-operational environments. This validation process is designed to test the functionality of the tools, assess their usability in different national law enforcement contexts, and ensure their national compliance with both technical and regulatory standards. The validation also includes an assessment of the governance and procedural frameworks established within each NN, ensuring that they provide the necessary support for the adoption and operationalization of the MVPs.

The National Nodes serve as the primary platforms for customizing, tailoring, validating, coordinating the implementation, maintenance and support activities for the MVPs. Each NN comprises a network of national stakeholders, including law enforcement agencies, law enforcement fighting cybercrime experts, service providers and technology providers. These stakeholders collaborate to deliver the MVPs and provide feedback on their effectiveness and potential for operational deployment.

3.2. Key Involved Actors and Stakeholders

The validation of the MVPs within Task T5.2 involves a diverse range of stakeholders, each playing a critical role in the evaluation process. At the national level:

- Targeted end-users are the primary end-users of the tools, providing insights into their operational requirements and assessing the tools' effectiveness in addressing real-world challenges.
- Research institutions and technology providers contribute by refining the tools based on feedback from law enforcement agencies, ensuring that they meet both technical and operational standards.

At the inter-node level:

- EACTDA serves as the central coordinating body, overseeing the governance and collaboration mechanisms between different National Nodes. EACTDA also plays a key role in integrating external products into the validation process, ensuring that innovative solutions developed outside the NNs are evaluated alongside the MVPs.

The involvement of these actors ensures a comprehensive validation process, with feedback loops established at both intra-node and inter-node levels. This collaborative approach ensures that the MVPs are refined and improved iteratively, based on the input of all relevant stakeholders.

4. Validation in Non-Operational Environments

4.1. Intra-Node Validation

Intra-node validation refers to the evaluation of the MVPs and governance frameworks within a single National Node. This process involves testing the tools in a controlled, non-operational environment, allowing stakeholders to assess their functionality and usability without the constraints of real-world deployment. The validation focuses on several key aspects:

- governance and procedural frameworks established within each NN are evaluated to ensure they provide adequate support for the implementation and operationalization of the tools. This includes an assessment of decision-making

processes, stakeholder roles, and the mechanisms for coordinating between different actors within the node.

- the tools themselves are tested for their technical performance and compliance with regulatory standards. This involves rigorous testing of the tools' functionality, ensuring that they meet the specific needs of law enforcement agencies in areas such as data security, privacy, and operational efficiency.
- feedback from stakeholders is collected and analyzed, allowing for iterative improvements in both the tools and governance frameworks. This feedback loop ensures that any issues identified during the validation process are addressed before the tools are deployed in operational environments.

4.1.1. NN Conceptual Structures and Operational Models

The situation of the different NNs as of October 2024 is as follows:

1. **Lithuania:** Operates under L3CE with informal governance mechanisms, involving stakeholders such as the police and StratCom. The NN's processes are largely based on best practices and rely on ad hoc funding. It is actively engaging stakeholders but lacks formal legal and innovation structures.
2. **Spain:** Structured within the Ministry of Interior, this NN shows a high maturity in governance and leadership, with formal mechanisms and clear authority. Membership includes select stakeholder categories, and funding is managed on a project basis. Innovation activities are moderate, with gradual enhancement in collaboration with industry and academia.
3. **France:** France's NN is in progress, built around existing networks and organizations. The NN leverages the French National Police Research Centre as a central hub, acting as a network for coordination among law enforcement agencies (LEAs), academics, and industry. The objective is to create a capability-driven NN that brings together various stakeholders through a focused thematic approach. It operates on a collaborative network basis, aiming to mobilize existing components around specific topics.

Also, it is worth noting the work done in Portugal by Polícia Judiciária (PJ), an EACTDA member. A very similar concept to EACTDA NN has been defined and it is being implemented within PJ. This PJ node operates through PJ's Directorate of Services for Innovation and Development, mainly engaging internal PJ members. It has formalized financial processes and high access to innovation facilities but lacks full external stakeholder representation and formal legal agreements. EACTDA's NN pilot and PJ have regular meetings to update each other and seek for synergies and concrete collaborations related to the concept of NNs.

In October 2024, a maturity assessment survey has been conducted in all NNs (and PJ). Below, the conclusions of the survey are presented. The details of the maturity assessment survey can be found at: https://ec.europa.eu/eusurvey/runner/EACTDA_NN_SELF_ASSESSMENT

Section	Lithuania	Spain	France	Portugal ¹
Vision, Strategy, and Governance	High	High	Moderate	High

¹ PJ is not taking formally part of the EACTDA NNs pilot

Management and Leadership	Moderate	High	Moderate	High
Membership	Low	Moderate	Low	Low
Funding	Low	Low	Low	Low
Legal and Regulatory	Moderate	Moderate	Low	Moderate
Innovation Uptake	Low	Low	Low	Low

Table 1 - Summary of the NNs maturity assessment survey conducted in October 2024

The common maturity level across these NNs can be characterized as **Low and moving towards moderate**, with strengths in high-level governance structures and leadership but lacking consistency in documented processes, formalized membership rules, and sustained financial and legal frameworks. Moving towards high maturity would require formalizing governance and funding structures, broadening stakeholder engagement, and enhancing innovation infrastructure.

4.1.2. NN validation

Validation instrument: https://ec.europa.eu/eusurvey/runner/EACTDA_NN_2024_1

National Node (NN)	Establishment Status	Governance Structure	Selected Solution for Validation	Validation Stage	Challenges	Limitations	Suggested Support
France	In Progress (Feb 2025)	In Progress	Not specified	N/A	Stakeholder engagement, diverse landscape, limited coordination	HR, technical infra, funding	Dedicated HR
Spain	Established	Yes	Person detection and re-identification	Functional evaluation	None significant	HR, technical infra, funding, governance	Increased internal resources
Lithuania	In Progress (May 2025)	In Progress	Fusion Sec	Functional evaluation	Leader availability	HR, technical infra, funding, governance	Dedicated funding
Portugal¹	Not formally established, uses DS-ID for implementation	Yes	N/A	Functional evaluation	Technical and budget limitations	HR, technical infra, funding	Prioritization of initiatives

Summary of Findings

Establishment and Structure:

- Most NNs are either recently established or in progress, with varying degrees of formal governance and legal status. Notably, Portugal operates through its existing Directorate for Innovation (DS-ID), bypassing formal NN establishment.
- In all three pilots some rethinking and dedicated effort for improved frameworks for engaging stakeholders across targeted end-users and other entities are critical for smoother NN operations.
- Establishing clearer governance structures, including decision-making protocols and leadership roles, to ensure cohesive functioning and get some level of formalization.

Validation of Solutions:

- NNs (e.g., Spain and Lithuania) are actively validating solutions like person re-identification tools and cross-capability planning for public events, addressing security and operational needs for law enforcement.
- Difficulty in securing sustained engagement from diverse stakeholders, limited access to dedicated human resources and funding, barriers in infrastructure readiness may affect progress in next phases.

Common challenges include:

- Leaders are over-extended with multiple duties, impacting their involvement in NN activities.
- Lack of stakeholder engagement, resource limitations, and technical issues. Coordination issues were also observed in multi-stakeholder environments.
- Across the NNs, there is a need for additional human resources, dedicated funding, and technical infrastructure. Some respondents also highlighted the need for shared best practices and strategic scheduling of events to improve efficiency.
- Incomplete governance frameworks that hinder streamlined operations.

4.2. Inter-Node Validation

Inter-node validation focuses on the collaboration and coordination between different NNs. This process is critical for ensuring that the governance frameworks and tools developed within each NN are aligned with the broader objectives of the EACTDA network. Inter-node validation involves several key activities:

First, the coordination mechanisms between NNs are evaluated to ensure they provide a robust framework for collaboration. This includes an assessment of the governance structures established by EACTDA, as well as the processes for sharing information, resources, and best practices between NNs.

Second, the integration of external products into the validation process is assessed. This involves evaluating the ability of NNs to incorporate innovative solutions developed outside the network, ensuring that these products meet the same standards of governance, functionality, and usability as the MVPs developed within the NNs.

Finally, inter-node validation includes the collection and analysis of feedback from stakeholders across different NNs. This feedback is used to refine the tools and governance frameworks, ensuring that they are aligned with both national and EU-wide law enforcement fighting cybercrime objectives.

4.2.1. Implementation of Inter-Node validation

At the beginning of 2024, the LT and FR National Nodes engaged in a joint meeting focused on innovation within the police sector.

It was followed by Police Conference on innovations in Lithuania, 2024 September. This event facilitated discussions on cutting-edge tools and approaches for enhancing law enforcement capabilities, with a focus on:

- **Predictive Policing Tools:** Solution that enhance the capacity of law enforcement agencies to predict and prevent criminal activities per geographical areas based on the criminal statistics.
- **AI in Disinformation Analysis:** Tools utilizing recent artificial intelligence development to analyze disinformation, a rising threat in EU countries.
- **AI for Online Terrorism Detection:** A toolset aimed at identifying and analyzing terrorist threats attributes having activities in online environments, providing early warnings to law enforcement.

- **Cyclope Initiative:** An initiative presented during the event, which focuses on enhancing public safety by integrating advanced surveillance and monitoring tools. The meeting was attended by key stakeholders from both the LT and FR nodes.

Event	Inter-Node Collaboration
2024.02.11	National Nodes concept review in Vilnius
2024.03.13	EACTDA Yearly Event in Portugal (Lisbon)
2024.04.30	National Nodes implementation plan internal review (online)
2024.06.07	EACTDA NN communication and dissemination workshop (ONLINE) 1
2024.06.13	EACTDA NN communication and dissemination workshop (ONLINE) 2
2024.09.18	EACTDA NN and Starlight Innovation uptake process workshop in Lisbon, Portugal
2024.09.18	EACTDA NN and LT Police Innovations conference priorities in Lithuania, (Vilnius + Online)
2024.10.22	EACTDA Yearly Event in Spain (Majorca)
2024.12.06	EACTDA NN concept review, LT NN Establishment in Lithuania (Vilnius)

Table 2 - Summary with the NNs inter-node coordination meetings held in 2024

Joint National Nodes Workshop (Scheduled for December 2024)

In December 2024, a follow-up workshop is scheduled to take place, focusing on the individual progress of NN and will involve practical sessions to ensure that the tools are validated across all National Nodes. The collaborative effort will continue to build on the work initiated earlier in the year, ensuring that pilot nodes remain aligned in their development and validation efforts.

Additional Collaborations and New Members

Beyond these key events, the collaboration between EACTDA National Nodes has expanded to include new members and initiatives. New stakeholders, including **PPHS**, **Laurea**, **WebIQ**, and **CERTH**, have expressed the need and potential for establishment of NN in respected MS: Poland, Finland, Netherlands, Greece. Additionally, ongoing collaboration with **European Cybercrime Training and Education Group (ECTEG)** has been pivotal in aligning training and education efforts across the nodes, ensuring that law enforcement personnel are adequately equipped to leverage the innovative tools being developed.

4.2.2. Next Steps and Future Collaboration

The next major milestone for this collaboration will be the December 2024 workshop, where the focus will shift toward validation of the tools and refinement of the solutions innovation uptake process defined earlier in the year. Moving forward, national nodes will continue to foster this partnership, sharing insights and processes to enhance law enforcement's capacity to deal with complex innovation uptake process challenge in cybercrime and security domains.

4.3. Feedback Loop and Iterative Improvements

The EACTDA National Nodes initiative seeks to support law enforcement and public safety agencies across Europe by providing innovative tools to address modern challenges in cybersecurity and crime prevention. The feedback instrument for the EACTDA National Nodes is a critical component in this process, ensuring that tools are validated, refined, and aligned with the real-world needs of end-users. This instrument serves multiple functions: gathering

structured and unstructured feedback, fostering interaction between tool developers and end-users, ensuring confidentiality, and facilitating continuous improvement.

The feedback instrument is designed to address the complexities inherent in law enforcement and public safety validation processes, where participants may be cautious about disclosing their technological experimentation and specific needs. The instrument also supports interactions across different countries and between multiple user organizations, ensuring effective intermediation without compromising confidentiality or objectivity.

4.3.1. Structure of the Feedback Instrument

The feedback instrument is composed of several key elements that ensure a comprehensive, structured approach to gathering and processing feedback. These components include:

1. **Organizational and Governance Structure:** Outlines the roles, scope, intended outcomes, and procedural guidelines for implementing the feedback process across National Nodes.
2. **Feedback Anonymization:** Ensures that all feedback remains confidential, protecting the identities of participants and allowing for objective responses.
3. **Validator-Developer Coordination:** Facilitates structured interaction between tool validators (end-users) and developers, ensuring that feedback flows efficiently and is actionable.
4. **Continuous Improvement Mechanism:** Establishes a loop for iterative development, where feedback informs regular tool updates and refinements.
5. **Engagement Facilitation:** Provides strategies and tools to encourage active participation from the National Node community, ensuring broad and representative input.
6. **Structured and Unstructured Feedback Options:** Allows participants to provide both formalized feedback and freeform comments, balancing quantitative data with qualitative insights.

4.3.2. Feedback instrument Goals and Objectives

The primary goal of the feedback instrument is to create a robust, transparent, and structured system for validating tools and fostering continuous improvement within the EACTDA National Nodes. Specific objectives include:

- **Facilitating Non-Subjective, Objective Feedback:** Ensures that feedback is based on measurable criteria rather than personal opinions, supporting unbiased validation.
- **Maintaining Confidentiality:** Protects sensitive information about the technologies, needs, and individuals involved, critical for law enforcement and public safety agencies.
- **Enabling Efficient Validator-Developer Interaction:** Coordinates interaction to ensure that feedback is clearly understood and implemented without requiring direct contact.
- **Supporting Continuous Improvement:** Establishes mechanisms for iterative tool development based on validated feedback from actual end-users.

- **Encouraging Active Community Engagement:** Builds a community of stakeholders who feel invested in the feedback process, ensuring their ongoing participation and input.

4.3.3. Feedback Loops

The feedback loop is a critical component of the validation process, ensuring that both the MVPs and governance frameworks are continuously refined based on the input of stakeholders. This iterative process involves several key steps:

- feedback is collected from law enforcement agencies, technology providers, and other stakeholders involved in the validation process. This feedback focuses on the functionality, usability, and compliance of the tools, as well as the effectiveness of the governance frameworks established within each NN.
- the feedback is analyzed and used to identify areas for improvement.
- the tools and governance frameworks are updated based on the feedback received, ensuring that they are ready for operational deployment.

This iterative process ensures that the tools meet the needs of law enforcement agencies and that the governance frameworks provide the necessary support for their adoption and use.

4.3.4. Operational Importance

The feedback instrument is strategically vital for the EACTDA National Nodes, as it facilitates informed decision-making and ensures that tools evolve in response to real-world needs. It addresses key strategic goals:

- **Aligning with National and EU Security Objectives:** Ensures that the tools validated through this instrument are fit for purpose, helping to align law enforcement capabilities evolution with recent technological advancements.
- **Maintaining Confidentiality and Objectivity:** Enables agencies to experiment with technologies discreetly, supporting strategic innovation without compromising sensitive information.
- **Building Trust Between Providers and Users:** By anonymizing feedback and ensuring structured intermediation, the instrument fosters collaboration and trust between tool developers and end-users, especially across MS.

Operationally, the instrument enables effective collaboration, feedback processing, and iterative development:

- **Streamlined Validation Processes:** Provides a standardized framework that makes feedback easier to gather, analyze, and act upon.
- **Facilitated Collaboration Across Agencies:** Supports coordinated feedback from multiple end-users, across different geographies (even in different MS), ensuring consistency and comprehensive operational readiness.
- **Effective Adaptation to Changing Needs:** Through continuous improvement, the instrument helps adapt tools to evolving operational contexts more proactively.

4.3.5. Role of the National Nodes in the Feedback Process

National Nodes play a central role in the feedback process, acting as facilitators and coordinators of feedback collection, anonymization, and interaction between validators and developers. Their responsibilities include:

- **Coordination of Feedback Activities:** Organizing sessions for feedback collection, ensuring that validators understand the process, and gathering input from various stakeholders within their jurisdiction.
- **Ensuring Confidentiality and Anonymity:** Processing and anonymizing feedback to protect sensitive information, ensuring that neither the tools nor the participants' details are compromised.
- **Facilitating Inter-National Collaboration:** Enabling cross-border interactions between developers and validators, especially important in cases involving multiple end-user organizations or tools tested across various countries.

The National Nodes are instrumental in bridging the gap between tool providers and end-users, fostering a collaborative environment while respecting the confidentiality needs of law enforcement and public safety agencies.

4.3.6. Importance of the Feedback Instrument for end-users

For law enforcement and public safety agencies, the feedback instrument is particularly valuable as it addresses their unique needs and constraints:

- **Confidentiality in Experimentation:** Many agencies are cautious about disclosing the technologies they are testing or the specific needs they aim to address. The feedback instrument enables them to provide meaningful input without publicly revealing these details.
- **Objective and Structured Feedback:** Law enforcement agencies require tools that are validated based on objective criteria. This instrument emphasizes structured, non-subjective feedback, ensuring that responses are actionable and focused on continuous improvement.
- **Avoidance of Direct Contact While Ensuring Collaboration:** Often, agencies prefer indirect feedback channels for reasons of confidentiality. The instrument facilitates efficient collaboration without requiring direct interaction between validators and developers, maintaining an adequate level of confidentiality.
- **Addressing Structured and Unstructured Feedback:** The instrument supports both structured and unstructured feedback, ensuring that participants can share general impressions as well as specific, structured insights. This flexibility enables better adaptation of tools to meet the varied needs of different agencies.

NB! A common challenge in feedback processes, particularly for law enforcement and public safety, is that feedback can be overly generalized or emotionally biased, often providing vague or unstructured impressions. This feedback instrument is specifically designed to mitigate such issues:

The EACTDA NNs feedback instrument is a vital tool in ensuring that the technologies developed for law enforcement and public safety are validated effectively and continuously improved. It balances the need for confidentiality with the goals of effective intermediation and collaboration across multiple agencies and countries. By emphasizing structured, objective feedback while also accommodating unstructured insights, this instrument supports the ongoing refinement of tools, making them more effective for end-users. The NNs play a pivotal

role in administering and maintaining the feedback process, ensuring that all stakeholders benefit from the collaborative efforts within the EACTDA framework.

5. Governance Framework for NNs

5.1. Governance and Procedures Validation

The governance framework within each NN plays a critical role in ensuring the successful adoption and operationalization of innovative tools. During the validation process, the governance structures are assessed to ensure they provide adequate support for decision-making, coordination, and stakeholder engagement.

Each NN operates under a governance framework established by EACTDA, which defines the roles and responsibilities of stakeholders, the decision-making processes, and the mechanisms for coordinating between different actors within the node. The governance framework is evaluated to ensure that it is aligned with the broader objectives of the Tools4LEAs project and that it provides the necessary support for the adoption and operationalization of the MVPs.

5.2. Regulatory and Soft Law Aspects

The legal and regulatory aspects of the governance framework are also evaluated during the validation process. This includes an assessment of the compliance of the tools and governance structures with relevant EU and national laws, as well as the internal policies and procedures established within each NN. The evaluation focuses on ensuring that the tools meet all legal requirements, including those related to data protection, privacy, and law enforcement fighting cybercrime.

The ELSA assessment, including AI compliance assessment, of any innovative product developed or integrated within a NN is essential for ensuring responsible and compliant innovation. When creating products intended for sensitive areas like law enforcement, it is critical to integrate privacy-preserving technologies from the outset. These technologies help to safeguard individual rights by minimizing data exposure and protecting personal information during data collection, processing, and storage.

However, the most significant risks of human rights infringements arise not from the technology itself but from its application in law enforcement activities. When innovative tools are used as part of routine operations by targeted end-users, there is an increased risk that improper handling or misuse could lead to privacy violations, unjust profiling, or other infringements on individual rights. While the responsibility for legal compliance during daily use of such technology rests with the targeted end-users, the NN can play a proactive role in supporting compliant and ethical practices.

To facilitate this, NNs could offer guidance and recommendations to national targeted end-users on the compliant use of innovative tools. This could involve developing best practices for data handling, emphasizing privacy and data protection, and advising on frameworks to mitigate the risk of rights violations. Additionally, NNs could provide training programs for personnel, focusing on privacy protection, personal data management, and ethical considerations associated with using these tools. These training sessions would ensure that the targeted end-users understand the boundaries and safeguards required by law and adhere to ethical standards when applying these technologies in real-world scenarios.

By embedding compliance support, guidelines, and training within their services, NNs would not only help reduce the risk of misuse but also contribute to a more responsible and transparent use of technology within law enforcement. Such proactive measures will foster greater public trust in both the technologies deployed and the agencies using them, ultimately promoting a balanced approach to innovation that respects individual rights and societal values. This support framework could also serve as a model for other sectors integrating advanced technologies in areas where legal and ethical considerations are paramount.

Soft law, including internal policies and procedures, is also evaluated to ensure that it provides adequate support for the adoption and operationalization of the tools. This includes an assessment of the internal rules established within each NN, as well as the procedures for coordinating between different stakeholders and managing the adoption of the tools.

The public procurement process often becomes a bottleneck for adopting innovative products, primarily due to the rigid requirements and lengthy procedures embedded in traditional procurement laws. Such regulations, while crucial for accountability and fairness, can hinder the rapid uptake of innovations, especially those developed by small and medium enterprises (SMEs) that may lack the resources to navigate complex procurement systems.

To address this, NN could play a transformative role by acting as "regulatory sandbox environments" where procurement procedures are simplified, enabling more agile and flexible purchasing processes for LEAs of innovative products. In this context, NN could test streamlined procurement pathways, providing exemptions from standard procurement rules or introducing tailored processes that reduce administrative burdens while maintaining compliance with essential regulations.

By creating such regulatory (procurement) sandboxes in NN it could accelerate LEAs innovation uptake by enabling faster adoption of novel technologies allowing LEAs to acquire innovative solutions without extensive delays and from the supplier that NN or LEA helped to develop the innovations, or it was jointly developed by them. The simplified public procurement processes would lower entry barriers to targeted end-users market for SMEs and research organizations. NN controlled environment – regulatory sandbox - would allow targeted end-users to identify potential challenges and best practices, ensuring that innovative products are effectively integrated into targeted end-users services without compromising on accountability. Ultimately, if successful, these NN sandboxed procurement pathways could inspire more permanent policy changes encouraging a national or even EU-wide shift towards procurement models that better support innovation, agility, and responsiveness in the law enforcement area.

5.3. Role of Innovative Products from External Sources

In addition to the tools developed within each NN, the validation process also involves the evaluation of innovative products sourced from outside the network. These products are integrated into the validation process to ensure that they meet the same standards of governance, functionality, and usability as the MVPs developed within the NNs.

The integration of external products is a key component of the inter-node collaboration, ensuring that the NNs are able to incorporate innovations developed outside the network into their operations. This process involves rigorous testing and evaluation of the external products, as well as coordination between the NNs and EACTDA to ensure that the products are aligned with the broader objectives of the project.

5.4. Piloting the LT NN innovation management process with FusionSec

Lithuanian National Node (LT NN) operates under the coordination of the L3CE which is a Research and Technology Organization (RTO). Given that access to Europol's Tool Repository (ETR) and the EACTDA tools repository is primarily restricted to target end-users, LT NN focuses on managing external innovations that fall outside the scope of the ETR and EACTDA tool portfolios.

Therefore, LT NN's primary objective is to assist national LEAs in adopting innovative solutions offered by the National Node. This LT NN function aligns with EACTDA's goal of expanding its portfolio of tools designed to tackle the investigative challenges associated with cybercrime.

Further we describe the piloting process to test FusionSec software platform in the scope of LT NN.

<...> the whole NN eco-system is involved in variety of activities, that can produce security relevant outputs. Those activities include participation in different projects, research made in academia, new solutions or adaptive solutions developed by industry. All of this might be of interest for LEA's. At this point the responsibility of NN operating body is to collect all information, cluster it into some groups where solutions can be interlinked or provide similar or integral functionalities. Based on this list, NN operator should initiate the review of preselected innovations with LEAs. Initial list should be aligned with respective representatives from LEAs.

Preselected and aligned innovations are then to be reviewed by LEA representatives. This can be done in the format of demonstrations or presentations. In case of NN LT, innovations are reviewed by Innovations group at the National Police Department. In other NNs this can be done by other relevant groups or entities, depending on the structure of NN and engaged LEAs.

Based on review results, LEA provides short feedback on the relevance of presented solutions. If presented solution is not relevant to national LEAs, the process ends. In case the solution is not relevant, but mature enough, it can be forwarded to EACTDA or other NN for their consideration but is not further handled by the initial NN.

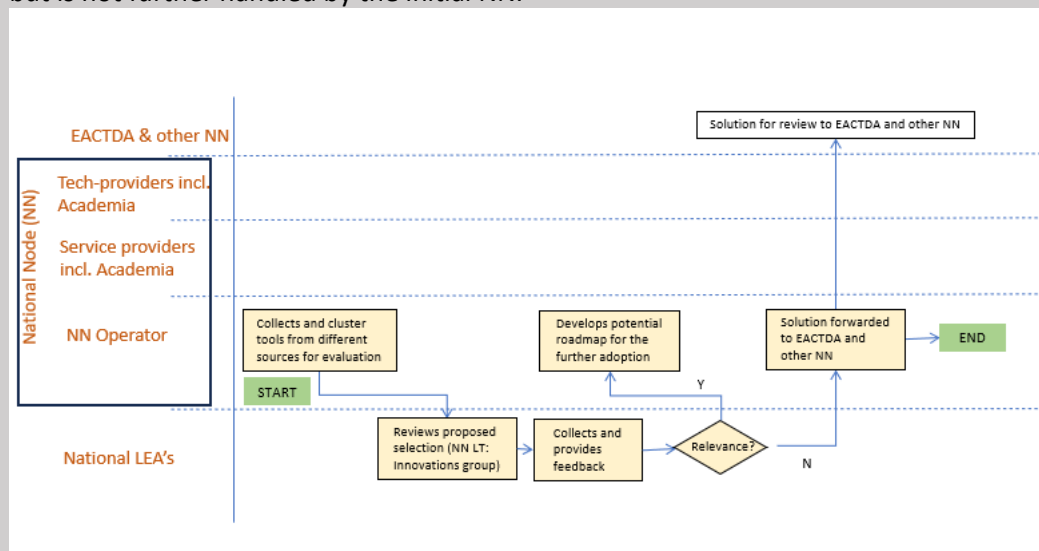


Figure 3 – NN initiated solution selection process.

Further activities of NN are related to the further development of the solution for the adoption of national LEA. This process is only started if presented solution is relevant and LEA is interested in further development or NN has LEA status and can assist with LEA specific tools, available in ETR or other limited access repositories.

The process is started by NN operating entity by developing the roadmap for further adoption. The process steps can be different and implemented in different sequence, but it usually will contain steps described further.

For further development / adaptation of potential solutions funding is essential. Therefore, NN operator should first identify potential funding opportunities. Those can vary from LEA funds to regional, national or EU level funding instruments. In some cases, if no suitable funding instruments are available, solution related activities can be postponed.

In parallel for funding, national compliance check can be done. Depending on the competence, this can be done by different actors of NN. Sometimes involvement of Academia might be needed, in some cases additional analysis might be needed (e.g.: description of “intended use”, etc.).

If some minor changes are needed for national compliance, the developer of the solution makes the necessary changes (if changes are not possible, solution is not to be developed further). In case significant effort is needed, further adoption depends on the available funding and those changes should be included in the features for further development.

Next step is to define the features for additional development. This can be different aspects, like language, compliance changes, data integration, or others. Those have to be defined by LEAs who consider solution for up-take.

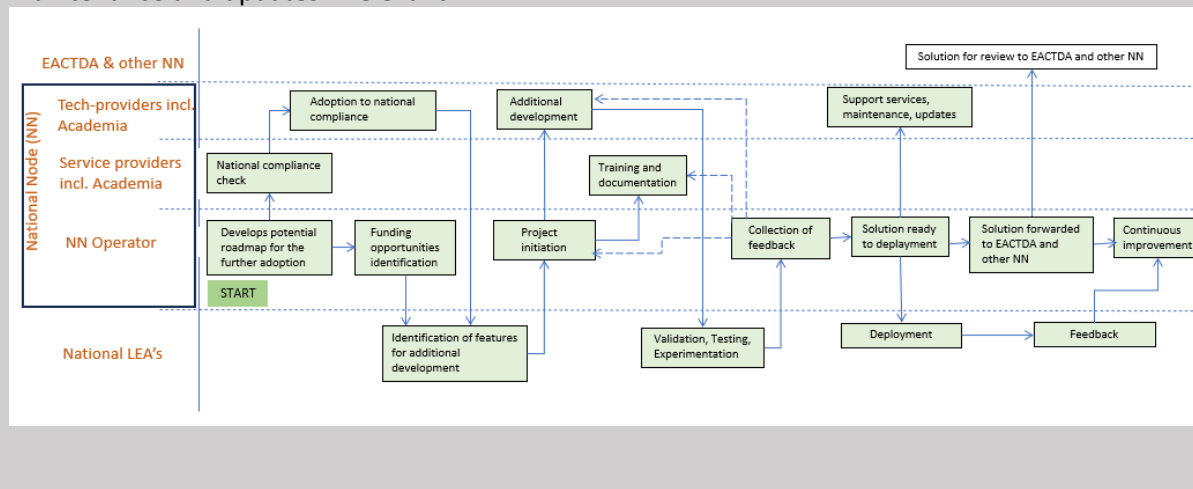
Based on this and funding instruments, NN operator initiates the project. Project can contain different steps. Those can include additional technical development, preparation of supporting materials (e.g.: manuals, training materials) or other relevant components. Depending on the competence, different components can be developed by different actors of the NN. Mainly this is done by technical providers and service providers.

When additional developments are completed, solution is available for testing, validation, or experimentation. The main actor at this step are LEAs', but they can also be supported by other actors of the NN. Some can provide data, develop scenarios, provide technological environment for testing etc.

NN operator collects the feedback from validation, testing or experimentation activities and this might result in some additional developments, corrections, or clarifications. So the process can be returned back to development and repeated testing. Such cycle can be repeated several times if funding is sufficient, or new funding instruments are utilized.

After completion of the project or several iterations the solution is ready to be deployed. LEAs deploy it in their environment.

To ensure continuous improvements feedback is still to be collected in a structured way. This might lead to initiation of other projects. The provider of the solution handles support services, maintenance and updates if relevant.



The LT NN's innovation management process follows a structured, bottom-up approach that actively supports the national ecosystem through key activities.

LT NN's core responsibilities encompass identifying and consolidating the needs of national end-users (including LEAs and other organizations engaged in cybercrime investigations), conducting early-stage validation of innovations, organizing demonstrations aligned with national use cases, and facilitating the overall process of innovation development and adoption. To assess the effectiveness of the LT NN established processes, the LT NN conducted a practical exercise of piloting the FusionSec solution, co-developed by two SMEs: Nuuk Technologies (Spain) and UAB Iterato (Lithuania). In this chapter the process, observations and lessons learned are documented.

5.4.1. FusionSec Solution Overview

FusionSec is a software solution developed to facilitate the protection of public spaces during large-scale, high-risk events. This platform supports various aspects of event management, including planning, resource coordination, real-time data collection and analysis, and decision support for command-and-control centres. It enables digital evidence extraction needed to investigate criminal incidents occurring during events.

5.4.2. LT NN process structure

LT NN process falls into ecosystem of EACTDA, thus complies to EACTDA standards. Process is designed to efficiently accommodate interests and perspective of local LEAs. To achieve this, process is separated in the following steps:

1. **Structured Needs Assessment:** Regular engagement channels with national end-users are established to continuously gather and refine innovation needs. This includes workshops, interviews, and leverage of collaborative platform that capture both technical and operational requirements.
2. **Validation and Feedback Loops:** Early-stage validations involves hands-on testing and direct feedback sessions with national end-users to ensure that innovations meet real-world needs before proceeding to the next stage. This iterative feedback process is essential for aligning national operational demands with EACTDA's EUAB priorities.
3. **Cross NN collaboration:** Close ties with EACTDA and other NNs are established to streamline knowledge exchange and collective validation of innovations that hold cross-national value. As outcome, inter-node collaboration can enhance the relevance and scalability of solutions within the EACTDA ecosystem.

5.4.3. Role of LT NN in Innovation Development Path

Throughout FusionSec development LT NN played a facilitators role, providing guidance and support at each stage — starting with the initial concept to the creation of a functional prototype. This prototype was tested and validated within the operational framework of the Command-and-Control Center of the Lithuanian Police during three major public events. The development of FusionSec took place over a 12-month period, during which LT NN provided extensive mentorship to the development team, focusing on critical areas to ensure the innovation met real-world needs and achieved operational readiness.

Key areas of LT NN mentorship included:

- **Needs Analysis:** LT NN assisted in collecting and analysing the specific operational requirements of the Lithuanian Police to ensure FusionSec addressed targeted challenges in public space protection.
- **Partnership Matchmaking:** LT NN organized matchmaking events to help the technology providers find strategic partners capable of addressing identified needs.
- **Co-Creation Workshops:** By facilitating co-creation workshops, LT NN enabled active collaboration between end-users and technology developers, fostering a shared understanding and tailored innovation. Additionally, the LT NN provided comprehensive consultation on national regulations and data privacy considerations to prevent potential problems in the future use of innovation.
- **Demonstration Support:** LT NN played a vital role in planning and organizing demonstration sessions, providing essential exposure for FusionSec and engaging end-users from the Latvian and Spanish police forces, thus validating the tool across different national contexts.

- **Awareness and Outreach:** To bolster visibility, LT NN led awareness-raising activities through national media, presenting FusionSec at national and EU conferences, enhancing the platform's profile and potential reach.
- **Feedback and Improvement:** LT NN conducted follow-up sessions to gather end-user feedback, supporting iterative improvements that refined the solution further.
- **New End-User Engagement:** LT NN facilitated the engagement of additional stakeholders, including event organizers and law enforcement agencies from other EU countries, to broaden FusionSec's applicability and future adoption potential.

5.4.4. Challenges in Transitioning the Innovation to EACTDA

Transitioning FusionSec solution to EACTDA presented several challenges that must be addressed for the whole concept to work. These challenges include ensuring that the technologies meet the necessary readiness and maturity levels defined by EACTDA, as well as aligning with regulatory frameworks and licensing schemes. Development of a clear business case for innovative solution proved to be critical to encourage technology providers to engage with the EACTDA licensing model.

Addressing these challenges requires a coordinated effort among all stakeholders, including the NN network and EACTDA, to facilitate a smooth transition and maximize the impact of innovative solutions in LEA operations.

5.4.5. Advancing Development of FusionSec with the LEAD-Pro project

Recognizing above listed challenges, NN took proactive steps to advance FusionSec's further development.

LT NN coordinated the initiation of a new project, named "LEAD-Pro", which secured funding through the Horizon-CL3-SSRI-01-02 program.

The LEAD-Pro project involves a few EU LEAs each participating in piloting of FusionSec solution across distinct locations with unique use-case scenarios.

Upon project completion, the innovation would achieve a higher TRL, enabling it to meet EACTDA's standards for final assessment and potential inclusion in the EACTDA tools repository.

5.4.6. Lessons Learned from the Pilot Process

The FusionSec pilot demonstrated the critical role of the LT NN in innovation development pathway.

With LT NN holistic approach, it succeeded in aligning ecosystem members (technology providers, LEAs, ELSA experts and other stakeholders) toward the shared goal of creating innovation that fulfills diverse operational needs of a particular LEA – Lithuanian Police, in the next stage broadening it to diverse LEAs with various use-cases.

However, there were identified shortfalls and gaps in the process that require more in-depth assessment and validation within the NN network and EACTDA.

Notably, developing a robust business case is essential for technology providers for the acceptance of the model and the EACTDA licensing scheme.

By refining this process, the NN has the potential to become a powerful resource for enhancing the accessibility of innovations for targeted end-users across the EU. This improvement would create a more streamlined and compelling pathway for technology adoption, enabling targeted end-users to more effectively integrate new solutions into their operations.

6. Feedback Loop and Lessons Learned

6.1. National Nodes Feedback

The feedback loop implemented in Task T5.2 serves as a fundamental process to ensure the iterative refinement of both the Minimum Viable Product (MVP) and the NNs governance frameworks. The feedback mechanisms are designed to gather input from all relevant stakeholders, including law enforcement agencies, technology providers, policy makers, and the EACTDA governing bodies. Feedback involves cross-node coordination, wherein stakeholders from different NNs share their experiences and insights. This inter-node exchange is crucial for identifying common issues and best practices, allowing for the collective refinement of tools and governance mechanisms. Feedback is shared through periodic coordination meetings, hosted by EACTDA, and structured reporting processes to ensure systematic tracking of lessons learned.

The feedback gathered on the NN organization highlights several key challenges and opportunities for growth. Currently, the organizational structure of NNs in each Member State (MS) is still taking shape, and much of the work is being carried out through ad-hoc initiatives rather than established, consistent frameworks. With no dedicated employment structure in place, activities rely on the efforts of a few highly committed champions, who often balance these responsibilities alongside other demanding roles.

While it is acknowledged that it may be too early to finalize a sustainability structure and plan, questions have arisen regarding the long-term funding model and financial support for the NNs. The early stages of community establishment mean that members are still getting acquainted with one another, leading to a slower pace of collaboration. This has created a “chicken-and-egg” scenario, where limited interaction and collaboration hinder further development and cohesion among the NNs.

In addition, while the involvement of public security practitioners fighting cybercrime remains somewhat limited at this stage, the early development of NNs has been largely championed by NGOs and RTOs. The presence of varying NN structures across Member States provides valuable flexibility and room for experimentation. However, this diversity also brings challenges in defining a unified concept of NNs, as different structures contribute to a broader, more fluid understanding of what each NN represents and how it operates.

6.1.1. Early NN Feedback loop results

Evolving Structure of NNs Across Member States (MS)

- **Challenge:** Currently, the National Nodes lack a defined, consistent organizational structure across Member States. This early-stage framework is still in development and varies from country to country.
- **Actionable Consideration:** Establish a foundational framework with adaptable guidelines that each Member State can customize to their specific context. This could ensure a shared understanding of the NN model while allowing for tailored, localized implementations.

Reliance on Ad-Hoc, Activity-Based Leadership

- **Challenge:** In the absence of dedicated employment positions within the NNs, activities are driven by ad-hoc initiatives led by a few core individuals who often have other primary responsibilities.

- **Actionable Consideration:** Consider developing part-time or role-specific positions within each NN, even on a temporary basis, to support these key initiatives. Identifying funding mechanisms for such roles could help sustain activities consistently and reduce the workload on current champions.

Concentration of Responsibilities Among Core Champions

- **Challenge:** The workload within each NN is concentrated among a few leaders who, due to their extensive involvement, risk becoming overburdened. This reliance on a small group could impact the resilience and sustainability of the NNs.
- **Actionable Consideration:** Encourage the delegation of tasks and create mentorship opportunities to broaden the pool of engaged members. Developing a support network or team structure could help distribute responsibilities more evenly and support the NNs' continuity.

Lack of Long-Term Sustainable Vision

- **Challenge:** While it may be early in the NN lifecycle, there is currently no defined sustainability strategy or plan for securing future funding and resource support.
- **Actionable Consideration:** Begin developing a preliminary sustainability roadmap with potential funding sources and partnership models. Incorporating a plan for engaging public and private sector partners could strengthen the NNs' long-term viability.

Financial Support for Long-Term Activities

- **Challenge:** Questions remain around the long-term financing model for the NNs, especially as they transition from project-based support to sustained operations.
- **Actionable Consideration:** Explore and outline potential funding options, including EU programs, Member State contributions, and partnerships with industry stakeholders. Developing a diversified financial strategy could provide the stability needed for continued operations.

Early-Stage Community Building and Limited Collaboration

- **Challenge:** The NN communities are still forming, with members unfamiliar with each other. This stage of development has limited opportunities for collaboration, creating a “chicken-and-egg” dilemma in which the lack of interaction hampers growth.
- **Actionable Consideration:** Organize structured activities such as regular networking sessions, joint workshops, and knowledge-sharing events to foster connections. Investing in community-building activities early on could accelerate trust and collaboration among members.

Limited Involvement of Law Enforcement Agencies (LEAs)

- **Challenge:** Targeted end-users have limited involvement in NN activities, with current initiatives primarily led by NGOs and research and technology organizations (RTOs). This early-stage dynamic may not fully align with the NNs' intended focus on public safety and law enforcement support.

- **Actionable Consideration:** Increase outreach to targeted end-users by emphasizing the benefits of NN involvement for public safety and national security goals. Offering customized engagement opportunities for targeted end-users and involving them in pilot activities could encourage their active participation.

Diverse Structures Across Member States: Balancing Flexibility and Consistency

- **Challenge:** The flexibility of different structures across Member States allows for experimentation but also creates some ambiguity around the core concept of NNs, which may affect cohesion and a unified approach.
- **Actionable Consideration:** Define core principles that all NNs can adopt, while allowing flexibility for implementation at the national level. Establishing these core elements could help clarify the NN model and create a stronger collective identity across Member States

This feedback underscores the importance of ongoing efforts to refine the NN framework, foster stronger inter-community connections, and build sustainable engagement models to support long-term goals.

6.2. Evaluation of Results from MVP and Inter-NN Validation

The evaluation of results from the validation process provides a comprehensive overview of the MVP's readiness for operational deployment, as well as the effectiveness of the governance structures supporting each NN.

In evaluating the MVPs, several dimensions are assessed:

- **Technical performance:** This involves evaluating the tools' performance in simulated cybercrime scenarios, examining their capacity to assist targeted end-users in detecting, preventing, and investigating cybercrime activities. Key performance metrics include accuracy, processing speed, data integrity, and scalability.
- **Usability and integration:** The MVPs must be adaptable to existing law enforcement workflows and systems. Feedback focuses on how well the tools integrate with current IT infrastructures, databases, and operational platforms used by LEAs.
- **Compliance and security:** Evaluating the MVPs for their compliance with EU law enforcement fighting cybercrime standards and data protection regulations, such as the GDPR, is critical. This also includes ensuring that the tools adhere to national-level requirements for data security and confidentiality in law enforcement operations.

For the governance frameworks, the evaluation focuses on the following aspects:

- **Decision-making processes:** The ability of the NN governance bodies to coordinate actions, allocate resources, and make strategic decisions is assessed. This involves a close look at the processes for engaging different stakeholders, handling conflicting interests, and ensuring that end-user requirements are prioritized.
- **Stakeholder engagement:** The extent to which stakeholders, particularly end-users such as law enforcement agencies, are involved in the decision-making and feedback processes is evaluated. This ensures that the governance framework is not only top-down but incorporates the operational insights of those who will ultimately use the tools.

- **Cross-node coordination:** The mechanisms for inter-node collaboration, especially the sharing of resources, insights, and best practices, are critically evaluated. The effectiveness of EACTDA's role in facilitating this coordination is also assessed, as is the ability to integrate external innovative products into the nodes.

The results of these evaluations are then documented in a series of structured reports, which are circulated among the stakeholders for review. These reports form the basis for further refinement of both the MVP and the governance frameworks, ensuring that the next iteration of the tools is even more aligned with the needs of end-users.

Currently validation process is still in first iteration implementation and not all points are collected but the following emerged learning points have been shared among the NNs participants:

- Core processes for NN must be formulated and include:
 - NN presentation, testing, validation events must also be done on national level in order to ensure local stakeholders' engagement.
 - National Level maintenance and support services are critical for successful collaboration and solutions operationalizations.
- Process must be differently aligned between RTO and SME driven innovations as the business case, sustainability, and exploitation expectancies as well contexts are different.
- LEA and End-users are coming with different backgrounds, access to the information and experience in innovation uptake (central units constantly working with Europol or similar setups have higher expertise and understanding). Process should reflect more extensive new or lower maturity end-users onboarding.

7. Conclusions and Next Steps

7.1. Conclusions

Task T5.2 has provided an invaluable opportunity to validate the MVPs developed within the NNs, as well as the governance frameworks that underpin their operations. The validation process in non-operational environments has revealed several important insights that will shape the future development and deployment of the tools.

Key conclusions include:

- **MVP readiness:** The MVPs have demonstrated potential in addressing the operational needs of LEAs, in areas of digital forensics, data analytics, and cybercrime detection. However, further refinement is needed, particularly in terms of usability and scalability, to ensure seamless integration with law enforcement workflows.
- **Governance effectiveness:** The governance frameworks within each NN have proven effective in coordinating stakeholders and managing the validation process. However, improvements are needed in stakeholder engagement, particularly in ensuring that end-users have a more direct influence on decision-making processes.
- **Inter-node collaboration:** The inter-node collaboration mechanisms, facilitated by EACTDA, would be instrumental in ensuring the exchange of insights and best practices across NNs. This would allow for a more holistic approach to tool validation and refinement, ensuring that the tools are adaptable to different national contexts.

7.2. Next Steps

As Task T5.2 concludes, the focus shifts to several key next steps that will guide the future development and deployment of the MVPs and the governance frameworks.

1. **Operational Validation (Task T5.3):** Following the non-operational validation phase, the next step is to deploy the MVPs in operational environments. This will involve testing the tools in real-world law enforcement scenarios, allowing for a more rigorous evaluation of their functionality, usability, and compliance with operational standards.
2. **Refinement of Governance Frameworks:** Based on the lessons learned from the validation process, the governance frameworks within each NN will be refined to ensure more effective decision-making and stakeholder engagement. Special attention will be paid to strengthening the involvement of end-users in the decision-making process, as well as improving cross-node coordination mechanisms.
3. **Integration of External Innovations:** The NNs will continue to explore opportunities to integrate external innovative products into their operations. This will involve further collaboration with external stakeholders, including technology providers, research institutions, and policy-makers, to ensure that the tools remain at the forefront of law enforcement fighting cybercrime innovation.
4. **Continued Feedback and Iteration:** The feedback mechanisms established during Task T5.2 will be maintained and refined to ensure continuous monitoring and improvement of the MVPs and governance structures. This iterative process will be critical as the tools move towards operational deployment.

By following these steps, the Tools4LEAs project will continue to build on the foundation established in Task T5.2, ensuring that the tools developed are not only technically robust but also aligned with the operational needs of LEAs across the EU.

Annexes

List of Acronyms

This section will include a comprehensive list of all acronyms used in the document to ensure clarity and ease of reference for all readers.

Acronym	Full Term
EACTDA	European Anti-Cybercrime Technology Development Association
ECTEG	European Cybercrime Training and Education Group
ETR	Europol's Tool Repository
EUAB	End-User Advisory Board
GDPR	General Data Protection Regulation
LEA	Law Enforcement Agency
MVP	Minimum Viable Product
NGO	Non-Governmental Organisation
NN	National Node
RTO	Research Technology Organisation
SME	Small and Medium Enterprise

Reference Documents

This section will list all the documents referenced in the deliverable, including the relevant sections of the Tools4LEAs project materials and any external reports or guidelines used in the validation process. Where applicable, links to online versions of these documents will be provided to ensure easy access for readers.

List of References:

- Tools4LEAs v2 Technical Description (PART B)
- EACTDA National Nodes Conceptual Model Document
- National EACTDA NN Reports (France, Lithuania, Spain, Portugal)
- EACTDA NN Maturity Self-Assessment Reports (France, Lithuania, Spain, Portugal)