

D6.5: Standardisation, Exploitation and Sustainability Final Roadmap

Revision: v.1.0

Work package	WP6 - Dissemination, Communication, Exploitation
Task	Task 6.3 and Task 6.4
Due date	31/08/2026
Submission date	31/08/2026
Deliverable lead	DBC
Version	1.0
Authors	Erika Nika, Dafni Giakoumaki (Partner DBC), Mark Miller (CPT), Victoria Menezes Miller (CPT)
Reviewers	Anna Bolognesi (STAM)
Abstract	This deliverable presents the Final Standardisation, Exploitation and Sustainability Roadmap of the BAG-INTEL Project. It provides a consolidated assessment of the project's twenty Exploitable Results and defines the main pathways for their transition from research and demonstration towards sustainable implementation and wider deployment. The report consolidates the results into four Key Exploitable Results covering risk assessment and decision support, luggage re-identification and tracking, contraband detection and the integrated digital twin, knowledge and secure deployment layer. It also addresses exploitation opportunities, business cases, Intellectual Property Rights, stakeholder needs and standardisation requirements. The roadmap identifies key technological, operational and regulatory priorities for further maturity and deployment and sets out recommendations for post-project exploitation, sustainability, modular implementation, stakeholder engagement and continued standardisation activities.
Keywords	Standardisation, Exploitation, Sustainability, IPR, Ownership, Licensing

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	27/05/2026	1st edit - ToC	Erika Nika (<i>DBC</i>)
V0.2	23/06/2026	2nd edit	Erika Nika (<i>DBC</i>)
V0.3	01/07/2026	3rd edit	Daphne Giakoumaki (<i>DBC</i>)
V0.4	15/07/2026	4 th edit – incorporation of standardisation	Mark Miller, Victoria Menezes Miller (CPT)
V0.5	16/07/2026	5 th edit	Mark Miller, Victoria Menezes Miller (CPT)
V0.6	03/08/2026	Revision following review of 30/07/2026	Mark Miller, Victoria Menezes Miller (CPT)
V0.7	21/08/2026	Revision following review of 30/07/2026	Erika Nika, Daphne Giakoumaki (<i>DBC</i>)
V1.0	24/08/2026	Finalisation, ready for submission	Erika Nika, Daphne Giakoumaki (<i>DBC</i>)

DISCLAIMER



**Funded by
the European Union**

Project funded by



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
**State Secretariat for Education,
Research and Innovation SERI**

Funded by the European Union (BAG-INTEL, 101121309). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

COPYRIGHT NOTICE

© 2023 - 2026 BAG-INTEL

Project funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	Report	
Dissemination Level		
PU	Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project's page)	✓
SEN	Sensitive, limited under the conditions of the Grant Agreement	
Classified R-UE/ EU-R	EU RESTRICTED under the Commission Decision No2015/ 444	
Classified C-UE/ EU-C	EU CONFIDENTIAL under the Commission Decision No2015/ 444	
Classified S-UE/ EU-S	EU SECRET under the Commission Decision No2015/ 444	

* R: Document, report (excluding the periodic and final reports)

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

DATA: Data sets, microdata, etc.

DMP: Data management plan

ETHICS: Deliverables related to ethics issues.

SECURITY: Deliverables related to security issues

OTHER: Software, technical diagram, algorithms, models, etc.



**Funded by
the European Union**

Project funded by



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
**State Secretariat for Education,
Research and Innovation SERI**

EXECUTIVE SUMMARY

BAG-INTEL tackles the issue of ensuring effective customs control at international airport arrivals despite increasing passenger numbers and limited human resources. It has created an integrated AI-driven system that combines sophisticated contraband detection, luggage re-identification, risk evaluation, decision support, data integration, and operational optimization. This Final Standardisation, Exploitation and Sustainability Roadmap details how these innovations can advance from research into practical, long-term use, sustainable implementation, and broader deployment.

The roadmap is based on a systematic review of twenty Exploitable Results generated by the consortium. This review included quantitative analysis of innovation, exploitability, and potential impact, alongside qualitative examination of technological dependencies, market opportunities, ownership, intellectual property, stakeholder needs, and standards. It was further supported by developing business cases, an updated review of Intellectual Property Rights, and a second stakeholder survey on standardisation, which received 88 responses.

The analysis resulted in the consolidation of the twenty Exploitable Results into four Key Exploitable Results representing the principal functional layers of the BAG-INTEL solution:

1. **Customs Bag-Risk Assessment and Real-Time Decision Support Suite**, integrating risk indicators, data analysis, bag-level risk assessment and operational decision support;
2. **AI-Based Luggage Reidentification and Tracking System**, enabling suspicious luggage identified during scanning to be subsequently located within the customs environment without physical tagging;
3. **Advanced Contraband Detection System**, combining high-resolution baggage scanning with AI-assisted detection algorithms; and
4. **Integrated Digital Twin, Knowledge and Secure Deployment Layer**, providing the integration, simulation, knowledge management, security and lifecycle capabilities required for operational deployment.

A key conclusion is that these KERs are most valuable when functioning as modular, interoperable parts of a comprehensive customs-control system, rather than as standalone products. Their collective logic supports the entire process, from detection and risk assessment to inspection decisions, luggage re-identification, intervention, outcome recording, and ongoing performance enhancements. Simultaneously, modular deployment remains crucial, enabling individual KERs or their combinations to be implemented based on the technological maturity, operational needs, and procurement capabilities of each customs setting.

The business cases highlight national customs administrations and airport customs units as the main institutional users and purchasers. They are supported by airport operators, IT and security teams, technology providers, system integrators, and law enforcement organizations. Exploitation might involve hardware, software licensing, integration and customization services, operational consulting, training, maintenance, cybersecurity support, and long-term service. For public authorities, the value proposition goes beyond direct financial gains, offering improved inspection targeting, higher detection rates, better resource allocation, more consistent and auditable decisions, fewer unnecessary inspections, and smoother passenger flows.

Further operational maturity is required before deploying at scale. Main priorities involve validating performance in real airport settings, securing representative and legally acceptable data, managing false positives and negatives, integrating with diverse customs and airport systems, ensuring cybersecurity and data governance, and maintaining human oversight of intrusive or coercive decisions. Engaging stakeholders - such as customs authorities, airport operators, industry integrators, regulators, policymakers, and standardisation bodies - is vital for effective implementation.

The final IPR review outlines the ownership and management structure for the twenty Exploitable Results, including background assets, ownership and contributions, protection measures, licensing terms, and access arrangements after the project ends. Depending on each result's nature, protection could involve copyright, confidential know-how, trade secrets, proprietary licenses, or open-source models. For results with joint ownership, clear agreements must be in place regarding exploitation obligations, licensing, liability, and revenue sharing before broader market introduction.

The standardisation analysis shows that BAG-INTEL functions within a multi-layered regulatory environment instead of a single customs-specific standard. Relevant frameworks include customs risk management, data exchange, X-ray and CT equipment, video-surveillance interoperability, AI governance, cybersecurity, privacy, and operational requirements. Nonetheless, significant gaps exist, especially in customs-specific performance standards for AI-assisted contraband detection, interoperable interfaces among scanners, CCTV, targeting, and decision-support systems, as well as post-deployment AI performance monitoring.

The second standards survey confirms these results. It highlights international customs and law enforcement data sharing as the top standardisation priority. Meanwhile, Artificial Intelligence is seen as the most notable gap in standards. Responses suggest that operational tools like scanning and CCTV are relatively well-developed, but governance frameworks for trusted AI, data quality, explainability, accountability, human oversight, and privacy-focused data exchange still need further progress.

The post-project roadmap advises a phased strategy to transform the four KERs into modular, procurement-ready options. This includes validated performance data, deployment specifications, suitable licensing and pricing, along with training and lifecycle support. The joint exploitation should be backed by clearly assigned commercial leadership, with component owners and service providers aiding in integration, deployment, and maintenance. Using reference deployments and follow-up pilots can enhance operational evidence and facilitate the shift from demonstration to procurement. Simultaneously, ongoing collaboration with customs authorities, European institutions, the World Customs Organization, and relevant standardisation groups should prioritize trusted AI, interoperable data exchange, technology-neutral interfaces, and effective validation methods.

TABLE OF CONTENTS

DISCLAIMER	3
COPYRIGHT NOTICE	3
EXECUTIVE SUMMARY	4
TABLE OF CONTENTS	6
LIST OF FIGURES	11
LIST OF TABLES	12
LIST OF ABBREVIATIONS	13
1 INTRODUCTION	16
1.1 PURPOSE AND SCOPE	16
1.2 Approach for Work Package 6 and Relation to Other Work Packages and Deliverables	18
1.3 Relation to D6.3 and Evolution of the Strategy	21
1.4 RELATION TO Standardisation	23
1.5 Methodology and Structure of the Deliverable	26
2 ASSESSMENT OF EXPLOITABLE RESULTS AND IDENTIFICATION OF KEY EXPLOITABLE RESULTS (KERs)	29
2.1 OVERVIEW OF THE KER ASSESSMENT PROCESS	29
2.2 ASSESSMENT CRITERIA AND METHODOLOGY	30
2.3 ER ASSESSMENT RESULTS AND KER SELECTION	31
3 KER DESCRIPTIONS	38
3.1 Introduction to the KER Portfolio	38
3.2 KER A: Customs Bag Risk Assessment and Real-Time Decision Support Suite	39
3.2.1 General Description	39
3.2.2 Component ERs	39
3.2.3 Functional Scope	40
3.2.4 Value Proposition	40
3.2.5 Target Users and Market Segments	41
3.2.6 Exploitation Pathway	41
3.2.7 Key Risks and Dependencies	41
3.3 KER B: AI-Based Luggage Reidentification and Tracking System	41
3.3.1 General Description	41
3.3.2 Component ERs	42
3.3.3 Functional Scope	42
3.3.4 Value Proposition	43
3.3.5 Target Users and Market Segments	43

3.3.6	Exploitation Pathway	44
3.3.7	Key Risks and Dependencies	44
3.4	KER C: Advanced Contraband Detection System	44
3.4.1	General Description	44
3.4.2	Component ERs	44
3.4.3	Functional Scope	45
3.4.4	Value Proposition	45
3.4.5	Target Users and Market Segments	46
3.4.6	Exploitation Pathway	46
3.4.7	Key Risks and Dependencies	46
3.5	KER D: Integrated Digital Twin, Knowledge and Secure Deployment Layer	47
3.5.1	General Description	47
3.5.2	Component ERs	47
3.5.3	Functional Scope	47
3.5.4	Value Proposition	48
3.5.5	Target Users and Market Segments	48
3.5.6	Exploitation Pathway	49
3.5.7	Key Risks and Dependencies	49
3.6	Interdependencies Across the KERs	49
3.7	Overall Exploitation Significance of the KER Portfolio	50
4	KERS AS BUSINESS CASES	51
4.1	BUSINESS CASE FRAMEWORK AND APPROACH	51
4.2	BUSINESS CASE: KER 1 – CUSTOMS BAG-RISK ASSESSMENT AND REAL-TIME DECISION SUPPORT SUITE	52
4.2.1	Value Proposition	52
4.2.2	Target Market and Customers	53
4.2.3	Revenue Model and ROI Projections	54
4.2.4	Deployment and Delivery Model	55
4.2.5	Risks and Mitigation	56
4.3	BUSINESS CASE: KER 2 – AI-BASED LUGGAGE REIDENTIFICATION AND TRACKING SYSTEM	56
4.3.1	Value Proposition	56
4.3.2	Target Market and Customers	57
4.3.3	Revenue Model and ROI Projections	58
4.3.4	Deployment and Delivery Model	58
4.3.5	Risks and Mitigation	59
4.4	BUSINESS CASE: KER 3 – ADVANCED CONTRABAND DETECTION SYSTEM	60

4.4.1	Value Proposition.....	60
4.4.2	Target Market and Customers	60
4.4.3	Revenue Model and ROI Projections	61
4.4.4	Deployment and Delivery Model.....	61
4.4.5	Risks and Mitigation.....	62
4.5	BUSINESS CASE: KER 4 – INTEGRATED DIGITAL TWIN, KNOWLEDGE AND SECURE DEPLOYMENT LAYER	63
4.5.1	Value Proposition.....	63
4.5.2	Target Market and Customers	63
4.5.3	Revenue Model and ROI Projections	64
4.5.4	Deployment and Delivery Model.....	65
4.5.5	Risks and Mitigation.....	66
4.6	JOINT BUSINESS OPPORTUNITIES AND SYNERGIES ACROSS KERs.....	66
5	STAKEHOLDER ENGAGEMENT PLAN	69
5.1	OVERVIEW AND OBJECTIVES OF THE STAKEHOLDER ENGAGEMENT PLAN	69
5.2	STAKEHOLDER MAPPING AND UPDATE FROM D6.3	71
6	IPR MANAGEMENT FINAL UPDATE	77
6.1	Update on Background IP	77
6.2	Foreground IP Generated During the Project.....	78
6.3	IPR Matrix – Final Version	80
6.4	Ownership and Licensing – Final Arrangements.....	90
6.5	Project Results Protection – Final Status	90
6.6	Lessons Learned and Recommendations for Post-Project IPR Management	91
7	STANDARDISATION	92
7.1	Latest Developments in Standards and Standardisation Activities Customs Control of Airport Arriving Passengers Baggage.....	92
7.1.1	Standardisation Summary.....	92
7.1.2	Key Findings	93
7.2	Scope and Operating Context	94
7.3	Customs-Specific Standards and Guidance.....	95
7.3.1	WCO SAFE Framework and NII	95
7.3.2	WCO Data Model, API, PNR and Targeting.....	95
7.3.3	Detection Systems Beyond X-Ray	96
7.4	X-Ray, CT and Radiation-Protection Standardisation	96
7.4.1	Cabinet X-Ray Systems.....	96
7.4.2	Personnel and Cargo/Vehicle Systems	96

7.4.3	CT and Multi-View Imaging.....	97
7.5	Aviation-Security Standards Affecting Airport Baggage Scanners.....	97
7.5.1	4.1 ECAC CEP and EDS/EDSCB.....	97
7.5.2	EU Aviation-Security Implementing Rules	97
7.6	CCTV and Video-Surveillance Standardisation.....	98
7.6.1	ISO 22311 and Export Interoperability	98
7.6.2	IEC 62676 Family	98
7.6.3	DIN and CENELEC Adoption	98
7.6.4	CCTV Analytics.....	98
7.7	Artificial Intelligence Standards and AI Standardisation Activity.....	98
7.7.1	ISO/IEC JTC 1/SC 42 Standards.....	98
7.7.2	CEN-CENELEC/JTC 21 and the EU AI Act	99
7.7.3	DIN/DKE AI Roadmap.....	99
7.7.4	NIST and Other Non-European Frameworks	99
7.8	Standards Matrix.....	100
7.9	Procurement and Acceptance-Testing Implications.....	102
7.9.1	Recommended Tender Clauses for Customs	102
7.10	Data Protection, Fundamental Rights and Evidence	103
7.11	Standardisation Gaps and Expected Developments	103
7.12	Standardisation Conclusions.....	104
8	SECOND BAG-INTEL STANDARDS SURVEY	105
8.1	Objectives of the Survey	105
8.2	Methodology.....	105
8.2.1	Survey Design.....	105
8.2.2	Targetting the Stakeholder Community	106
8.2.3	Methodology for Analysis	106
8.3	Analysis of Replies to Survey	106
8.3.1	Question 1 -Identifying the Type of Stakeholder Respondent	106
8.3.2	Question 2 -Priority Areas for Standarization in Current Environment.....	108
8.3.3	Question 3 -Maturity Awareness of Standards Baseline	110
8.3.4	Question 4 -Areas in which Standards are Lacking.....	113
8.3.5	Question 5 - Known Areas of Standardisation Efforts	115
8.3.6	Question 6 - Stakeholder Recommendations	118
8.4	Evidence-Based Conclusions.....	120
8.5	Proposed Standards Roadmap for After the Completion of BAG-INTEL	121

8.6	Recommendation Outputs from this Survey	121
8.7	Bottom Line.....	124
8.8	Conclusions of Survey	124
8.8.1	Key Findings	124
8.8.2	Strategic Implications.....	124
8.8.3	Potential Conclusions.....	125
8.9	Messages from the Stakeholder Community	125
8.9.1	Message 1: Interoperability is the Dominant Concern	125
8.9.2	Message 2: AI is the Largest Standards Gap	125
8.9.3	Message 3: Operational Technologies are Ahead of Governance Technologies.....	125
8.9.4	Message 4: Stakeholders want Harmonisation Rather than More Isolated Standards	126
9	CONCLUSIONS.....	127
	REFERENCES.....	135
	ANNEXES	137
	ANNEX 1 - BAG-INTEL STANDARDISATION QUESTIONNAIRE Survey	137

LIST OF FIGURES

FIGURE 1-1 - HIGH-LEVEL WORKFLOW OF THE BAG-INTEL EXPLOITATION AND STANDARDISATION PROCESS.....	26
FIGURE 2-1 - OVERVIEW OF THE ASSESSMENT OF EXPLOITABLE RESULTS METHODOLOGY	29
FIGURE 7-1: REFERENCE ARCHITECTURE FOR ARRIVING PASSENGERS' BAGGAGE CUSTOMS CONTROL .	95
FIGURE 7-2: MATURITY PATH FROM MANUAL INSPECTION TO AI-ASSISTED DATA FUSION	97
FIGURE 7-3: GOVERNANCE CONTROL PRIORITIES FOR AI, CCTV AND X-RAY SYSTEMS.....	100
FIGURE 8-1: REPLIES RECEIVED ACCORDING TO STAKEHOLDER GROUP.....	107
FIGURE 8-2: STAKEHOLDER HEAT MAP SHOWING THE IMPORTANCE BY STAKEHOLDER GROUP	110
FIGURE 8-3: MATURITY / AWARENESS BASELINE ACCORDING TO STAKEHOLDERS REPLIES.....	111
FIGURE 8-4: HEAT MAP OF STANDARDS AWARENESS AND USAGE ACCORDING TO STATEHOLDER GROUP	112
FIGURE 8-5: STAKEHOLDERS' PERCEPTION OF AREAS WHICH LACK STANDARDS	113
FIGURE 8-6: IMPORTANCE VS STANDARDS GAP MATRIX	114
FIGURE 8-7: QUALITATIVE THEMES EMERGING ACROSS THE FREE-TEXT RESPONSES	115
FIGURE 8-8: KNOWN AREAS OF STANDARDISATION EFFORTS.....	116
FIGURE 8-9: COMPARISON OF STANDARDS NEEDS ACROSS THE CORE AREAS	117
FIGURE 8-10: STAKEHOLDERS' PRIORITY INDEX.....	118

LIST OF TABLES

TABLE 2-1 - OVERVIEW OF BAG-INTEL EXPLOITABLE RESULTS INCLUDED IN THE FINAL ASSESSMENT	32
TABLE 2-2 - QUANTITATIVE ASSESSMENT OF ERS	35
TABLE 5-1- STAKEHOLDERS MAPPING	72
TABLE 5-2- STAKEHOLDERS FUNCTION	75
TABLE 6-1- BAG-INTEL'S FINAL IPR MATRIX.....	81
TABLE 7-1: RELEVANT STANDARDS LANDSCAPE BY DOMAIN AND ISSUING ORGANISATION	92
TABLE 8-1: STAKEHOLDER GROUPS AND THEIR ROLES.....	108
TABLE 8-2: AREAS CONSIDERED IMPORTANT FOR STANDARDISATION	109
TABLE 8-3: SPECIFIC STANDARDS REFERENCED BY STAKEHOLDERS	111
TABLE 8-4: FOUR MAIN PRIORITY AREA RECOMMENDATIONS IN STANDARDISATION ACTIVITIES.....	118
TABLE 8-5: BREAKDOWN TO DEFINE TEN RECOMMENDATIONS IN KEY THEMES IN STANDARDISATION	119
TABLE 8-6: STAKEHOLDER GROUP AND TOP IMPORTANCE AND GAP SIGNALS	119
TABLE 8-7: WORKSTREAMS AND RECOMMENDED FOCUS	120
TABLE 8-8: KEY STANDARDS GAP IMPORTANCE RANKING.....	122
TABLE 8-9: IMPORTANCE, KNOWN, LACKING AND IN DEVELOPMENT RANKINGS IN RELATION TO STANDARDS.....	123

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
API	Application Programming Interface
APSS	Accessible Property Screening System
ASTM	American Society for Testing and Materials
CA	Consortium Agreement
CBP	Customs and Border Protection
CEP	Common Evaluation Process
CIA	Confidentiality, Integrity, Availability
CABRA	Connection-Analysis-Based Risk Assessment
CT	Computed Tomography
DICOM	Digital Imaging and Communications in Medicine
DICOS	Digital Imaging and Communication in Security
DMP	Data Management Plan
DSS	Decision Support System
ECAC	European Civil Aviation Conference
ECAC CEP	European Civil Aviation Conference Common Evaluation Process
EDS	Explosive Detection System
EDSCB	Explosive Detection Systems for Cabin Baggage
EOS	European Organisation for Security
ER	Exploitable Result

EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
HFOD	Hochschule für den Öffentlichen Dienst in Bayern
IATA	International Air Transport Association
IBM	Integrated Border Management
ICAO	International Civil Aviation Organization
ICCS	Institute of Communication and Computer Systems
IEC	International Electrotechnical Commission
IP	Intellectual Property
IP	Internet Protocol
IPR	Intellectual Property Rights
ISMS	Information Security Management System
ISO	International Standards Organization
KER	Key Exploitable Result
LTA	LEGIND TECHNOLOGIES AS
ML	Machine Learning
MRI	Magnetic Resonance Imaging
N/A	Not Applicable
NEMA	National Electrical Manufacturers Association
NIS	Network and Information Security

NII	Non-Intrusive Inspection
OA	Open Architecture
OH&S	Occupational Health and Safety
PESTLE	Political, Economic, Social, Technological, Legal, and Environmental
PNR	Passenger Name Record
ROI	Return on Investment
SDE	Smiths Detection Germany
SDO	Standards Development Organisation
SERI	State Secretariat for Education, Research, and Innovation (Switzerland)
STAM	Strategic Technology Analysis & Management
SWOTS	Strengths, Weaknesses, Opportunities, and Threats
TRL	Technology Readiness Level
TCP	Transmission Control Protocol
TSA	Transportation Security Administration
UGR	University of Granada
WCO	World Customs Organization
WP	Work Package

1 INTRODUCTION

1.1 PURPOSE AND SCOPE

The BAG-INTEL project addresses a critical challenge for contemporary customs administrations: how to maintain and improve the effectiveness of passenger baggage control at inland border airports as international air travel volumes continue to grow and the availability of customs personnel remains constrained. Customs authorities must identify baggage that may contain prohibited, restricted or undeclared goods within complex and time-sensitive airport environments. At the same time, they must avoid unnecessary disruption to compliant passengers, preserve the fluidity of airport operations and ensure that intrusive inspections are proportionate, justified and operationally manageable.

BAG-INTEL responds to this challenge through an integrated technological and operational approach. Rather than focusing on a single detection instrument or isolated software application, the project combines Artificial Intelligence, advanced baggage scanning, camera-based luggage reidentification, multi-source risk assessment, real-time decision support, knowledge representation, digital twin modelling and secure system integration. The project's value, therefore, lies in the interaction among multiple complementary results that collectively support the customs-control process, from the initial identification of suspicious baggage to the final decision and physical intervention.

Within this operational chain, advanced scanning and AI-assisted detection help identify potentially suspicious content. Risk-assessment components incorporate scanner-derived indicators, relevant external information, connection analysis, and statistically aggregated evidence. Decision-support tools present this information to customs officers in a structured, operationally usable form. Camera-based reidentification then supports the non-intrusive location of a bag selected for inspection when it later appears in the baggage-claim or customs area. The digital twin, knowledge, and secure-deployment components enable the system to be configured, integrated, maintained, and optimised for the specific conditions of an airport.

This deliverable defines the final standardisation, exploitation and sustainability roadmap for the BAG-INTEL results. It consolidates the work carried out throughout the project and translates the project's technological, operational, commercial, intellectual property and standardisation findings into a coherent post-project strategy. Its central objective is to determine how the results generated by BAG-INTEL can move beyond the research and demonstration context and progress towards further validation, operational adoption, commercial exploitation, institutional use and continued development.

The deliverable therefore provides the final assessment of the project's Exploitable Results. These results have been examined not only as technical outputs, but also as potential operational, commercial, methodological, training or research assets. The assessment considers their degree of innovation, technological maturity, practical exploitability, expected impact, ownership structure, dependency on other results, relevance to end-user needs, target markets, deployment requirements and potential pathways to further use.

A central feature of the final analysis is the consolidation of individual Exploitable Results into coherent Key Exploitable Results. This reflects the fact that customs authorities, airport operators and system integrators are unlikely to procure fragmented research components without the technical and organisational conditions required for their effective deployment. The project's results are therefore grouped into integrated solution bundles that address clear operational needs, including customs bag risk assessment and real-time decision support, AI-based luggage reidentification and tracking,

advanced contraband detection, and the digital twin, knowledge, and secure deployment capabilities required for system-level implementation.

The deliverable also translates these Key Exploitable Results into structured business cases. The business-case analysis examines the operational and institutional value offered by each solution, the principal buyers and users, the most plausible delivery and revenue models, the expected monetary and non-monetary return on investment, the conditions for deployment and the major risks that may affect commercialisation or uptake. Attention is given to the public-sector nature of the principal market. For customs administrations, value cannot be measured solely through financial return. It also includes improved inspection targeting, more effective personnel allocation, increased detection capacity, fewer unnecessary inspections, better traceability of decisions, and improved passenger flow.

The scope of the roadmap covers both individual and joint exploitation. Individual exploitation concerns the use of specific results by their owners or contributing partners, for example through integration into existing products, continued research, technology transfer, training, consultancy or licensing. Joint exploitation concerns the combined use of complementary results in broader deployment packages, pilot installations, commercial offers, procurement opportunities or follow-on research and innovation initiatives. This distinction is particularly important in BAG-INTEL, as several of the Key Exploitable Results are composite assets comprising multiple technical components and more than one result owner or service provider.

The document further sets out the final stakeholder-engagement approach. Stakeholders are treated as active participants in validation, adoption, and sustainability. Customs authorities, airport operators, law-enforcement bodies, airport IT departments, equipment manufacturers, technology providers, system integrators, policymakers, public procurement authorities, research organisations, and standardisation bodies each play a distinct role in the post-project pathway. Continued engagement with these groups will be necessary to validate performance, clarify operational requirements, prepare procurement specifications, ensure legal and regulatory alignment, develop commercial partnerships, and support future standardisation activities.

The scope also includes the final update to the project's Intellectual Property Rights arrangements. The deliverable consolidates information on Background and Foreground Intellectual Property, ownership of results, joint ownership, access rights, licensing conditions, protection instruments, and post-project responsibilities. This work is essential because exploitation depends on a clear understanding of which partner owns each result, which pre-existing assets are required for its use, which partners have contributed to its development, and which legal or contractual conditions apply to further deployment.

Standardisation constitutes another central dimension of the roadmap. BAG-INTEL operates at the intersection of customs procedures, non-intrusive inspection, baggage scanning, video surveillance, Artificial Intelligence, data exchange, cybersecurity, privacy and airport operations. No single standard governs the complete BAG-INTEL environment. The project must therefore be considered against a layered framework of standards, regulatory requirements, guidance documents and operational practices. The deliverable identifies the most relevant standards, examines their implications for system design and procurement, assesses existing gaps and proposes areas for future standardisation and pre-standardisation activity.

The second BAG-INTEL standards survey forms an important part of this evidence base. It gathers input from a broad range of relevant stakeholders on standards awareness, current use, priority areas, perceived deficiencies and future needs. The survey findings are used alongside the standards

landscape analysis to identify practical recommendations for trusted Artificial Intelligence, interoperable data exchange, equipment and system interfaces, operational testing, governance, and post-deployment monitoring.

Sustainability is understood throughout the deliverable as a multidimensional concept. Technical sustainability requires maintainable architectures, controlled software updates, model monitoring, cybersecurity and interoperability. Commercial sustainability requires viable value propositions, appropriate pricing and delivery models, clear partner roles and credible channels to market. Operational sustainability requires user acceptance, training, workflow integration and continued performance validation. Legal and ethical sustainability requires compliance with data protection, Artificial Intelligence governance, fundamental rights principles, and human oversight requirements. Institutional sustainability requires continued engagement with customs authorities, policymakers and procurement bodies. Knowledge sustainability requires documentation, research continuity, training, technology transfer and standardisation.

The roadmap is primarily addressed to the BAG-INTEL consortium and the owners and contributors of the project results. It is also intended to support customs administrations, airport stakeholders, public authorities, technology providers, system integrators, researchers, investors, policymakers and standardisation organisations that may participate in the further development, procurement, deployment or governance of BAG-INTEL-related solutions.

The business cases and exploitation pathways presented in the document should be interpreted as strategic and roadmap-level guidance. They do not replace the detailed commercial, contractual, or licensing agreements required before market deployment. Exact pricing, liability, maintenance, support, revenue-sharing and licensing arrangements must be agreed by the relevant partners on a case-by-case basis. Similarly, the standardisation analysis does not claim that BAG-INTEL can complete the development of a formal European or international standard during the project lifetime. Its purpose is to identify the relevant standards environment, provide evidence of gaps and priorities, and prepare a credible foundation for future standardisation or pre-standardisation work.

1.2 APPROACH FOR WORK PACKAGE 6 AND RELATION TO OTHER WORK PACKAGES AND DELIVERABLES

Work Package 6 provides the horizontal framework through which the results of BAG-INTEL are communicated, disseminated, positioned for exploitation, and connected with relevant stakeholder and standardisation communities. The Work Package is responsible not only for increasing awareness of the project but also for creating the conditions under which its results can be understood, validated, adopted, transferred, commercialized, or further developed.

The approach in Work Package 6 is based on the principle that exploitation and standardisation must evolve alongside the scientific and technical work. They cannot be treated as activities that begin only after technological development is complete. A result may appear promising from a research perspective but remain unsuitable for exploitation if ownership is unclear, integration requirements are not understood, operational users do not accept it, or applicable legal and standardisation requirements have not been considered. Conversely, an enabling result that receives less visibility as a stand-alone technology may be indispensable for secure deployment, interoperability or long-term maintenance.

For this reason, the final roadmap has been developed through continuous interaction with the project's technical, operational and management Work Packages. The relationship is bidirectional. The

other Work Packages provide the technical evidence, operational feedback and governance information required for exploitation and standardisation planning. Work Package 6, in turn, provides feedback concerning market relevance, stakeholder expectations, intellectual property, commercial packaging, procurement, interoperability and the conditions required for sustainable uptake.

Work Package 1 provides overall project management, quality assurance, risk management, innovation management, and data management framework. Its contribution is fundamental because the exploitation roadmap must remain aligned with the Grant Agreement, the Consortium Agreement, the project objectives and the responsibilities of the individual partners. Information on project progress, risks, deviations, result maturity, partner contributions and legal or ethical obligations supports the reliability of the final assessment. The project's management and governance arrangements also provide the basis for handling disputes, monitoring the quality of partner inputs and ensuring that exploitation decisions remain consistent with the contractual framework.

The legal, ethical, privacy, and data-management work undertaken in the project management context is particularly relevant to BAG-INTEL. Many of the project's results depend on sensitive operational information, passenger-related data, scanner images, CCTV feeds or external risk indicators. Their future exploitation therefore requires a clear understanding of lawful processing, confidentiality, security, data minimisation, access control and long-term data management. These considerations directly influence the feasibility of different deployment and service models.

Work Package 2 provides the requirements, architectural, integration and digital twin foundations of the project. It defines the operational needs of end users, translates those needs into system requirements, establishes a secure-by-design architecture, and develops the data, knowledge, and integration mechanisms required for the overall platform. It also supports a digital twin that replicates airport operations and enables examination of different configurations and what-if scenarios.

The outputs of Work Package 2 are essential to the exploitation analysis because they clarify how the individual components interact, what data and interfaces are required, how the system can be adapted to different airport environments and which components may be deployed independently. They also provide the evidence needed to define the Integrated Digital Twin, Knowledge and Secure Deployment Layer as a Key Exploitable Result. Without these integration, knowledge-management and deployment capabilities, the project's more visible detection and decision-support technologies could not be transformed into a coherent operational solution.

The end-user, legal and ethical requirements developed within Work Package 2 also help ensure that the exploitation strategy is grounded in real operational practice. Customs authorities do not adopt technologies solely because of their technical novelty. They require solutions that fit existing procedures, can be used by officers under time pressure, comply with national and European legal requirements and preserve institutional accountability. The exploitation roadmap therefore treats operational usability, legal acceptability and secure integration as central elements of market readiness.

Work Package 3 develops the AI-based capabilities for contraband detection and luggage reidentification. Its outputs include the collection and preparation of data, the development of automatic contraband-detection algorithms and the creation of image-analysis tools for luggage characterisation, tracking and reidentification. These results form the technological core of the Advanced Contraband Detection System and the AI-Based Luggage Reidentification and Tracking System.

The relationship between Work Package 3 and the final roadmap concerns both technological value and deployment feasibility. The assessment considers the novelty and maturity of the AI models, the

quality and representativeness of available datasets, performance under realistic conditions, requirements for annotation and retraining, and dependence on scanner or CCTV infrastructure. These factors determine not only whether a result is technically promising, but also how close it is to operational or commercial use.

The reidentification solution provides a particularly clear example of this relationship. The concept has strong potential because it offers a non-intrusive means of locating a bag selected for inspection without visible marking or manual tagging. Its exploitation prospects, however, depend on performance under variable lighting, different camera angles, baggage occlusion, crowded conditions and diverse airport layouts. Work Package 3 therefore provides both the core technological asset and the evidence required to identify the additional validation and deployment work needed after the project ends.

Work Package 4 develops the risk-assessment and decision-support capabilities that convert detection, external data and reidentification outputs into operationally usable customs intelligence. The relevant work includes the derivation of risk indicators, connection analysis, bag-level risk assessment, statistical aggregation, real-time visualisation, management decision support and continuous learning.

These results underpin the Customs Bag-Risk Assessment and Real-Time Decision Support Suite. They are central to the BAG-INTEL value proposition because detection alone does not determine whether a bag should be inspected. Customs officers require a structured understanding of the available evidence, the relative importance of different indicators and the rationale behind the system's recommendation. The exploitation roadmap therefore assesses the extent to which the decision-support tools improve targeting, traceability, consistency and resource allocation.

The outputs of Work Package 4 also raise important governance issues. AI-supported risk assessment must not result in unaccountable or fully automated intrusive decisions. Human officers must remain responsible for the final intervention, and the system must provide sufficiently clear information to support professional judgement. Explainability, logging, auditability, role-based access, and continuous monitoring are therefore treated as essential conditions for exploitation and standardisation.

Work Package 5 provides the testing, evaluation, demonstration and training evidence required to assess operational readiness. Its activities examine system performance, usability, user acceptance, integration with airport processes and the extent to which the results meet the needs of customs and other end users. This Work Package also develops the training curricula required for operational users.

The final exploitation roadmap draws upon these activities to distinguish between technical functionality and genuine deployment readiness. Successful operation in a laboratory or controlled test environment does not automatically demonstrate performance in a live airport. Testing and evaluation findings are therefore used to identify remaining technical limitations, site-specific adaptation needs, user-training requirements, and evidence of what future buyers are likely to request.

The training outputs of Work Package 5 are also relevant to sustainability. Technology uptake depends not only on equipment and software, but also on the capacity of customs officers and managers to understand system outputs, apply appropriate procedures, respond to alerts and recognise the limitations of AI-supported recommendations. Training is consequently treated as part of the exploitation offer and not merely as a dissemination activity.

Within Work Package 6 itself, the present deliverable is closely connected to the project's communication, dissemination, community-building and earlier exploitation activities. The communication and dissemination work created visibility for the project and provided channels through which its results could reach scientific, industrial, operational and policy audiences. Community-building activities established links with customs organisations, law-enforcement bodies, technology providers, research initiatives and European stakeholder networks.

These relationships supported the preparation of the final roadmap. They enabled the consortium to obtain feedback, identify potential users and partners, distribute the standards survey and assess the relevance of the project's results beyond the consortium. The dissemination and stakeholder-engagement activities therefore served as an evidence and validation mechanism for exploitation and standardisation.

The earlier D6.3 deliverable established the preliminary exploitation, Intellectual Property Rights, sustainability and standardisation framework. D6.5 builds directly on this foundation but reflects the project's more mature state. It uses final partner inputs, structured assessment results, consolidated business cases, updated ownership information and broader stakeholder evidence to define the post-project pathway.

Work Package 7 provides the ethics requirements that apply to the project. Although it does not generate a market-facing solution, its relevance to exploitation is substantial. BAG-INTEL technologies operate in sensitive security and border-control contexts and may involve personal data, behavioural information, video analytics, and AI-assisted decisions that have consequences for individuals. Ethical compliance, human dignity, fairness, proportionality, privacy, due process and human oversight must therefore remain embedded in any future deployment.

The relationship between Work Package 6 and the other Work Packages demonstrates that exploitation is not a separate commercial layer added to the project after development. It is the process through which technical maturity, operational evidence, ownership, legal compliance, stakeholder acceptance, market positioning and standards alignment are combined into a credible pathway towards post-project use.

1.3 RELATION TO D6.3 AND EVOLUTION OF THE STRATEGY

D6.3, Standardisation, Exploitation and Sustainability Strategy and Plan, established the initial structured framework for the exploitation and standardisation of BAG-INTEL. It documented the preliminary portfolio of Exploitable Results, identified the Background Intellectual Property contributed by partners, described initial ownership and protection principles, examined the market and competitive environment, mapped relevant stakeholder groups and presented the first analysis of applicable standards and potential standardisation gaps.

At the time of D6.3, many project results were still under development or had not yet undergone final integration, demonstration and evaluation. The exploitation strategy therefore relied partly on preliminary technological descriptions, expected progression in Technology Readiness Level, provisional ownership information, and early assumptions concerning target markets and pathways to uptake. D6.3 provided the strategic direction, but it could not yet offer a final prioritisation of results or a fully validated post-project roadmap.

D6.5 represents the maturation and operationalisation of that strategy. It does not simply reproduce the structure of D6.3 with updated dates or additional descriptive information. It reflects a shift from

preliminary planning to evidence-based prioritisation and from individual research outputs to deployable solution configurations.

One of the most important developments concerns the assessment of the Exploitable Results. D6.3 gathered and described the results submitted by partners, including their expected strengths, weaknesses, maturity and commercial potential. D6.5 subjects the full portfolio to a common evaluation framework based on innovation, exploitability and impact. This quantitative assessment is complemented by qualitative analysis of technical maturity, operational relevance, ownership, integration requirements, data dependencies and market positioning.

The purpose of the assessment is not to automatically exclude lower-scoring results. In an integrated system, certain enabling components may have limited stand-alone commercial visibility while remaining essential for interoperability, cybersecurity, data management or deployment. The final strategy therefore distinguishes between market-facing results, strategic components, enabling technologies, methodologies and outputs with primarily research, training or institutional value.

A second major development is the transition from individual Exploitable Results to Key Exploitable Result bundles. D6.3 largely described results separately, reflecting the manner in which they were generated by different partners and tasks. The final analysis demonstrates that the operational and commercial value of BAG-INTEL lies mainly in combinations of complementary results.

The Customs Bag-Risk Assessment and Real-Time Decision Support Suite combines risk indicators, connection analysis, risk aggregation, operational methodology and real-time visualisation. The AI-Based Luggage Reidentification and Tracking System combines detection, characterisation, matching, probabilistic optimisation, CCTV integration and deployment knowledge. The Advanced Contraband Detection System combines scanning infrastructure with AI-assisted detection. The Integrated Digital Twin, Knowledge and Secure Deployment Layer combines the platform, digital twin, knowledge graph, integration, encryption and deployment mechanisms required for system-level use.

This bundling logic reflects how potential customers are likely to approach procurement. Customs administrations do not ordinarily procure an abstract algorithm without interfaces, operational workflows, user support and maintenance. The evolution towards Key Exploitable Result bundles therefore represents a transition from a research-result perspective to a market and deployment perspective.

The strategy has also evolved from general exploitation intentions to structured business cases. D6.3 identified potential licensing, commercialisation, consultancy and integration routes. D6.5 examines these pathways in relation to each final Key Exploitable Result. The analysis identifies the value proposition, target customers, revenue logic, deployment model, expected return on investment, commercial roles and principal risks.

This business-case approach provides a stronger basis for partner decisions after the project. It makes it possible to distinguish between solutions that may be integrated into an existing product portfolio, solutions that require joint exploitation, service-based offerings, and results that are better suited to further research or technology transfer. It also clarifies the importance of recurring services, including integration, model calibration, maintenance, training, cybersecurity updates and long-term support.

Joint exploitation receives greater emphasis in D6.5. The earlier strategy recognised the possibility of collaboration among partners, but the final roadmap identifies more specific joint business opportunities. The full BAG-INTEL deployment model brings together all four Key Exploitable Results. Modular packages may also be offered, depending on customer needs and the maturity of the individual components.

This evolution makes the allocation of commercial roles more important. A composite Key Exploitable Result may involve one or more owners, a service provider responsible for deployment and maintenance, and a business champion or seller responsible for market engagement and contracting. Clear role allocation will be required before joint commercialisation can proceed.

The stakeholder strategy has similarly become more operational. D6.3 identified broad stakeholder groups and communication approaches. D6.5 links stakeholder engagement directly to the needs of the Key Exploitable Results. Customs officers are required for usability and workflow validation. Airport operators and IT departments are required for infrastructure and integration. System integrators are required for scalable deployment. Policymakers and regulators are required for legal and institutional alignment. Standardisation organisations are required for interoperability and assurance. Research organisations are required for further maturation.

The Intellectual Property Rights framework has also progressed from a preliminary record to a final reference structure. D6.5 updates the Background Intellectual Property inventory, records the Foreground Intellectual Property generated during the project and consolidates the ownership, contribution and licensing information in the final Intellectual Property Rights Matrix.

This update is essential because the bundling of results raises additional questions concerning joint ownership, access to Background Intellectual Property, licensing of complementary components, and revenue sharing. The final roadmap therefore identifies the post-project actions required to maintain protection, clarify unresolved arrangements and prepare result-specific exploitation agreements.

The standardisation strategy has undergone a comparable evolution. D6.3 identified relevant standards and gathered the initial views of stakeholders. D6.5 provides an updated standards landscape, examines the implications of standards for procurement and acceptance testing, and incorporates the findings of a broader second survey with 88 responses.

The final strategy focuses less on compiling a general list of standards and more on understanding how standards can facilitate trusted deployment. Attention is given to Artificial Intelligence governance, system interoperability, data exchange, performance testing, human oversight, cybersecurity and post-deployment monitoring.

D6.5 also changes the strategy's time perspective. D6.3 was primarily concerned with actions to be undertaken during the remaining project period. D6.5 is explicitly designed for the post-project phase. It identifies the work required to move from prototypes and project results towards operational products and services, including validation, commercial packaging, licensing, procurement preparation, reference deployments, training, standardisation and lifecycle support.

The evolution from D6.3 to D6.5 can therefore be understood as a transition from identification to prioritisation, from individual results to integrated solutions, from preliminary market assumptions to business cases, and from project-period planning to an actionable post-project roadmap.

1.4 RELATION TO STANDARDISATION

The standardisation component of D6.5 updates and extends the work initially undertaken in D6.3. It provides a final assessment of the standards environment relevant to the customs control of passenger baggage and identifies how standards can support the interoperability, trustworthiness, procurement readiness and long-term sustainability of BAG-INTEL results.

Standardisation is particularly important for BAG-INTEL because the project integrates technologies and processes originating from several different domains. Customs risk management, baggage scanning, CCTV, Artificial Intelligence, external data analysis, digital twin modelling, cybersecurity, and operational decision support are each governed by distinct technical practices, standards, and regulatory requirements. The challenge is therefore not merely to determine whether each component complies with a specific standard, but to establish how the combined system can be designed, tested, procured and operated within a coherent assurance framework.

The updated analysis presents a snapshot of the relevant standards and standardisation environment at the end of the project. It considers customs-specific instruments and guidance, including the World Customs Organization SAFE Framework, non-intrusive inspection guidance, customs data models and risk-management principles. It also examines equipment and safety standards relevant to X-ray and Computed Tomography systems, video-surveillance standards, Artificial Intelligence standards, information-security frameworks, privacy requirements and emerging European standardisation activities associated with the EU AI Act.

A central conclusion is that no single standard covers the entire BAG-INTEL operational environment. The applicable framework is layered. Equipment standards may address scanner safety or performance. Video-surveillance standards may address image quality and interoperability. AI standards may address risk management, lifecycle processes, governance and data quality. Customs instruments may address risk targeting, data exchange and operational procedures. Cybersecurity and privacy standards may address access control, security management and data protection.

The challenge for future deployment is to integrate these layers into a coherent system-level assurance approach. This is especially important because a technically compliant component may still pose operational or governance risks when integrated with other systems. For example, a scanner may meet equipment requirements, while the AI model interpreting the images lacks an appropriate monitoring or retraining framework. A CCTV system may provide adequate image quality but lack the metadata or interfaces required for luggage reidentification. A risk engine may operate effectively but lack sufficient explainability, logging or human oversight controls.

The second BAG-INTEL standards survey was designed to validate and extend the findings of the earlier D6.3 survey. The questionnaire was directed at relevant stakeholder communities and covered a broader range of standardisation issues, including priority areas, awareness and usage, perceived gaps, known initiatives, and future recommendations.

The survey received 88 responses from a diverse stakeholder community. Respondents included representatives of customs organisations, law-enforcement bodies, government agencies, technology providers, equipment manufacturers, service providers, consultants, research institutions, and European or international organisations. The volume and diversity of responses provide a credible indication of stakeholder priorities and concerns.

The survey findings show that interoperability and data sharing are among the most important needs for standardisation. International customs and law-enforcement data exchange received the highest level of priority, followed by detection and scanning technologies and risk assessment. These results reflect the fact that modern customs systems depend increasingly on information from different organisations, jurisdictions and technical platforms.

Artificial Intelligence emerged as the area where stakeholders perceive the largest standards gap. This finding is significant because AI is not a single component within BAG-INTEL. It is used for contraband detection, luggage reidentification, risk assessment and decision support. The lack of sufficiently

mature and sector-specific standards affects data quality, model validation, explainability, bias, human oversight, accountability, cybersecurity, retraining and post-deployment monitoring.

The evidence also suggests that operational technologies are more mature than governance technologies. Equipment such as scanners and CCTV systems already operate within established testing, safety and performance environments. By contrast, the standards needed to govern integrated AI-supported systems are still developing. This creates a gap between technical deployment and institutional assurance.

Stakeholders do not primarily call for the creation of numerous isolated new standards. Their responses favour harmonisation, practical interoperability, technology-neutral requirements and alignment between European and international approaches. They also emphasise the need for standards to support procurement, testing, certification and operational implementation.

The final standardisation analysis therefore identifies several priority areas. One is the development of customs-specific approaches for evaluating the performance of AI-assisted contraband detection. Existing equipment testing does not necessarily provide a complete framework for evaluating model accuracy, false-alarm behaviour, training-data quality, drift or performance across different concealment methods.

A second priority is the development of common interfaces and metadata structures connecting scanners, CCTV systems, risk engines, decision-support applications and customs case-management environments. The absence of common interfaces can increase integration costs, create vendor lock-in and limit the possibility of transferring solutions between airports or Member States.

A third priority concerns post-deployment governance. AI-supported customs systems require monitoring after installation. Performance may change due to new concealment practices, changes in passenger behaviour, different camera configurations, or shifts in the operational environment. Standards or guidance are needed for model drift, false positives, false negatives, officer overrides, alert fatigue, adversarial manipulation and retraining triggers.

A fourth priority concerns procurement and acceptance testing. Customs authorities need practical methods for translating standards into tender requirements, contractual obligations and measurable acceptance criteria. Laboratory performance should be distinguished from operational performance, and suppliers should be required to provide evidence concerning data, algorithms, cybersecurity, interfaces, updates, maintenance and human oversight.

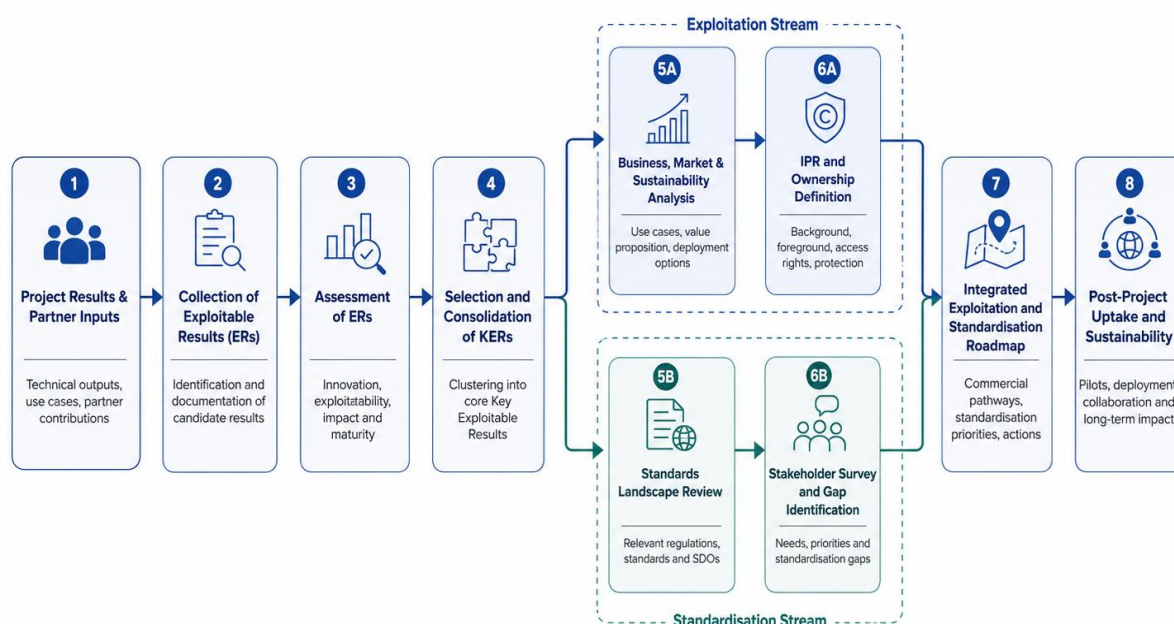
The recommendations arising from the standardisation work are intended to inform the European Commission, customs administrations, Standards Development Organisations, technology providers, system integrators, airport operators and future projects. BAG-INTEL cannot complete a formal European or international standardisation process within its project duration. It can, however, provide evidence, terminology, technical requirements, procurement recommendations and pre-standardisation material that may support later work.

The standardisation outputs should therefore be treated as a living resource. Artificial Intelligence, cybersecurity, data governance and interoperability standards continue to evolve. Future owners and deployment partners must reassess the applicable framework before each implementation and maintain compliance throughout the lifecycle of the deployed solution.

1.5 METHODOLOGY AND STRUCTURE OF THE DELIVERABLE

The methodology used for D6.5 combines quantitative and qualitative approaches. This mixed-method design was necessary because the exploitation potential of BAG-INTEL cannot be assessed through a single measure. Technology Readiness Level, partner scoring, market relevance, ownership, operational validation, standards and stakeholder acceptance must all be considered together.

Figure 1-1 - High-Level Workflow of the BAG-INTEL Exploitation and Standardisation Process



The work began with a review of the project's contractual and technical evidence. This included the Grant Agreement, the Description of the Action, the earlier D6.3 deliverable, technical and operational deliverables, partner input, testing evidence, stakeholder information and available Intellectual Property Rights documentation. The purpose of this review was to establish the intended functions of the system, the relationships between the components and the extent to which earlier exploitation assumptions remained valid.

The Exploitable Result inventory was then reviewed and consolidated. Each result was examined in relation to its owner and contributors, functional description, category, related tasks, Technology Readiness Level progression, strengths, weaknesses, opportunities, risks, target market, time to market, expected return and path to exploitation. This ensured that the assessment covered both technological and business dimensions.

A structured partner-scoring exercise was undertaken using three criteria: innovation, exploitability and impact. Innovation assessed the novelty and differentiation of the result. Exploitability assessed maturity, market potential, ownership clarity, integration readiness and the credibility of the path to use. Impact assessed the expected contribution to customs effectiveness, operational efficiency, passenger flow, resource allocation, traceability and security.

The criteria were equally weighted, and the final score for each result was calculated as the average of the three criterion-level averages. Blank entries were treated as non-responses. This was important because not every partner possessed sufficient expertise to evaluate every technical result.

The quantitative assessment was supplemented by qualitative interpretation. The final selection of Key Exploitable Results was not treated as a mechanical ranking exercise. The project develops an integrated system, and some results achieve their greatest value only when used together. The analysis therefore considered system dependencies, operational workflows, data requirements, deployment constraints and customer purchasing logic.

The result of this process was the consolidation of the project outputs into four Key Exploitable Result bundles. Each bundle was then described in terms of its component results, functional scope, value proposition, target users, exploitation pathway, dependencies and risks.

The next methodological stage involved the development of business cases. Each Key Exploitable Result was examined from the perspective of a potential adopting authority, buyer, user, service provider or commercial partner. The analysis considered the operational problem addressed, customer groups, delivery model, revenue streams, return on investment, procurement pathway and principal barriers.

The business-case analysis recognises that BAG-INTEL targets a predominantly public-sector market. The procurement of customs and security technologies is influenced by security requirements, public procurement procedures, budget cycles, national regulations, and the need for strong evidence of performance. The analysis therefore includes non-monetary value and places particular emphasis on pilot-to-production pathways.

The stakeholder methodology updated the earlier stakeholder mapping and more directly linked each group to the final Key Exploitable Results. Stakeholders were analysed according to their interest, influence, capacity to support deployment, role in validation and relevance to commercial, institutional or standardisation objectives.

The Intellectual Property Rights analysis reviewed the Background and Foreground Intellectual Property associated with the project. It consolidated information on ownership, joint ownership, access rights, restrictions, protection instruments, licensing and intended exploitation. The purpose was to create a final reference that can support post-project agreements.

The standardisation methodology combined desk research, a review of existing standards and guidance, an analysis of the BAG-INTEL architecture, and an interpretation of stakeholder evidence. It examined the standards relevant to customs operations, data exchange, non-intrusive inspection, baggage scanners, video surveillance, Artificial Intelligence, cybersecurity, data protection, procurement and acceptance testing.

The second standards survey used a structured questionnaire informed by the findings of D6.3. The responses were analysed quantitatively and qualitatively. Quantitative analysis included counts, rankings, stakeholder comparisons, priority indices and gap analysis. Qualitative analysis identified recurring themes in free-text recommendations.

The final stage consisted of synthesising the exploitation, business, stakeholder, Intellectual Property Rights and standardisation findings into a common roadmap. The synthesis identifies the most promising results, the conditions required for adoption, the agreements needed for joint exploitation, the outstanding validation requirements and the priorities for post-project action.

Following this introductory chapter, Chapter 2 presents the assessment of the Exploitable Results and the selection of the Key Exploitable Results. Chapter 3 describes the final Key Exploitable Result portfolio. Chapter 4 develops the corresponding business cases and joint business opportunities. Chapter 5 provides the stakeholder-engagement plan. Chapter 6 presents the final Intellectual Property Rights update. Chapter 7 analyses the standards and standardisation environment. Chapter 8 presents the second standards survey and the proposed post-project standards roadmap. Chapter 9 consolidates the conclusions and recommendations. The survey questionnaire is included in the annex.

2 ASSESSMENT OF EXPLOITABLE RESULTS AND IDENTIFICATION OF KEY EXPLOITABLE RESULTS (KERs)

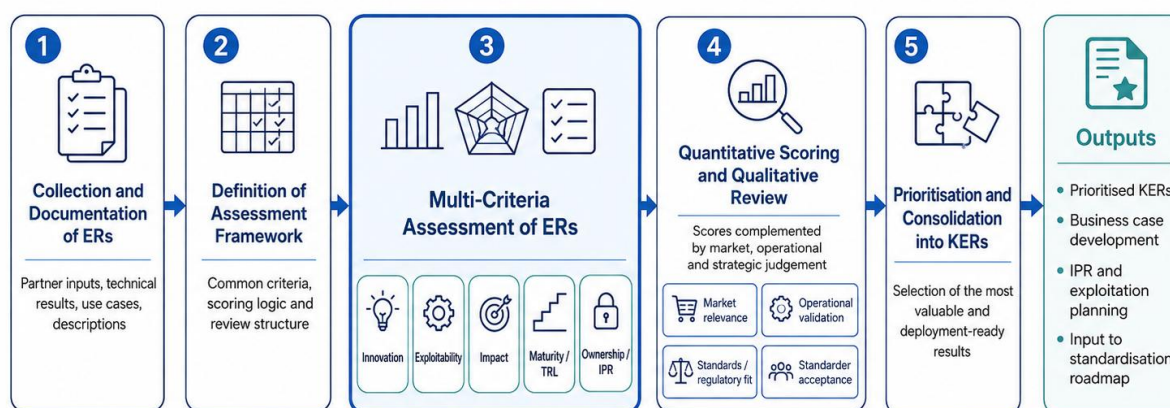
2.1 OVERVIEW OF THE KER ASSESSMENT PROCESS

The present section provides the final assessment of the BAG-INTEL Exploitable Results (ERs) and identifies the project's Key Exploitable Results (KERs). The analysis builds on the exploitation work already undertaken during the project and updates it, drawing on the structured partner assessment exercise, the maturity of the technical results, the exploitation information collected from ER owners and contributors, and the final consolidation of the results into coherent, exploitable bundles.

The BAG-INTEL project produces a broad portfolio of technological, methodological, operational and training-related outputs. These outputs are not isolated research artefacts, but elements of an integrated customs intelligence environment designed to improve the effectiveness and efficiency of customs control over passenger baggage arriving on international flights. The ER portfolio therefore includes AI-based contraband detection, AI-based luggage reidentification, digital twin-based customs management decision support, real-time risk and decision support, knowledge graph and data integration components, secure integration methods, operational methodologies, and training modules.

The KER assessment process was designed to determine which ERs have the highest strategic relevance for exploitation, market uptake, operational deployment, and sustainability after the project ends. The process followed four complementary steps.

Figure 2-1 - Overview of the Assessment of Exploitable Results methodology



First, the ER inventory was consolidated. Each ER was described by its name, category, owner, contributors, related tasks, Technology Readiness Level (TRL) progression, exploitation potential, strengths, weaknesses, opportunities, threats, targeted market, expected time to market, expected return on investment, and envisaged path to market. This ensured that all ERs were assessed not only as technical outputs, but also as potential exploitation assets.

Second, the consortium partners assessed the ERs using a common scoring framework. The framework asked partners to evaluate each ER against three criteria: innovation, exploitability and impact. These three dimensions were selected because they reflect the core Horizon Europe exploitation logic: the result must be sufficiently novel, sufficiently mature and exploitable, and sufficiently relevant to expected operational, societal and economic impacts.

Third, the quantitative assessment was complemented by qualitative interpretation. The final score for each ER was calculated as the average of the three criterion-level averages. However, the identification of final KERs was not treated as a purely mechanical ranking exercise. This is particularly important in BAG-INTEL, because the project delivers an integrated system of systems. Several ERs have their real exploitation value only when combined with complementary components. Conversely, some results with moderate individual scores are indispensable for operational deployment, interoperability, security, data access, or end-user acceptance.

Fourth, the ERs were consolidated into KER bundles. This final consolidation reflects BAG-INTEL's market and deployment logic more accurately than a simple list of individual results. Customs authorities, airport stakeholders and system integrators are unlikely to procure or deploy every component as a standalone research result. They are more likely to adopt coherent operational solutions that address concrete customs needs, risk assessment, real-time decision support, luggage reidentification and tracking, contraband detection, and integration and deployability. For this reason, the final KER structure is based on integrated bundles that combine high-scoring core ERs with necessary enabling or supporting ERs.

The final KER portfolio therefore distinguishes among high-priority ERs with strong quantitative performance, strategic ERs central to the BAG-INTEL operational concept, and enabling ERs that support integration, deployment, security, data interoperability, or operationalisation. This approach ensures that the KER selection remains both evidence-based and exploitation-oriented.

2.2 ASSESSMENT CRITERIA AND METHODOLOGY

The assessment methodology was centered on a partner-scoring exercise, using a 1-10 scale for each criterion—where 1 meant very low performance and 10 signified very high performance. Consortium partners assigned scores to the ERs, understanding that not all partners were expected to score every ER, especially if it was outside their technical, exploitation, or operational expertise. Cells left blank in the assessment matrix were considered non-responses or non-applicable and were not viewed as negative scores.

The three assessment criteria were defined as follows.

- **Innovation** assessed the degree to which the ER represents a novel or differentiated contribution compared with existing customs control, baggage screening, risk assessment, reidentification or digital twin solutions. This criterion considered technological novelty, methodological originality, AI-based advancement, integration of new data sources, improvement over current operational practice, and the ability of the ER to provide a distinctive position in relation to competing solutions.
- **Exploitability** assessed the practical and commercial potential of the ER. This included maturity, TRL progression, ownership clarity, integration readiness, compatibility with customs and airport operational contexts, expected time to market, potential exploitation model, market attractiveness, path to market, and the capacity of the owner or consortium to embed

the result into a product, service, methodology, training offer, consultancy package or broader BAG-INTEL deployment.

- **Impact** assessed the expected contribution of the ER to the objectives and impacts of BAG-INTEL. This included the potential to improve customs inspection targeting, increase contraband detection, reduce unnecessary inspections, support better allocation of customs resources, improve traveller flow, strengthen operational traceability, support risk-based decision-making, contribute to safer societies, and support customs authorities, airport stakeholders, and related security actors.

The final score for each ER was calculated as follows:

Final Score = (Average Innovation Score + Average Exploitability Score + Average Impact Score) / 3

All three criteria were assigned the same weight, which was suitable since BAG-INTEL exploitation depends on a balanced mix of technological innovation, deployability, and operational impact. A highly innovative result that lacks exploitability would need more development before qualifying as a priority KER. Likewise, a mature, easily exploitable result with limited innovation or project-level impact would not automatically qualify as a strategic KER.

For interpretation purposes, the ERs were grouped into three broad categories:

- **High-priority KER candidates:** ERs with final scores above 7.00. These results show strong combined performance and are considered particularly relevant for exploitation.
- **Strong strategic or supporting candidates:** ERs with final scores between 6.50 and 6.99. These results demonstrate clear relevance to exploitation, especially when integrated with other components.
- **Maturing, enabling or specialised results:** ERs with final scores below 6.50. These results may still be valuable, but generally require additional validation, integration, data access, operational refinement or market positioning before standalone exploitation.

This categorisation served as an analytical guide rather than a rigid threshold. The final KER selection also considered qualitative factors, including the ER's role in the BAG-INTEL architecture, dependencies between components, market bundling logic, data and regulatory constraints, expected end-user value, and the need to present deployable solutions rather than fragmented outputs.

2.3 ER ASSESSMENT RESULTS AND KER SELECTION

Before the quantitative assessment and ranking, the table below summarizes the twenty Exploitable Results included in the final evaluation. It provides a common reference point for understanding each result's scope and functional contribution, aiding in interpreting the ranking and KER consolidation that follow. The ER portfolio includes technological, methodological, operational, integration, and training outputs, which together form the core elements from which the final Key Exploitable Results were derived. Further details on ownership, Intellectual Property Rights, exploitation conditions, and the role of individual ERs within the final KER portfolio are available in later sections of this document.

Table 2-1 - Overview of BAG-INTEL Exploitable Results included in the final assessment

ER	Exploitable Result	Concise description
ER1	Multimethod Modelling	Modelling methodology underpinning the BAG-INTEL digital twins and supporting the simulation and analysis of customs operations.
ER2	Customs Management Decision Support System (CMDSS)	Digital twin-based decision-support capability for customs management, including operational analysis and what-if scenario evaluation.
ER3	Risk-based Decision Support for Customs in Selecting the Best Bags for Inspection	Supports customs officers in selecting baggage for inspection by combining bag-risk assessment and luggage reidentification information.
ER4	Connection Analysis-based Risk Assessment (ConnRisk)	Derives risk information from direct and indirect connections identified across available external data sources and databases.
ER5	Methodology for Operational BAG-INTEL (CustomsBagControl)	Provides the methodology for configuring, implementing and operating BAG-INTEL capabilities in real customs environments.
ER6	Customs Real-Time Decision Support System (CRDSS)	Provides AI-supported real-time decision support to customs officers during operational baggage-control activities.
ER7	Advanced Detection Systems	Provides advanced AI-assisted contraband-detection capabilities based on the analysis of baggage-scanning data.
ER8	Knowledge Graph Database and Intelligent Analysis	Integrates and analyses heterogeneous data through knowledge-graph technologies to support customs risk assessment and decision support.
ER9	Integrated Customs Information System	Provides an integrated environment for consolidating, managing and exchanging customs-related information required by BAG-INTEL services.
ER10	CCTV AI Detection Integrator	Integrates CCTV infrastructure with AI-based object-detection capabilities for automated monitoring within customs environments.

ER	Exploitable Result	Concise description
ER11	CI/CD Methodologies and Encryption Techniques for the Integrated BAG-INTEL System	Supports secure software integration, controlled deployment, continuous delivery and encryption of BAG-INTEL components.
ER12	Advanced Baggage Scanning System	Combines high-resolution baggage-scanning hardware with AI-assisted capabilities for enhanced contraband detection.
ER13	AI Tool for External Data-based Risk Assessment	Extracts risk indicators from external data sources and supports external-data-based baggage risk assessment.
ER14	Customs Bag-Risk Management	Supports the management of contraband risk at individual bag level and the prioritisation of baggage for inspection.
ER15	Training and Education Modules for Customs	Provides training and educational materials supporting the effective operational use of BAG-INTEL technologies and methodologies.
ER16	Optimal Probabilistic Bijective Mapping (OPBM)	Provides a probabilistic matching methodology to improve luggage reidentification under conditions of uncertainty.
ER17	Multi-Risk Indicators Statistical Weighting and Aggregation of Qualitative and Quantitative Data	Combines multiple qualitative and quantitative risk indicators into an aggregated risk measure supporting inspection decisions.
ER18	Providing CCTV for Object Detection	Provides deployment methodology and practical guidance for configuring CCTV systems to support AI-based object detection and luggage reidentification.
ER19	Secure-by-Design Scheme of the Architecture	Defines Secure-by-Design principles and architectural requirements supporting the secure development and integration of BAG-INTEL.
ER20	Luggage Reidentification	Provides the AI pipeline for luggage detection, characterisation, tracking and reidentification throughout the customs-control process.

The partner assessment offered a clear view of the BAG-INTEL ER portfolio. It highlights that the top-rated ERs are focused on the project's main technological strengths: AI-driven luggage reidentification, AI-powered baggage scanning and contraband detection, real-time customs decision support, and customs management via digital twin features.

The highest-scoring individual ER was ER3, Risk-based decision support for customs in selecting the best bags for inspection, with a final score of 7.94. This result achieved consistently high scores across innovation, exploitability and impact. Its strong performance reflects its strategic importance within the BAG-INTEL concept: it addresses the critical operational challenge of reidentifying suspicious baggage after scanning and enabling customs officers to intervene at the appropriate point in the passenger flow.

The second-highest scoring ER was ER12, Advanced Baggage Scanning System, with a final score of 7.61. This confirms the importance of AI-enhanced scanning and contraband detection for the project's exploitation potential. The result combines the established relevance of advanced scanning hardware with the added value of AI-based detection algorithms for customs applications.

The third highest-scoring ER was ER20, Luggage reidentification, with a final score of 7.56. This result is closely related to ER3 and strengthens the overall value proposition for luggage reidentification and tracking. It provides the core AI pipeline for luggage detection, characterisation, tracking and reidentification.

Other high-scoring results included ER6, Customs Real-time Decision Support System (CRDSS) with 7.29, ER7, Advanced Detection Systems with 7.26, ER2, Customs Management Decision Support System (CMDSS) with 7.19, ER16, Optimal Probabilistic Bijective Mapping (OPBM) with 7.17, and ER9, Integrated Customs Information System with 7.08. These scores indicate that the project's strongest exploitation assets are distributed across four functional layers: detection, reidentification, decision support, and integration.

The second group of ERs received strong but slightly lower scores. These include ER8, Knowledge Graph Database and Intelligent Analysis, with 6.95; ER5, Methodology for operational BAG-INTEL, including CustomsBagControl, with 6.83; ER10, CCTV AI Detection Integrator, with 6.76; ER1, Multimethod modelling, with 6.73; ER4, Connection analysis-based risk assessment (ConnRisk), with 6.73; and ER14, Customs bag risk management, with 6.70. These ERs are highly relevant for exploitation, particularly as part of broader operational bundles. Their value does not always lie in standalone commercialisation, but in their contribution to integrated deployment, risk intelligence, operational configuration, and decision support.

The remaining ERs received moderate scores, but several still play important enabling roles. ER11, CI/CD methodologies and encryption techniques for the integrated BAG-INTEL system, scored 6.46 and is important for secure and maintainable deployment. ER13, an AI tool for external data-based risk assessment, scored 6.31 and is a relevant risk intelligence component, although it depends strongly on data availability and training. ER17, Multi Risk Indicators Statistical Weighting and Aggregation of Qualitative and Quantitative Data, scored 5.81 but remains relevant as a methodological component for constructing global risk indicators. ER18, Providing CCTV for Object Detection, scored 5.37 but provides practical deployment knowledge that supports AI-based reidentification in real airport environments. ER15, Training and Education Modules for Customs, and ER19, Secure by Design scheme of the architecture, are also relevant project outputs, although their final scores indicate that they are better treated as supporting or sustainability-oriented outputs rather than primary market-facing KERs.

The table below summarises the quantitative assessment:

Table 2-2 - Quantitative assessment of ERs

Rank	ER	ER name	Innovation	Exploitability	Impact	Final score	Assessment interpretation
1	ER3	Risk-based decision support for customs in selecting the best bags for inspection	8.0	7.9	7.9	7.94	Core KER candidate
2	ER12	Advanced Baggage Scanning System	7.1	8.1	7.6	7.61	Core KER candidate
3	ER20	Luggage reidentification	7.7	7.7	7.3	7.56	Core KER candidate
4	ER6	Customs Real-time Decision Support System (CRDSS)	7.7	7.1	7.1	7.29	High-priority KER component
5	ER7	Advanced Detection Systems	6.9	7.6	7.3	7.26	High-priority KER component
6	ER2	Customs Management Decision Support System (CMDSS)	7.3	7.1	7.1	7.19	High-priority KER component
7	ER16	Optimal Probabilistic Bijective Mapping (OPBM)	7.25	7.5	6.75	7.17	High-priority KER component
8	ER9	Integrated Customs Information System	7.3	7.0	7.0	7.08	High-priority integration component
9	ER8	Knowledge Graph Database and Intelligent Analysis	6.4	7.1	7.3	6.95	Strong supporting KER component
10	ER5	Methodology for operational BAG-INTEL (CustomsBagControl)	6.3	6.5	7.7	6.83	Strong operationalisation component
11	ER10	CCTV AI Detection Integrator	6.4	7.1	6.8	6.76	Strong supporting component

Rank	ER	ER name	Innovation	Exploitability	Impact	Final score	Assessment interpretation
12	ER1	Multimethod modelling	5.4	7.8	7.0	6.73	Exploitable output, mainly digital twin-related
13	ER4	Connection analysis-based risk assessment (ConnRisk)	7.2	6.5	6.5	6.73	Strategic risk assessment component
14	ER14	Customs bag risk management	6.6	7.2	6.3	6.70	Strategic risk management component
15	ER11	CI/CD methodologies and encryption techniques	5.1	7.0	7.3	6.46	Secure deployment enabler
16	ER13	AI tool for external data-based risk assessment	5.6	6.8	6.5	6.31	Risk intelligence component requiring data maturity
17	ER19	Secure by Design scheme of the architecture	4.2	6.0	7.4	5.87	Architecture and standardisation support output
18	ER17	Multi Risk Indicators Statistical Weighting and Aggregation	5.0	6.1	6.3	5.81	Methodological support component
19	ER15	Training and Education Modules for Customs	4.2	6.2	7.0	5.80	Training and uptake support output
20	ER18	Providing CCTV for Object Detection	5.1	6.1	4.9	5.37	Deployment knowledge and CCTV configuration enabler

The ranking confirms that the project's final KERs should not be presented as a disconnected set of individual technical outputs. The strongest exploitation proposition arises from integrating complementary ERs into deployable bundles. This is particularly evident in the following cases.

First, ER3, ER20 and ER16 form a coherent AI-based reidentification chain. ER3 represents the customs-focused reidentification use case, ER20 provides the broader AI reidentification pipeline, and ER16 contributes probabilistic optimisation under uncertainty. ER10 and ER18, although not among the

highest-scoring individual ERs, support practical deployment by addressing CCTV AI integration and camera configuration requirements.

Second, ER7 and ER12 together form a coherent contraband-detection proposition. ER7 represents the advanced detection algorithmic capability, while ER12 represents the advanced scanning system that integrates high-resolution scanning and AI. Their joint value exceeds their individual value because customs adoption depends on the combined availability of scanning infrastructure, detection algorithms, operational accuracy, and integration with the wider BAG-INTEL workflow.

Third, ER6, ER14, ER13, ER17, ER5, and ER4 form a risk and decision-support suite. ER6 provides real-time customs decision support; ER14 manages contraband risk at the bag level; ER13 extracts risk indicators from external data; ER17 provides statistical weighting and aggregation; ER4 provides connection-analysis-based risk assessment; and ER5 provides the operational methodology for configuring and running BAG-INTEL solutions. This suite directly addresses the operational logic of customs decision-making: selecting which bags to inspect and using multiple sources of risk evidence, while supporting traceable, explainable, and operationally usable decisions.

Fourth, ER2, ER8, ER9 and ER11 provide integration and deployability capabilities. ER2 provides management-level decision support through digital twin-based scenario analysis. ER8 provides a knowledge graph and support for intelligent analysis. ER9 addresses the need for a unified customs information system. ER11 supports secure integration, CI/CD and encryption. Even where some of these components are not treated as standalone KERs, they are essential to system-level deployment, scalability, security and long-term maintainability.

Based on this, the final KER selection was determined using a bundling approach that considers both quantitative scores and the system's potential for exploitation. The resulting KER bundles are shown in the next section.

3 KER DESCRIPTIONS

3.1 INTRODUCTION TO THE KER PORTFOLIO

After evaluating the BAG-INTEL Exploitable Results and identifying the project's Key Exploitable Results, this section offers a clear overview of the final KER portfolio. It details each KER's functions, reasons for exploitation, ownership, intended users, deployment opportunities, and sustainability importance.

The final KER portfolio is not merely a collection of technical outputs but is organised into coherent exploitation bundles. These bundles illustrate how customs authorities, airport stakeholders, border control system integrators, and security technology providers are expected to utilize BAG-INTEL results. This approach is especially suitable for BAG-INTEL, which aims to develop an integrated solution to enhance the effectiveness and efficiency of passenger baggage control at inland border airports. The value of the project's exploitation lies in the seamless connection of scanning, detection, reidentification, risk assessment, decision support, digital twin modeling, secure integration, and operational deployment.

The four final KERs are the following:

KER	Title	Core function
KER A	Customs Bag Risk Assessment and Real-Time Decision Support Suite	Risk-based customs inspection decision support
KER B	AI-Based Luggage Reidentification and Tracking System	Non-intrusive reidentification and tracking of luggage selected for inspection
KER C	Advanced Contraband Detection System	AI-enhanced detection of contraband in passenger baggage
KER D	Integrated Digital Twin, Knowledge and Secure Deployment Layer	System integration, digital twin management support, knowledge representation and secure deployment

These KERs collectively define BAG-INTEL's integrated exploitation approach. KER A helps customs decide which bags to inspect. KER B enhances the ability to reidentify selected bags within the customs area. KER C improves contraband detection in scanned baggage. KER D supports integration, simulation, knowledge management, and secure deployment, enabling the system to function effectively in real-world customs and airport settings.

3.2 KER A: CUSTOMS BAG RISK ASSESSMENT AND REAL-TIME DECISION SUPPORT SUITE

3.2.1 General Description

The Customs Bag Risk Assessment and Real-Time Decision Support Suite is a composite KER that supports customs authorities in making targeted, transparent, and operationally efficient decisions on intrusive baggage inspections. It consolidates project results on risk indicator extraction, connection analysis, risk aggregation, bag-level risk management, real-time decision support, and operational visualisation.

This KER responds to a central challenge in modern customs control: identifying suspicious luggage accurately and efficiently in a high-volume passenger environment, without increasing the mobilisation of customs personnel or causing unnecessary delays to compliant travellers. In this context, KER A provides customs officers and operational control units with a structured decision support environment that combines multiple sources of risk evidence and translates them into actionable inspection guidance.

3.2.2 Component ERs

Component ER	Title	Owner(s)	Role within KER A
ER6	Customs Real Time Decision Support System (CRDSS)	LTA	Provides AI based real time decision support for customs operations
ER14	Customs bag risk management	LTA	Manages the risk of contraband at bag level
ER13	AI tool for external data-based risk assessment	EXUS, UGR	Extracts and assesses external data-based risk indicators
ER17	Multi Risk Indicators Statistical Weighting and Aggregation of Qualitative and Quantitative Data	INSA	Supports the construction of global risk indicators
ER5	Methodology for operational BAG-INTEL, including CustomsBagControl	LTA	Provides the methodology for configuring and operating BAG-INTEL solutions
ER4	Connection analysis-based risk assessment (ConnRisk)	LTA	Derives risk from suspicious direct and indirect connections across available databases

3.2.3 Functional Scope

KER A provides multi-layered decision support. At the analytical layer, it supports extracting risk indicators from external sources, including passenger, travel, customs, and other relevant datasets, where lawful access is available. At the connection analysis layer, it identifies suspicious links and indirect associations that may increase the likelihood that a bag is suitable for inspection. At the risk aggregation layer, it supports the statistical weighting and combination of qualitative and quantitative indicators into a more consolidated risk picture. At the operational layer, it provides real-time decision support and visualisation for customs officers.

The suite aims to improve the traceability and consistency of inspection decisions. Rather than relying solely on manual judgement or isolated risk signals, customs authorities can use a structured decision-support process that records relevant indicators, presents the combined risk logic, and supports a defensible inspection recommendation. This is particularly important in regulated public-authority environments, where decisions must be proportionate, auditable, and aligned with operational policy.

3.2.4 Value Proposition

The main value proposition of KER A is rationalising customs inspection decision-making. KER A enables customs authorities to target intrusive inspections on bags with higher-risk indicators, while reducing unnecessary checks on low-risk passengers and baggage. It supports better use of limited human resources and improves the operational balance between security effectiveness and passenger flow.

The KER offers these specific benefits:

Value dimension	Contribution of KER A
Operational efficiency	Supports prioritisation of suspicious baggage and better allocation of customs resources
Decision quality	Combines multiple indicators into a structured, repeatable and explainable decision support process
Traceability	Enables more transparent reasoning behind inspection recommendations
Risk intelligence	Incorporates external data-based indicators and connection analysis where legally and operationally feasible
Scalability	Can be configured for different airport sizes, customs workflows and operational requirements
Sustainability	Can be maintained as a modular risk and decision support suite within broader BAG-INTEL deployments

3.2.5 Target Users and Market Segments

The main target users include national customs authorities and airport customs units responsible for passenger baggage screening at inland border airports. Additionally, the KER is applicable to airport-based customs management teams, border control system integrators, airport IT stakeholders, and security solution providers collaborating with public authorities.

In adjacent contexts, selected components of the KER may also be relevant to law enforcement agencies for investigative analysis, particularly the connection analysis capability, provided legal, ethical, and data-access requirements are met. However, for customs use, the most realistic exploitation pathway is not selling each component as a separate tool but deploying the suite as part of an integrated BAG-INTEL-style customs control solution.

3.2.6 Exploitation Pathway

KER A is suitable for exploitation through a combination of software licensing, solution bundling, customisation, integration services, maintenance and operational support. Given the public-authority nature of the target market, direct business-to-government procurement, framework agreements, pilot-to-production pathways, and system integrator-led deployment are likely to be the most relevant channels.

The exploitation pathway should emphasise operational validation, alignment with national customs rules, data governance arrangements, integration with existing customs and airport systems, and training for operational users. In practice, deploying KER A will require site-specific adaptation, including defining relevant data sources, risk thresholds, user roles, visualisation requirements, escalation workflows, and audit procedures.

3.2.7 Key Risks and Dependencies

The effectiveness of KER A heavily relies on the availability, quality, and lawful use of relevant data. Its performance can be limited if customs authorities cannot access certain external data sources or if data sharing with other authorities is restricted. Additional risks involve data protection, cybersecurity, interoperability with legacy systems, user acceptance, and the importance of not overdependence on automated recommendations.

The principal mitigation measures include privacy and security by design, strict role-based access control, human-in-the-loop decision-making, clear operational protocols, explainability of risk indicators, phased validation with customs users, and continuous performance monitoring.

3.3 KER B: AI-BASED LUGGAGE REIDENTIFICATION AND TRACKING SYSTEM

3.3.1 General Description

The AI-based Luggage Reidentification and Tracking System is one of BAG-INTEL's most distinctive KERs. It addresses the operational challenge of reidentifying luggage selected for inspection during scanning that later appears in the customs area, either carried by the passenger or moved within the baggage flow. This challenge is particularly difficult because the bag may be viewed from different camera angles, in crowded environments, on trolleys, near other luggage, or under varying lighting and acquisition conditions.

KER B provides a non-intrusive, AI-based approach to luggage reidentification. It aims to help customs authorities track and reidentify suspicious luggage without physical tags, visible marks, or manual labels. This is highly relevant because visible marking could alert smugglers, create operational delays, require additional personnel, and introduce environmental or logistical burdens.

3.3.2 Component ERs

Component ER	Title	Owner(s)	Role within KER B
ER20	Luggage reidentification	CEA	Provides the AI pipeline for luggage detection, characterisation, tracking and reidentification
ER3	Risk-based decision support for customs in selecting the best bags for inspection.	LTA	Decision support for customs in selecting the best bags for inspection based on the overall bag risk assessment (including scanning results) and the reidentification results
ER16	Optimal Probabilistic Bijective Mapping (OPBM)	INSA	Optimises reidentification under uncertainty through probabilistic matching
ER10	CCTV AI Detection Integrator	CEA, PSI	Integrates CCTV technology with AI object detection modules
ER18	Providing CCTV for Object Detection	PSI	Provides practical deployment knowledge for CCTV configuration in customs zones

3.3.3 Functional Scope

KER B encompasses the entire reidentification process. It starts with image acquisition and luggage detection, then moves to luggage characterisation and feature extraction. The process continues with tracking and matching, ending with an alert or decision-support output that signals when a bag seen in the customs area matches one previously chosen for inspection.

The KER includes both algorithmic and deployment-oriented components. The algorithmic components focus on detection, characterisation, reidentification and probabilistic optimisation. The deployment components address the integration of CCTV infrastructure, camera placement, data pipeline configuration and adaptation to airport-specific conditions.

Including OPBM is particularly important because reidentification is not deterministic in real environments. Matching scores may be uncertain and affected by occlusion, perspective, lighting, luggage similarity and partial visibility. Probabilistic optimisation can therefore strengthen the robustness of the matching logic and support more reliable reidentification outcomes.

3.3.4 Value Proposition

The main value proposition of KER B is a non-intrusive, AI-based, and operationally actionable luggage reidentification capability. It enables customs authorities to maintain continuity between the scanning decision and the physical inspection stage. Without such a capability, a bag identified as suspicious during scanning may be difficult to locate once it enters the passenger and carousel environment.

KER B therefore contributes directly to the effectiveness of BAG-INTEL as an operational customs solution. It ensures that the intelligence generated during scanning and risk assessment can be converted into an actual intervention by customs officers.

Value dimension	Contribution of KER B
Non-intrusive control	Avoids visible tagging or physical marking of suspicious luggage
Operational continuity	Links scanning stage, carousel area and customs exit area
Resource efficiency	Reduces manual tracking requirements and supports targeted interventions
Security	Prevents passengers from knowing that their luggage has been selected for inspection
Passenger flow	Maintains baggage movement without introducing additional physical handling steps
Differentiation	Provides a distinctive capability compared with conventional baggage control approaches

3.3.5 Target Users and Market Segments

The primary target users are customs authorities operating at airports, especially customs units responsible for passenger baggage control in inbound international arrivals. The KER is also relevant to airport operators, airport security departments, and system integrators involved in deploying AI video analytics, baggage flow monitoring, or smart airport security systems.

The broader market may include organisations that require luggage tracking and reidentification capabilities beyond customs, provided that the application context is lawful, proportionate, and compatible with data protection requirements.

3.3.6 Exploitation Pathway

KER B can be exploited through software licensing, AI-as-a-service models, technology transfer, integration services, maintenance and support contracts, and partnerships with airport security technology providers or system integrators. Given the need for site-specific adaptation, professional services will be a major component of the exploitation pathway. These services may include airport surveys, CCTV placement analysis, integration with existing video systems, model calibration, validation against operational scenarios, staff training, and periodic performance tuning.

A realistic go-to-market route would begin with pilot-to-production deployments in selected airport environments, followed by reference installations and integration into broader customs modernisation or airport security programmes. The KER may also be bundled with KER A and KER C, as reidentification is most valuable when integrated with risk-based selection and contraband detection.

3.3.7 Key Risks and Dependencies

The main technical risk concerns re-identification accuracy under real-world operational conditions. Crowded environments, stacked luggage, variable lighting, occlusion, different camera angles and passenger handling behaviours may affect model performance. Data availability and annotation are also critical. Sufficient representative image data is required to train, test and continuously improve the models.

Further dependencies relate to CCTV infrastructure, cybersecurity, data protection and operational acceptance. Since the KER involves video analytics in sensitive airport environments, deployment must be supported by a clear legal basis, data minimisation, access control, retention rules and human oversight.

Mitigation measures include phased validation, realistic data collection, CCTV configuration guidelines, continuous monitoring of false positives and false negatives, privacy by design, and operational protocols defining how customs officers should act on reidentification alerts.

3.4 KER C: ADVANCED CONTRABAND DETECTION SYSTEM

3.4.1 General Description

The Advanced Contraband Detection System consolidates the scanning and AI-based detection outputs of BAG-INTEL. It improves contraband detection in passenger baggage by combining high-resolution scanning technology with AI-based detection algorithms.

This KER addresses a core customs control function: identifying luggage that may contain illegal or undeclared goods and should therefore be selected for further inspection. It contributes directly to the project's objective of increasing customs effectiveness while maintaining efficient passenger flow.

3.4.2 Component ERs

Component ER	Title	Owner(s)	Role within KER C
ER7	Advanced Detection Systems	SDE	Provides high precision contraband detection technology and detection algorithms
ER12	Advanced Baggage Scanning System	SDE	Provides high resolution scanning with integrated AI for contraband detection

3.4.3 Functional Scope

KER C integrates scanning hardware, image analysis, and AI-driven contraband detection. The scanner produces high-resolution data on baggage contents, while the detection system employs AI and analytical techniques to spot suspicious materials, objects, or patterns that could suggest contraband.

The KER is particularly relevant for customs applications because customs screening differs from conventional aviation security screening. While aviation security focuses primarily on threats to flight safety, customs control must identify a wider set of prohibited, restricted or undeclared goods. BAG-INTEL therefore positions this KER in relation to inbound passenger baggage and customs inspection decisions.

KER C's output extends beyond just the detection event. The detection results are designed to integrate into the wider BAG-INTEL risk assessment and decision-making workflow. Accordingly, KER C works closely with KER A and KER B. It detects suspicious baggage; KER A provides the decision logic for inspection prioritization; and KER B assists with reidentification when the luggage arrives at customs.

3.4.4 Value Proposition

The main value proposition of KER C is improved detection accuracy and operational targeting in customs baggage control. By combining advanced scanning with AI-based detection, KER C can help customs authorities identify higher-risk luggage more effectively than manual inspection alone.

Value dimension	Contribution of KER C
Detection effectiveness	Supports improved identification of contraband in passenger baggage
Customs targeting	Provides detection indicators that feed risk-based inspection decisions
Throughput support	Enables screening without necessarily increasing manual inspection workload
Product portfolio potential	Can extend the detection capabilities of the technology owner's product offering

Value dimension	Contribution of KER C
Integration value	Provides core detection input for the wider BAG-INTEL system
Market relevance	Addresses customs, airports, border security and public security stakeholders

3.4.5 Target Users and Market Segments

The primary target markets are customs administrations, airport customs units, border security organisations and airport operators involved in customs-related screening infrastructure. Additional market relevance may exist for police, border management authorities, and security organisations that require high-precision contraband detection.

The KER is particularly attractive where customs authorities seek to modernise inbound baggage screening and move towards more automated, intelligence-led, and AI-supported control models.

3.4.6 Exploitation Pathway

The exploitation pathway for KER C is closely aligned with the owner's product portfolio and commercial strategy. The most realistic route is to integrate new detection algorithms and customs-oriented AI capabilities into existing or future scanning products and services. This may include software upgrades, scanner-based product extensions, deployment packages for custom use cases, and support and maintenance agreements.

The KER may be marketed as part of a broader BAG-INTEL solution or as an advanced detection capability for customs agencies seeking to improve scanning performance. Its deployment will depend on the availability of appropriate training data, validation against relevant contraband types, tuning of detection thresholds and operational acceptance by customs personnel.

3.4.7 Key Risks and Dependencies

The main risks include implementation costs, the availability of training data, detection performance for small quantities or low-purity materials, false-alarm rate management, and the need for continuous retraining as contraband concealment methods evolve. There may also be competition from other computed tomography, X-ray diffraction, and adjacent detection technologies.

Mitigation requires sustained access to representative data, continuous algorithm improvement, validation in customs-relevant scenarios, a careful balance between detection probability and false alarm rate, and strong integration with the broader BAG-INTEL decision-support process.

3.5 KER D: INTEGRATED DIGITAL TWIN, KNOWLEDGE AND SECURE DEPLOYMENT LAYER

3.5.1 General Description

The Integrated Digital Twin, Knowledge, and Secure Deployment Layer is a foundational KER that underpins the operational deployment, interoperability, and sustainability of the BAG-INTEL system. It is not tied to a specific function, such as scanning or reidentification. Instead, it provides the digital twin, knowledge management, data integration, and secure deployment features needed to turn individual components into a comprehensive, deployable customs solution.

This KER is essential because public-sector customs environments are complex, security-sensitive, and operationally heterogeneous. A technically promising AI component cannot be exploited effectively unless it can be integrated with existing systems, deployed securely, maintained over time, connected to relevant data flows and adapted to the specific layout and operational requirements of each airport.

3.5.2 Component ERs

Component ER	Title	Owner(s)	Role within KER D
ER9	Integrated Customs Information System	LTA	Provides a unified platform for customs data integration
ER2	Customs Management Decision Support System (CMDSS)	STAM	Provides digital twin-based customs management decision support and scenario analysis
ER8	Knowledge Graph Database and Intelligent Analysis	UGR	Supports advanced data models for decision support and risk assessment
ER11	CI/CD methodologies and encryption techniques for the integrated BAG-INTEL system	INTRA	Supports secure integration, deployment, continuous delivery and encryption

3.5.3 Functional Scope

KER D combines four complementary functions:

- It supports data integration through a unified customs information environment. This is necessary for connecting scanning outputs, risk indicators, baggage identifiers, external data sources, decision-support modules, and operational interfaces.
- It supports digital twin-based management decision support. The Customs Management Decision Support System enables airport and customs stakeholders to simulate operational

scenarios, assess resource allocation options, examine passenger and baggage flows, and evaluate different configurations before or during deployment.

- It supports knowledge representation and intelligent analysis through knowledge graph-based methods. This strengthens the system's ability to represent relationships between data entities, risk concepts, customs knowledge and operational events.
- It supports secure and maintainable deployment through CI/CD methodologies and encryption techniques. This is particularly important for a multi-component system operating in sensitive customs and airport environments where security, continuity, maintainability and controlled updates are essential.

3.5.4 Value Proposition

The main value proposition of KER D is deployability. It provides the enabling architecture and operational intelligence required for BAG-INTEL to function as an integrated system rather than as a collection of separate modules.

Value dimension	Contribution of KER D
Integration	Connects the different BAG-INTEL components and data flows
Operational optimisation	Uses digital twin modelling to support airport-specific configuration and resource planning
Knowledge management	Structures customs and risk-related information for analysis and decision support
Security	Supports encrypted integration and secure deployment practices
Maintainability	Enables continuous integration, controlled updates and long-term technical support
Scalability	Supports adaptation to different airports, customs contexts and system architectures

3.5.5 Target Users and Market Segments

The primary users of KER D are customs management teams, airport operators, airport IT departments, system integrators and technology providers responsible for deploying, integrating and maintaining customs control solutions. While customs officers may use some outputs indirectly, the main users are those responsible for system configuration, operational planning, data integration, and technical governance.

The KER is also relevant to public procurement authorities and programme managers responsible for customs modernisation, because it provides a framework for implementing BAG-INTEL capabilities in a controlled, scalable and secure manner.

3.5.6 Exploitation Pathway

KER D can be monetised through licensing, integration services, digital twin consulting, deployment engineering, DevSecOps support, data modelling services, and maintenance and support agreements. The digital twin component may also be offered as a specialised decision-support tool for airport process optimisation, while the secure deployment and CI/CD components may be positioned as part of a broader secure integration service.

The exploitation pathway is likely to be strongly service-based. Each airport has different layouts, legacy systems, operational procedures, data access conditions and security requirements. Therefore, KER D will require significant customisation and co-design with the adopting authority or system integrator.

3.5.7 Key Risks and Dependencies

The main risks are integration complexity, dependence on legacy systems, differences across national customs environments, data protection requirements, cybersecurity expectations, and public-sector procurement constraints. Customers may also underestimate the value of integration layers if they focus only on visible front-end capabilities such as scanning or reidentification.

Mitigation requires clearly articulating KER D as the deployment backbone of BAG-INTEL, early involvement of airport IT and customs system owners, a modular architecture, open interfaces where feasible, cybersecurity controls, documentation, operational testing, and long-term maintenance planning.

3.6 INTERDEPENDENCIES ACROSS THE KERS

The four KERs work together to strengthen each other. KER C identifies suspicious content in scanned baggage. KER A uses detection results, along with external data and risk indicators, to support inspection decisions. KER B allows customs officers to identify specific luggage as it arrives in the customs area. KER D offers the digital twin, knowledge management, integration, and secure deployment layers that support the operation of the other KERs in real airport environments.

This interdependency is central to the BAG-INTEL exploitation strategy. The project's value is not limited to one technological module. It lies in the ability to connect detection, risk intelligence, decision support and reidentification into a coherent operational workflow for customs authorities.

The table below summarises the functional relationship among the KERs.

Operational need	Relevant KER	Contribution
Identify suspicious content in baggage	KER C	AI-enhanced scanning and contraband detection
Decide whether a bag should be inspected	KER A	Risk aggregation and real-time decision support

Operational need	Relevant KER	Contribution
Locate the selected bag at the customs area	KER B	AI-based luggage reidentification and tracking
Configure and deploy the system securely	KER D	Digital twin, knowledge management, integration and secure deployment
Support long-term uptake and sustainability	All KERs	Combined commercialisation, operational validation, training, support and maintenance

3.7 OVERALL EXPLOITATION SIGNIFICANCE OF THE KER PORTFOLIO

The KER portfolio positions BAG-INTEL as an integrated customs innovation framework rather than a single technology product. The portfolio addresses the full operational chain for inbound passenger baggage customs control: scanning, detection, risk analysis, decision support, reidentification, system integration and operational optimisation.

The main significance of the portfolio's exploitation lies in five areas:

- It supports more effective customs targeting by enabling officers to focus on luggage with stronger risk indications.
- It improves operational efficiency by reducing reliance on random checks and manual tracking of suspicious luggage.
- It offers a non-intrusive reidentification pathway that avoids physical marking and supports passenger flow.
- It provides a modular basis for integration into diverse airport and customs environments.
- It creates multiple exploitation pathways, including product integration, software licensing, AI as a service, consultancy, customisation, maintenance, training and system integration.

The portfolio also has strong institutional relevance. Customs authorities operate within legal, ethical, security and public accountability constraints. Therefore, BAG-INTEL KERs must be applied through models that preserve human oversight, comply with data protection and security requirements, provide traceable decision logic, and support gradual adoption through pilots, validation and operational training.

4 KERS AS BUSINESS CASES

4.1 BUSINESS CASE FRAMEWORK AND APPROACH

This section translates the BAG-INTEL Key Exploitable Results into actionable business cases. It aims to show how each result can be positioned, implemented, commercialised, and sustained beyond the project. The analysis uses the Business Model Canvas framework previously applied to the KER bundles, adapting it to a more investment-focused format to produce the final exploitation roadmap.

The business case framework is based on five analytical dimensions:

- The **value proposition** outlines the operational, institutional and commercial value the KER offers to customs authorities, airport operators, security stakeholders and system integrators. In the BAG-INTEL context, value extends beyond financial returns. It includes improved customs targeting, better use of human resources, greater traceability of inspection decisions, reduced unnecessary passenger disruption, enhanced contraband detection, improved luggage reidentification and stronger operational readiness.
- The **target market and customers** identify the primary buyers, end users, beneficiaries and adjacent market segments. For BAG-INTEL, the main institutional market comprises national and regional customs administrations, airport customs units, airport operators, airport IT departments, and stakeholders in border control and airport security. System integrators represent an important commercial channel because they can embed BAG-INTEL components within broader airport security, border management and digital transformation programmes.
- The **revenue model and Return on Investment (ROI) projections** describe the most plausible monetisation routes. BAG-INTEL does not rely on a single revenue model. Depending on the KER, revenue may be derived from software licensing, site-based platform licences, hardware sales, algorithm licences, subscriptions, AI-as-a-Service, integration services, customisation, consultancy, training, maintenance, updates, model retraining, DevSecOps support, and long-term managed services. ROI should be understood in both monetary and non-monetary terms, since public authorities assess investment not only through revenue or cost recovery, but also through security, operational efficiency, reduced manual workload, improved inspection success rates and public safety outcomes.
- The **deployment and delivery model** addresses how each KER can be implemented in real airport and customs environments. BAG-INTEL supports both on-premises deployment, which authorities often prefer due to security, sovereignty, and legal constraints, and off-premises or as-a-service models, where allowed by national rules and data governance requirements. In practice, the deployment model is expected to be case-specific. Sensitive data, law enforcement constraints and airport security requirements will often favour on-premises or hybrid deployment.
- The **risks and mitigation measures** identify the main barriers to commercialisation and adoption. These include data access constraints, legal and regulatory limitations, integration complexity, procurement constraints, cybersecurity requirements, AI performance under operational conditions, false alarm management, reidentification accuracy, user acceptance, partner role allocation and the need for sustained support and maintenance.

The business case framework also accommodates BAG-INTEL's multi-partner exploitation structure. The commercialisation of a KER may involve distinct roles: the Owner, who has developed and owns the relevant component or methodology; the Service Provider, who delivers deployment, integration, customisation, training, hosting, support or maintenance services; and the Seller or Business Champion, who leads marketing, procurement engagement, sales transactions and revenue distribution among the relevant partners. This separation of roles is particularly important because the BAG-INTEL KERs are composite bundles rather than single-owner standalone products.

The four business cases developed below correspond to the four final KER bundles:

KER	Business case title	Core exploitation logic
KER 1	Customs Bag-Risk Assessment and Real-Time Decision Support Suite	Software and service-based customs risk and decision support solution
KER 2	AI-Based Luggage Reidentification and Tracking System	AI vision-based reidentification and CCTV integration solution
KER 3	Advanced Contraband Detection System	Hardware, software and algorithm-based contraband detection solution
KER 4	Integrated Digital Twin, Knowledge and Secure Deployment Layer	Platform, digital twin, knowledge graph and secure deployment backbone

Business cases should be treated as final roadmap-level exploitation cases. They provide a structured basis for post-project commercialisation, but precise pricing, revenue-sharing arrangements, licensing terms and contractual configurations will need to be finalised through partner-level exploitation agreements, procurement discussions and follow-on validation with end users.

4.2 BUSINESS CASE: KER 1 – CUSTOMS BAG-RISK ASSESSMENT AND REAL-TIME DECISION SUPPORT SUITE

4.2.1 Value Proposition

KER 1 consolidates the BAG-INTEL risk engine and real-time customs decision-support capabilities. It brings together the following ERs: ER6 Customs Real-Time Decision Support System (CRDSS), ER14 Customs Bag-Risk Management, ER13 AI tool for external-data-based risk assessment, ER17 Multi-Risk Indicators Statistical Weighting and Aggregation, ER5 CustomsBagControl methodology, and ER4 ConnRisk.

The business case for KER 1 is grounded in a clear operational need: customs authorities must identify which bags to inspect in environments characterised by high passenger volumes, limited human resources, short decision windows, and increasingly complex smuggling patterns. KER 1 addresses this need by transforming fragmented risk signals into a structured, transparent, and operationally actionable decision-support process.

The value proposition consists of the following interrelated elements:

- KER 1 improves the **rationalisation of intrusive inspection decisions**. It supports a more transparent, traceable and justifiable decision-making process by combining external data indicators, scanner-derived indicators, connection analysis and statistical aggregation into a consolidated risk assessment.
- It improves **inspection targeting and operational efficiency**. Customs officers can prioritise bags with stronger risk indications, rather than relying primarily on random checks or manual assessment. This supports better allocation of limited customs resources.
- It enables **automated risk-indicator derivation** from external data sources, where lawful access is available. This reduces manual analytical workload and improves consistency across inspections.
- It supports **higher-quality risk scoring** through multi-source fusion. Qualitative and quantitative indicators can be weighted and aggregated into a more defensible global bag-risk indicator.
- It introduces **connection-analysis capability**. Suspicious direct or indirect links across available databases can strengthen risk hypotheses and support more informed inspection decisions.
- It provides an **operationalisation framework** through CustomsBagControl, bridging the gap between proof-of-concept outputs and deployable airport operations. This is essential because customs authorities do not purchase algorithms in the abstract; they require configurable workflows, governance arrangements, operational visualisation, and deployment support.

4.2.2 Target Market and Customers

The primary customer segment consists of **national and regional customs administrations** operating airport passenger controls. Within this segment, the most direct users are **airport customs units** at inland border airports, including small, medium-sized and large hubs. These customers select luggage for inspection and balance effective control with passenger flow.

A second customer group consists of **airport operators and airport security stakeholders** seeking throughput optimisation, process efficiency and smoother cooperation with customs authorities. While airport operators may not always be the direct purchasers of customs risk tools, they are important operational stakeholders because BAG-INTEL deployment affects airport flows, space configuration, IT connectivity and security procedures.

A third customer group consists of **border-control system integrators**. These actors may serve as delivery channels by embedding KER 1 with broader airport modernisation, border security, or critical infrastructure programmes.

A fourth, more selective, adjacent market consists of **law enforcement agencies** that may use connection-analysis capabilities beyond the customs environment, subject to legal, operational and data governance feasibility. This adjacent market should be approached cautiously, as some functionalities depend on access to specific databases and on national rules concerning automated querying and inter-agency data use.

The early adopter profile for KER 1 is likely to include customs authorities already participating in digital transformation programmes, airports facing growing passenger volumes, and customs units seeking

to move from manual or static risk assessment to dynamic, data-informed, AI-supported decision support.

4.2.3 Revenue Model and ROI Projections

KER 1 is best suited to a mixed revenue model that combines solution bundling, software licensing, professional services, and recurring maintenance:

- The primary model is **solution bundling**. KER 1 is unlikely to be sold as six separate ERs. Its strongest commercial proposition is as a bundled customs risk assessment and real-time decision support suite, either as part of a full BAG-INTEL deployment or as a modular risk-and-DSS package integrated into existing customs infrastructure.
- A second revenue stream is **software licensing**. Licensing may be structured on per-site, per-airport deployment, per-functional-module, per-number-of-concurrent-users, or, where acceptable for public buyers, per-number-of-cases-or-investigations-processed basis.
- A third revenue stream is **professional services**, including data connector implementation, configuration of risk policies, integration with customs and airport systems, customisation of dashboards, workflow design, compliance support, operational setup and training.
- A fourth revenue stream is **annual maintenance and support**, including updates to risk logic, connectors, model calibration, security patches, user support and operational performance monitoring.

The ROI of KER 1 is expected to be driven primarily by operational and institutional benefits rather than by direct financial revenues for the public buyer. The most relevant ROI indicators include improved inspection targeting, reduced manual analytical workload, better allocation of customs officers, more consistent inspection decisions, fewer unnecessary inspections, improved traceability of decisions, and greater capacity to process passenger flows without proportionate increases in personnel.

From the owners' and service providers' commercial perspective, ROI will depend on the number of airport sites adopting the suite, the degree of customisation required, the balance between one-off deployment fees and recurring maintenance income, and the extent to which core components can be reused across multiple deployments.

Indicative revenue logic for KER 1 can be summarised as follows:

Revenue stream	Indicative commercial logic
Software licence	Site-based or module-based licence for customs risk and DSS functionality
Customisation	One-off configuration for local risk policies, workflows, dashboards and connectors
Integration services	Paid integration with airport and customs IT systems

Revenue stream	Indicative commercial logic
Training and operational readiness	Structured training and deployment support for customs users
Maintenance and updates	Annual support, model calibration, connector updates and security updates
Usage-based options	Possible pricing by users or cases, where compatible with public procurement rules

4.2.4 Deployment and Delivery Model

KER 1 is expected to be deployed primarily via on-premises or hybrid models, given the sensitivity of customs data, potential connections to law enforcement databases, and national restrictions on data transfer. In some cases, an off-premises or as-a-service model may be feasible for non-sensitive components, training environments, or analytics functions that use appropriately protected or anonymised data. However, operational deployments in customs environments will most likely require strong local control.

The delivery process ought to adhere to a defined sequence:

Deployment phase	Main activities
Site assessment	Mapping of airport customs processes, data sources, IT systems and operational constraints
Data governance setup	Identification of lawful data sources, access permissions, retention rules and accountability arrangements
Technical integration	Implementation of connectors, APIs, user interfaces and system interoperability
Risk configuration	Definition of risk indicators, thresholds, workflows, alert logic and escalation rules
Pilot validation	Testing with customs users in controlled or operationally realistic settings
Training and change management	User training, operational playbooks and governance procedures

Deployment phase	Main activities
Operational support	Maintenance, calibration, performance monitoring and continuous improvement

The most realistic channel is business-to-government procurement, either directly with customs administrations or through system integrators that manage broader border control or airport digital transformation programmes. Pilot-to-production pathways are particularly important, as public authorities will require evidence of operational feasibility, security and user acceptance before full procurement.

4.2.5 Risks and Mitigation

The main risks for KER 1 concern data, legality, integration and user adoption.

- **Limited access to timely and relevant datasets.** External data, real-time feeds, and training data are essential to the performance of ER13, ER4, and the broader risk engine. If data access is limited, the suite's added value may be reduced. Mitigate this through early data governance mapping, modular design that allows partial deployment, and prioritisation of data sources that are legally accessible and operationally meaningful.
- **Restrictions on law enforcement database access.** Connection analysis may be constrained in jurisdictions where customs cannot automatically query relevant databases. Mitigate this by configuring ConnRisk only within lawful access boundaries, separating customs and law enforcement use cases, and documenting the legal basis for each data connector.
- **Over-reliance on automated recommendations.** Customs decisions must remain accountable and proportionate. Mitigation is to keep human officers in the decision loop, provide explainable risk indicators, log decision logic, and avoid fully automated intrusive inspection decisions without appropriate human validation.
- **Integration complexity.** Customs and airport IT environments are heterogeneous and may include legacy systems. Mitigation requires standardised APIs, early technical due diligence, modular deployment and involvement of airport IT stakeholders from the start.
- **User resistance or low operational adoption.** Customs officers may be reluctant to rely on new risk tools if they are perceived as opaque or disruptive. This should be mitigated through co-configuration workshops, user-centred interface design, training, pilot demonstrations and gradual integration into existing procedures.

4.3 BUSINESS CASE: KER 2 – AI-BASED LUGGAGE REIDENTIFICATION AND TRACKING SYSTEM

4.3.1 Value Proposition

KER 2 delivers the BAG-INTEL AI-based luggage reidentification and tracking capability. It brings together ER20 Luggage Reidentification, ER3 AI4bagReID, ER16 Optimal Probabilistic Bijective Mapping (OPBM), ER10 CCTV AI Detection Integrator and ER18 Providing CCTV for Object Detection.

The core business problem addressed by KER 2 is operational continuity. When a bag is flagged as suspicious during scanning, customs must be able to locate and reidentify it later, when it reaches the carousel, the exit zone or the customs area. Without reliable reidentification, the intelligence generated by scanning and risk assessment may not lead to an effective inspection.

KER 2 provides a non-intrusive, AI-camera-based solution to this problem. It avoids physical tagging or visible marking of suspicious luggage and uses computer vision to detect, characterise, track and reidentify luggage across airport zones. The bundle therefore supports targeted customs intervention without alerting travellers or disrupting baggage flow.

The value proposition includes the following main benefits:

- KER 2 enables **operationally actionable reidentification**. It links the suspicious bag identified earlier in the process to the bag observed in the customs area.
- It offers an **end-to-end AI pipeline**, including detection, signature extraction, feature-based characterisation, recognition, matching and alerting.
- It improves matching under uncertainty through **OPBM**, which strengthens the reidentification process where matching scores are noisy or acquisition conditions are variable.
- It provides **CCTV-AI integration and deployment guidance**, ensuring that airport video infrastructure can support AI-based object detection rather than merely human-monitored surveillance.
- It offers a **non-intrusive alternative** to approaches based on RFID tagging or physical marking. This is particularly valuable in customs contexts, where visible tagging may undermine enforcement by alerting passengers.

4.3.2 Target Market and Customers

The primary customers are **national customs administrations** and **airport customs units** deploying risk-based inspection workflows. These authorities need a reliable method to reidentify luggage selected for inspection after scanning.

Secondary customers include **airport operators and airport security departments** seeking AI-enabled baggage tracking, situational awareness and enhanced CCTV analytics. These stakeholders may not always purchase the customs reidentification solution directly, but their infrastructure and operational cooperation are essential for deployment.

A third customer segment consists of **border-control and security system integrators**, which can embed KER 2 into broader airport security and customs modernisation programmes.

Adjacent markets may include other organisations that require luggage tracking and reidentification beyond customs, provided that the use case is lawful, proportionate, and compatible with data protection constraints. However, the strongest and most project-consistent market remains customs control at airports.

Early adopters are expected to be customs authorities and airports participating in advanced security, AI video analytics, or smart airport initiatives, especially where operational conditions allow representative camera data collection and validation.

4.3.3 Revenue Model and ROI Projections

KER 2 supports a mixed revenue model based on software licensing, AI-as-a-Service, integration services, CCTV configuration, support and model maintenance:

- The first revenue stream is **software licensing** for AI4bagReID, luggage reidentification modules and CCTV integration components. Licences may be structured by airport, camera zone, number of video streams, or functional module.
- The second revenue stream is **subscription or AI-as-a-Service**. This model may be appropriate where continuous model updates, performance optimisation and retraining are required. In sensitive operational environments, AI-as-a-Service may need to be delivered through on-premises or private cloud configurations.
- The third revenue stream is **professional services**, including site surveys, CCTV placement design, camera configuration, integration with BAG-INTEL decision support, airport-specific calibration, validation, user training and operational readiness support.
- The fourth revenue stream is **maintenance and support**, including model updates, false-positive and false-negative monitoring, system health monitoring, retraining, software updates, and incident response.
- The fifth revenue stream is **methodology licensing or research-commercial pathways** for OPBM, including licensing to AI security firms, integration with research institutions or incorporation into related matching and reidentification applications.

Customer ROI is expected to come from reduced manual tracking, a higher probability of successfully inspecting selected suspicious luggage, improved customs intervention accuracy, reduced need for physical tagging, improved passenger flow, and more effective conversion of scanning decisions into actual enforcement actions.

For the commercial partners, ROI depends on repeatability across airports, the extent to which AI models and CCTV integration patterns can be reused, and the degree of recurring income generated through maintenance, calibration and subscription services.

4.3.4 Deployment and Delivery Model

KER 2 is deployment-intensive. It requires adaptation to each airport's physical layout, camera infrastructure, lighting conditions, baggage flows, passenger density and customs procedures. Therefore, deployment should be treated as a co-engineering process rather than a simple software installation.

The deployment model should include the following stages:

Deployment phase	Main activities
Operational mapping	Analysis of baggage flow from scanning to carousel and customs exit
CCTV assessment	Review of camera placement, coverage, resolution, angles and network constraints
Data collection	Collection of representative images from conveyor belt, carousel and customs areas
Model configuration	Calibration of detection, characterisation, tracking and reidentification models
OPBM integration	Application of probabilistic optimisation to improve matching under uncertainty
Workflow integration	Linking reidentification alerts to customs officer interfaces and decision support tools
Performance validation	Testing against site-specific KPIs such as matching accuracy, false alerts and response time
Continuous improvement	Model retraining and operational tuning after deployment

On-premises deployment is expected to be the preferred model where video data is sensitive or subject to strict national controls. A private cloud or edge cloud model may be possible, in which the customer or an authorised service provider controls the infrastructure. Public cloud deployment would require careful legal and security assessment and may be unsuitable for many operational customs environments.

4.3.5 Risks and Mitigation

- **Reidentification performance under real conditions.** Crowded spaces, stacked luggage, occlusion, poor lighting, different viewing angles, motion blur and passenger behaviour may reduce accuracy. Mitigation requires realistic data collection, site-specific CCTV optimisation, model retraining, probabilistic matching and careful threshold calibration.
- **Airport-specific customisation effort.** Camera infrastructures differ significantly across airports. Mitigation requires standard deployment guidelines, reusable integration patterns and early site surveys.
- **Data protection and privacy sensitivity.** Video analytics in airport environments may involve personal data or indirectly identifiable information. Mitigation requires privacy by design, data

minimisation, strict access control, retention limits, legal basis documentation and human oversight.

- **False positives and false negatives.** Incorrect reidentification may lead either to unnecessary intervention or missed inspection opportunities. Mitigation requires performance monitoring, human confirmation of alerts, confidence scoring and continuous validation.
- **Procurement fragmentation.** Customs authorities, airport operators and CCTV infrastructure owners may be different entities. Mitigation requires early stakeholder alignment, clear responsibility definitions, and integrator-led procurement where appropriate.

4.4 BUSINESS CASE: KER 3 – ADVANCED CONTRABAND DETECTION SYSTEM

4.4.1 Value Proposition

KER 3 constitutes the contraband detection pillar of BAG-INTEL. It combines the ER7 Advanced Detection System and the ER12 Advanced Baggage Scanning System. The KER integrates high-resolution CT/X-ray scanning with AI-based image analysis to detect contraband and support time-critical customs decisions.

The value proposition is based on the need to improve customs detection capabilities for inbound passenger baggage. Traditional manual image review places a significant burden on officers, requires high expertise and may be difficult to scale under high passenger volumes. KER 3 supports automated or semi-automated recognition of suspicious materials, objects and concealment patterns.

The key benefits are as follows.

- KER 3 provides **enhanced contraband recognition** through AI-based image analysis, with relevance to narcotics and other customs-relevant contraband categories.
- It reduces the burden of **manual image review** by supporting customs officers and less experienced analysts with automated detection outputs.
- It enables **faster decision-making** under short operational time windows, which is critical in passenger baggage control.
- It provides a **hardware-software proposition**, combining scanning infrastructure with AI detection modules. This is commercially important because customs authorities often require integrated solutions rather than detached algorithms.
- It supports **future extensibility**, since the detection pipeline can be updated, retrained and extended to new contraband types as additional data becomes available.
- KER 3 provides essential input for the broader BAG-INTEL workflow. Its detection outputs feed the risk assessment and decision support processes of KER 1 and trigger the reidentification workflow supported by KER 2.

4.4.2 Target Market and Customers

The primary customers are **customs administrations and airport customs units** seeking improved detection of contraband in inbound passenger baggage. Airports with inbound baggage flows that

require screening capability integrated into baggage handling processes are also a core market segment.

Secondary customers include **border security and law enforcement organisations**, where CT-based contraband detection is operationally relevant and legally authorised.

A further customer group consists of **security system integrators** delivering airport screening and border control modernisation programmes. These integrators can incorporate KER 3 into larger infrastructure deployments.

The early adopter profile includes customs authorities seeking to modernise scanning capability, airports with high international passenger flows, and jurisdictions interested in AI-supported detection of narcotics or undeclared goods.

4.4.3 Revenue Model and ROI Projections

KER 3 has a more hardware-oriented revenue model than the other KERs. The main revenue streams include hardware sales, software licensing, integration fees, support contracts and retraining services:

- The first revenue stream is **hardware sales** for scanning systems, including scanner unit sales, installation and commissioning.
- The second revenue stream is **software licensing** for contraband detection algorithms and AI modules. Licensing may be structured by scanner, site, algorithm package, or contraband detection category.
- The third revenue stream is **integration and commissioning services**, including integration with baggage-handling systems, integration with downstream decision-support interfaces, and operational testing.
- The fourth revenue stream is **support and maintenance contracts**, including scanner maintenance, software updates, security updates and performance tuning.
- The fifth revenue stream is **upgrade and retraining services**, including algorithm updates, retraining with additional data, extension to new contraband categories and tuning of detection thresholds.

Customer ROI should be measured by improved detection rates, reduced manual image-analysis burden, greater consistency, fewer missed contraband cases, higher throughput, and enhanced effectiveness of customs control. For commercial partners, ROI depends on scanner sales, algorithm licensing, installed-base upgrades, annual support and the ability to expand detection capabilities over time.

4.4.4 Deployment and Delivery Model

KER 3 requires physical deployment in airport baggage-handling or customs-screening areas. Unlike purely software-based KERs, deployment depends on scanner installation, available space, integration with baggage flows, safety requirements, operational scheduling, and maintenance capacity.

A typical deployment sequence would include:

Deployment phase	Main activities
Operational feasibility assessment	Review of airport layout, baggage flow, customs workflow and available space
Hardware installation	Scanner procurement, installation, commissioning and physical integration
Software deployment	Installation of detection algorithms and AI modules
Data and model setup	Calibration using relevant image data and contraband categories
Integration	Connection to BAG-INTEL risk and decision support components
Performance testing	Testing of detection accuracy, throughput and false alarm rate
Training	Training of customs officers and technical staff
Maintenance	Ongoing hardware service, software updates and algorithm retraining

KER 3 may be deployed as a completely new scanning capability or, where technically feasible, as an upgrade or retrofit pathway for an existing installed scanning base. The installed-base upgrade route may be commercially attractive because it reduces capital expenditure and accelerates adoption. However, feasibility will depend on scanner compatibility, data access, software architecture and certification or regulatory constraints.

4.4.5 Risks and Mitigation

- **High capital and implementation cost.** Advanced scanning infrastructure can be expensive, especially when combined with integration and operational change. Mitigation may include staged procurement, modular algorithm upgrades, pilot deployments, funding schemes and integration into wider customs modernisation programmes.
- **Availability of training data.** AI-based contraband detection depends on representative labelled datasets. Mitigation requires structured collaboration with customs authorities, controlled data collection, annotation protocols and continuous learning.
- **False alarm rate management.** High false alarm rates can reduce trust and increase manual workload. Mitigation requires tuning operational thresholds, validating with customs users, and conducting periodic performance reviews.

- **Trade-off between throughput and detection accuracy.** Customs environments require fast decisions. Mitigation requires optimisation of algorithms for operational speed, hardware-software performance testing and clear KPI monitoring.
- **Competition from other CT vendors and adjacent technologies.** Mitigation requires differentiation through customs-specific AI detection, integration with BAG-INTEL risk and reidentification workflows, and continuous product improvement.

4.5 BUSINESS CASE: KER 4 – INTEGRATED DIGITAL TWIN, KNOWLEDGE AND SECURE DEPLOYMENT LAYER

4.5.1 Value Proposition

KER 4 consolidates the deployment-grade capabilities required to integrate, operate and evolve BAG-INTEL as a unified platform in airport and customs environments. It includes ER9 Integrated Customs Information System, ER2 Customs Management Decision Support System (CMDSS), ER8 Knowledge Graph Database and Intelligent Analysis, and ER11 CI/CD and Encryption Framework.

The value proposition of KER 4 is deployability. BAG-INTEL's technical components can create sustainable impact only if they can be integrated with airport and customs systems, operated securely, adapted to local infrastructure, maintained over time, and configured for site-specific operational needs.

KER 4 provides the following main value elements:

- It offers a **unified customs data integration platform** that consolidates heterogeneous data sources into a single operational environment.
- It provides **digital-twin-driven management decision support**, enabling customs and airport managers to conduct what-if scenario analysis, resource allocation planning and operational optimisation.
- It provides **knowledge graph and semantic intelligence capabilities**, supporting the modelling of customs information flows, alerts, passenger-related information, reidentification outputs and operational decisions.
- It provides **regulatory-ready secure integration**, including access control, encrypted communications and continuity-of-service provisions.
- It supports **industrialised deployment and lifecycle management** through CI/CD practices, controlled releases, interoperability testing and secure updates.

KER 4 is therefore the backbone that enables the other KERs to transition from isolated components to an integrated, deployable BAG-INTEL system.

4.5.2 Target Market and Customers

The primary customers are **national customs administrations**, particularly airport customs units responsible for inbound baggage controls at inland border airports.

A second customer group consists of **airport operators and airport IT departments**, particularly those responsible for integration, deployment, operational optimisation and governance of airport systems.

A third customer segment comprises border control and security stakeholders, including airport security units and police units that may benefit from management decision-support outputs.

A fourth customer group consists of **system integrators for border and airport digital transformation**. These actors may become the most important channel for deployment, integration, and lifecycle-managed services.

A fifth, more specialised customer group consists of **security analytics and software developers** who may license or integrate the knowledge graph methodology into customs, border security, or related analytics products.

4.5.3 Revenue Model and ROI Projections

KER 4 has the clearest service platform revenue structure. It can generate revenue through platform licensing, DSS project fees, knowledge graph licensing, secure deployment services and managed support.

The revenue streams can be structured as follows:

Revenue stream	Indicative model
Platform licence for ER9	Site-based or airport-based annual licence, indicatively €30k–€80k, scaled by airport size and number of active integration points
DSS project fees for ER2	Tailored digital twin and management decision support projects, indicatively €30k–€80k, plus annual support of approximately 5% of project value
ER8 knowledge graph licensing and consulting	Initial methodology licensing and configuration, indicatively €15k–€40k, with recurring consulting as the knowledge base evolves
ER11 secure deployment and lifecycle services	Initial CI/CD setup, integration engineering and customisation, indicatively €20k–€50k per deployment, with optional managed-services contracts
Maintenance and support	Annual cybersecurity patching, release management, helpdesk, monitoring and upgrade services
Customisation	Site-specific modelling, dashboard configuration, API integration and scenario design

The customer-side ROI is expected to arise from reduced deployment risk, improved interoperability, better operational planning, faster configuration of airport-specific scenarios, stronger compliance posture, reduced manual integration effort and more sustainable system maintenance.

For commercial partners, ROI depends on the repeatability of integration patterns, the reuse of platform components, the scalability of the digital twin methodology, recurring managed services contracts, and long-term maintenance revenues.

4.5.4 Deployment and Delivery Model

KER 4 is likely to be deployed through an on-premises or hybrid model, especially in operational customs environments. However, some components, such as simulation models, training tools or non-sensitive analytical services, may be deployed off-premises if data governance allows.

The deployment model should be modular. Not all airports will require the full BAG-INTEL stack from the outset. The platform architecture should support selective component activation, ranging from full deployments with scanning, reidentification, risk assessment, and digital twin functionality to lighter deployments focused on risk assessment, data integration, or management decision support.

A typical deployment pathway includes:

Deployment phase	Main activities
Architecture assessment	Mapping of existing customs and airport IT systems
Integration design	Definition of APIs, data schemas, event flows and interoperability requirements
Platform installation	Deployment of the integration layer, edge database, message bus and security controls
Digital twin configuration	Modelling of local airport processes, resource flows, baggage flows and KPIs
Knowledge graph setup	Configuration of ontology, data pipelines and semantic relationships
CI/CD setup	Automated build, test, release and deployment pipelines
Security validation	Access control, encryption, penetration testing and continuity checks
User readiness	Training, documentation, support model and operational governance

KER 4 requires a strong service provider role. It cannot be delivered as a licence alone. Integration engineering, digital twin modelling, security configuration, DevOps and training are essential parts of the business case.

4.5.5 Risks and Mitigation

- **Integration complexity.** Customs and airport environments include heterogeneous systems, legacy infrastructure and different national procedures. Mitigation requires standardised REST APIs, modular architecture, formal data schemas, early IT engagement and phased interoperability testing.
- **Security and compliance burden.** BAG-INTEL operates in regulated environments and may process sensitive operational data. Mitigation requires access control, encryption, privacy by design, data protection impact assessment, cybersecurity testing and clear governance.
- **Underestimation of the integration layer's value.** Customers may focus on visible capabilities such as scanning or AI reidentification and underestimate the importance of secure deployment and lifecycle management. Mitigation requires positioning KER 4 as the deployment backbone of BAG-INTEL and demonstrating its role in reducing operational and procurement risk.
- **Customisation cost escalation.** Site-specific integration and digital twin configuration can become costly if requirements are not controlled. Mitigation requires reusable templates, generic simulation interfaces, standard deployment packages and clear scoping during procurement.
- **Partner coordination complexity.** KER 4 involves multiple owners and contributors. Mitigation requires clearly defining the Owner, Seller, and Service Provider roles, exploitation agreements, service-level responsibilities, and revenue-sharing principles.

4.6 JOINT BUSINESS OPPORTUNITIES AND SYNERGIES ACROSS KERS

The BAG-INTEL KERS are more commercially viable when positioned as complementary modules within an integrated customs control ecosystem rather than as isolated products. Each KER addresses a different part of the operational chain, and their combined value creates the basis for a more compelling business proposition.

KER 3 identifies suspicious content in baggage. KER 1 translates detection outputs and other risk indicators into a structured inspection decision. KER 2 enables customs officers to reidentify the selected bag upon its arrival at the customs area. KER 4 integrates these components into a secure, deployable and maintainable platform. This creates full operational logic: detect, assess, decide, reidentify, inspect, learn and optimise.

The main joint business opportunities are set out below:

Joint opportunity	Involved KERS	Business rationale
Full BAG-INTEL customs solution	KER 1, KER 2, KER 3, KER 4	End-to-end customs baggage control solution for airport deployments

Joint opportunity	Involved KERs	Business rationale
Risk-driven inspection package	KER 1, KER 4	Lower-complexity deployment focused on risk assessment, data integration and decision support
Detection and reidentification package	KER 2, KER 3	Integrated workflow from scanner-based suspicion to AI-based localisation of the bag
Digital twin and operational optimisation service	KER 4, KER 1	Simulation, resource allocation and risk-policy configuration for customs management
Secure integration and managed services	KER 4 with all KERs	Deployment backbone for long-term support, updates, interoperability and cybersecurity
Pilot-to-procurement reference deployments	All KERs	Demonstration sites used as market evidence for procurement discussions
Training and operational readiness services	All KERs	Cross-KER training, standard operating procedures and adoption support
System integrator partnerships	All KERs	Scaling through airport, border control and critical infrastructure integration channels

The most commercially attractive joint business case is the **full BAG-INTEL solution**, in which all four KERs are deployed as a modular yet integrated customs control platform. This model offers the greatest value to customs authorities because it covers the entire operational chain, from detection to inspection support. It also supports multiple revenue streams: hardware sales, algorithm licensing, platform licensing, integration services, digital twin configuration, training, maintenance and managed support.

A second promising opportunity is the **risk-driven inspection package** that combines KER 1 and KER 4. This package may suit customers who do not yet wish to deploy new scanning or reidentification infrastructure but are interested in improving risk assessment, decision support, operational planning, and data integration. It may offer a lower barrier to entry and can serve as a first phase towards fuller BAG-INTEL deployment.

A third opportunity is the **detection-and-reidentification package that combines** KER 2 and KER 3. This is particularly relevant where customs authorities already have a strong interest in AI-enhanced scanning and need a practical method to act on suspicious baggage after it leaves the scanning stage. The commercial logic is strong because detection without reidentification may not lead to effective intervention, while reidentification without reliable detection has limited enforcement value.

A fourth opportunity is the **digital twin and deployment advisory service**, based mainly on KER 4 but connected to the other KERs. This service can support airport-specific feasibility analysis, what-if scenarios, resource planning, customs workflow optimisation and procurement preparation. It may be particularly useful before full system deployment, helping customers understand operational requirements, expected benefits and integration needs.

From a commercial governance perspective, joint exploitation requires clear rules on ownership, revenue allocation, customer-facing responsibility, maintenance obligations, liability, support and IPR licensing. A Business Champion or Seller role may be needed for each joint package, supported by Service Providers responsible for deployment and Owners responsible for individual components.

The recommended joint exploitation approach is therefore modular and phased:

Phase	Commercial focus	Expected outcome
Phase 1	Reference validation and customer engagement	Use pilots and demonstrations as market evidence
Phase 2	Modular packaging	Define KER packages according to customer maturity and procurement capacity
Phase 3	Business Champion selection	Assign lead commercial responsibility for each package or target market
Phase 4	Procurement-ready offers	Prepare technical, financial and operational documentation for public buyers
Phase 5	Long-term service model	Establish support, maintenance, training, updates and managed services

KERs' synergies boost BAG-INTEL's sustainability. Rather than relying on a single result or partner, the project can pursue various exploitation approaches: integrating commercial products with industry partners, licensing software and platforms to technology owners, providing services through integrators, ensuring validation by customs authorities, and advancing AI, risk, and digital twin techniques via continuous research.

5 STAKEHOLDER ENGAGEMENT PLAN

5.1 OVERVIEW AND OBJECTIVES OF THE STAKEHOLDER ENGAGEMENT PLAN

BAG-INTEL's Stakeholder Engagement Plan outlines a structured approach for communicating, validating, positioning, and preparing the project's Key Exploitable Results for relevant audiences in institutions, operations, industry, research, policy, and society. By the final roadmap stage, stakeholder engagement extends beyond mere dissemination or awareness-raising. It becomes a vital tool for ensuring exploitation and sustainability, as deploying BAG-INTEL solutions relies on acceptance, trust, operational participation, and procurement readiness within highly regulated customs and airport environments.

BAG-INTEL focuses on a sensitive and complex area: customs control of passenger baggage at inland border airports. The KER portfolio features AI-driven contraband detection, luggage reidentification, risk-based decision support, digital twin-enabled management, secure system integration, and knowledge management. For these efforts to have lasting impact, they must align with the needs, constraints, and decision-making processes of customs authorities, airport stakeholders, law enforcement, technology providers, regulators, standardisation bodies, research communities, and the public.

The Stakeholder Engagement Plan facilitates the shift from technical project results to solutions that are credible, deployable, and accepted by institutions. It outlines the engagement strategy needed to ensure that the final KERs are perceived not merely as theoretical research findings, but as assets that are operationally effective, legally compliant, commercially transparent, and practically usable.

The specific objectives of the Stakeholder Engagement Plan are the following:

Objective	Description	Relevance to BAG-INTEL
Validation of KER relevance	To confirm that the final KERs respond to real customs, airport and security needs	Ensures that exploitation priorities are grounded in end user requirements
Support for operational adoption	To prepare customs officers, airport authorities and related operational users for the practical use of BAG-INTEL capabilities	Reduces adoption barriers and improves user acceptance
Exploitation and market positioning	To engage potential buyers, integrators, commercial partners and institutional adopters	Supports procurement readiness, business case refinement and post-project commercialisation
Regulatory and policy alignment	To involve competent authorities, policy actors and compliance stakeholders	Ensures that deployment pathways remain compatible with customs, border security, AI, data protection and cybersecurity requirements

Objective	Description	Relevance to BAG-INTEL
Standardisation and interoperability	To involve standardisation and pre-standardisation communities where relevant	Supports future compatibility, scalability and alignment with relevant technical and operational frameworks
Public trust and transparency	To communicate the purpose, safeguards and public value of BAG-INTEL technologies	Supports societal acceptance of AI-based customs control and reduces risks of misunderstanding
Sustainability beyond the project	To maintain strategic links with relevant communities after project completion	Supports follow-on pilots, further research, exploitation agreements and market uptake

The engagement approach is based on the following principles:

- It is **stakeholder-specific**. Different groups require different information, channels and levels of technical detail. Customs officers require practical demonstrations and training. Policy stakeholders require evidence of compliance, security and public value. Technology providers require integration documentation and commercial clarity. The public requires transparent, accessible communication about purpose, safeguards, and expected benefits.
- Is **KER-oriented**. Engagement activities are linked to the four final KERs: Customs Bag-Risk Assessment and Real-Time Decision Support Suite; AI-Based Luggage Reidentification and Tracking System; Advanced Contraband Detection System; and Integrated Digital Twin, Knowledge and Secure Deployment Layer. This ensures stakeholders engage around concrete exploitation assets rather than general project messages.
- It is **evidence-based**. Stakeholder engagement must be supported by pilot findings, technical validation, user feedback, risk assessments, operational demonstrations and business case documentation. In public authority markets, adoption depends on credible evidence rather than promotional claims.
- It is **two-way and iterative**. Stakeholders are not passive recipients of information. Their feedback informs KER refinement, deployment models, training needs, risk mitigation, market positioning and sustainability planning.
- It is **ethics and security-aware**. Because BAG-INTEL involves AI, video analytics, risk assessment, data integration and customs decision support, engagement must address data protection, human oversight, explainability, proportionality, cybersecurity, operational accountability and public trust.
- It is **exploitation-oriented**. Engagement is designed to support post-project uptake, licensing, deployment, integration, public procurement, training, standardisation contribution and further research. It therefore bridges communication, dissemination, exploitation and sustainability.

- It is **sustainability-focused**. Engagement should continue beyond the formal end of the project through reference deployments, follow-on pilots, partner networks, policy dialogues, standardisation activities, scientific dissemination and commercial contacts.

The relationship between the KERs and the core engagement objectives is summarised below.

KER	Main engagement need	Priority stakeholder groups
KER 1: Customs Bag-Risk Assessment and Real-Time Decision Support Suite	Validation of risk logic, user acceptance, lawful data access, decision support usability	Customs authorities, customs officers, data access authorities, regulators, airport operators
KER 2: AI-Based Luggage Reidentification and Tracking System	Validation of reidentification performance, CCTV configuration, privacy safeguards and operational workflows	Customs authorities, airport operators, airport IT/security teams, CCTV infrastructure owners, privacy and data protection stakeholders
KER 3: Advanced Contraband Detection System	Validation of detection performance, false alarm management, integration with customs workflows and procurement feasibility	Customs authorities, scanner technology stakeholders, airport operators, border security authorities, system integrators
KER 4: Integrated Digital Twin, Knowledge and Secure Deployment Layer	Integration readiness, digital twin uptake, secure deployment, interoperability and long-term maintenance	Airport IT departments, customs management, system integrators, cybersecurity stakeholders, technology providers, standardisation actors

The Stakeholder Engagement Plan is intended to ensure that BAG-INTEL's final KER portfolio is understood, tested, trusted and positioned for further uptake in the customs and airport security ecosystem.

5.2 STAKEHOLDER MAPPING AND UPDATE FROM D6.3

D6.3 laid out the initial stakeholder identification and analysis for BAG-INTEL. The stakeholder map categorised key groups such as regulatory authorities, end users, industry and technology providers, academia and research institutions, policy and standards bodies, and civil society and the public. This structure remains relevant and serves as the foundation for D6.5.

At the final roadmap stage, the mapping must be revised to reflect the KER assessment and business case development. The revised mapping more distinctly differentiates between direct users, institutional buyers, operational validators, deployment enablers, commercialisation partners, regulatory and policy actors, standardisation entities, research multipliers, and public trust audiences.

This update is essential because the project has shifted from a general stakeholder engagement phase to a KER exploitation and sustainability phase. The key question is now not only «who should know about BAG-INTEL, but also «who can validate, adopt, procure, integrate, regulate, standardise, finance, scale, or legitimise the BAG-INTEL KERs?"

The updated stakeholder mapping is presented below:

Table 5-1- Stakeholders mapping

Stakeholder group	Role in BAG-INTEL	Level of influence	Level of interest	Main KER relevance	Engagement priority
Customs authorities and airport customs units	Primary institutional users, validators and potential buyers	Very high	Very high	All KERs, especially KER 1, KER 2 and KER 3	Critical
Customs officers and operational staff	Day-to-day users of decision support, detection outputs and reidentification alerts	High	Very high	KER 1, KER 2, KER 3	Critical
Airport operators	Operational environment owners and key deployment stakeholders	High	High	KER 2, KER 3, KER 4	Critical
Airport IT and security departments	Technical integration, cybersecurity, CCTV and infrastructure stakeholders	High	High	KER 2, KER 4	Critical
Border control, police and law enforcement authorities	Adjacent operational users and institutional stakeholders	Medium to high	Medium to high	KER 1, KER 2, selected ConnRisk applications	High
Regulatory authorities and policy makers	Define legal, operational, customs, border security and AI governance conditions	Very high	Medium to high	All KERs	Critical

Stakeholder group	Role in BAG-INTEL	Level of influence	Level of interest	Main KER relevance	Engagement priority
Standardisation and pre-standardisation bodies	Support future interoperability, standardisation alignment and technical legitimacy	High	Medium	KER 3, KER 4, cross-KER interfaces	High
Technology providers and industrial partners	Component owners, suppliers, commercial partners and production actors	High	Very high	All KERs	Critical
System integrators	Potential deployment channels and service providers for full BAG-INTEL solutions	High	High	All KERs, especially KER 4	Critical
Data providers and data access authorities	Enable lawful access to relevant risk, customs, passenger, flight and operational data	High	Medium	KER 1, KER 4	High
Cybersecurity and privacy stakeholders	Support secure, lawful and trusted deployment	High	Medium to high	KER 2, KER 4, cross-KER governance	High
Research and academic institutions	Scientific validation, further R&D, publications, education and methodology transfer	Medium	High	All KERs, especially AI, digital twin and risk methodologies	Medium to high
Training and formation organisations	Support curricula, user readiness and operational capacity building	Medium	High	All KERs, especially operational adoption	Medium to high

Stakeholder group	Role in BAG-INTEL	Level of influence	Level of interest	Main KER relevance	Engagement priority
European and international networks	Dissemination, policy alignment, replication and cross-border uptake	Medium to high	Medium	All KERs	Medium to high
Media, travellers and the general public	Indirect beneficiaries and public trust audience	Medium	Medium	Public value and safeguards across all KERs	Medium

The updated mapping confirms that customs authorities remain the primary stakeholder group. They are the principal institutional adopters of BAG-INTEL and are central to operational validation, requirements definition, risk policy configuration, data governance, procurement, and post-project uptake. Their engagement should remain continuous and substantive, with an emphasis on hands-on demonstrations, operational workshops, decision-support usability, inspection workflows, training, and feedback loops.

Customs officers and operational end users are equally important because they determine whether the system can be used in practice under real-world conditions. Even if an authority procures the system, BAG-INTEL's effectiveness will depend on how officers interpret risk indicators, use alerts, respond to reidentification outputs, interact with visualisation interfaces, and trust AI-assisted recommendations. Therefore, end-user engagement must focus on usability, explainability, operational fit, and training.

Airport operators and airport IT/security departments become more prominent in the D6.5 mapping than in the earlier broad categorisation. This reflects the final KER structure. KER 2 depends on CCTV infrastructure, camera placement, video data flows and airport-specific operational settings. KER 3 depends on baggage handling integration and screening infrastructure. KER 4 depends on platform integration, digital twin modelling, cybersecurity and interoperability. These aspects require close engagement with airport stakeholders beyond customs alone.

Regulatory authorities and policymakers remain critical because BAG-INTEL operates in a sensitive field involving customs enforcement, AI, data protection, cybersecurity, airport operations, and potential law-enforcement data. Their role is not limited to approval or oversight; they also influence the institutional conditions under which AI based customs tools can be trusted, procured and deployed.

Technology providers, industrial partners and system integrators are essential for post-project exploitation. The final business cases demonstrate that BAG-INTEL KERs are unlikely to scale through research dissemination alone. They require productisation, integration services, licensing models, maintenance contracts, procurement packages and commercial partnerships. System integrators may become critical channels for embedding BAG-INTEL into broader airport or border control modernisation programmes.

Standardisation and pre-standardisation bodies remain relevant for future interoperability and wider acceptance. BAG-INTEL may not complete full standardisation within the project timeframe, but

engagement with standards communities can help identify gaps, promote compatibility and support future uptake. This is particularly relevant for data exchange, imaging standards, security controls, AI system assessment, human-system interaction and airport security workflows.

Research and academic institutions remain important for scientific sustainability. BAG-INTEL generates methods and knowledge in AI-based detection, computer vision, risk assessment, probabilistic matching, digital twin modelling, knowledge graphs and secure architecture. Engagement with this community supports publications, further research projects, doctoral and postgraduate education, open science outputs where appropriate, and technology transfer.

Civil society, media and the public should be engaged in a proportionate and transparent manner. They are indirect beneficiaries through safer borders, reduced contraband flows and potentially smoother passenger journeys. However, they may also have legitimate concerns about AI-based risk assessment, video analytics, privacy, bias, transparency and accountability. Public communication should therefore avoid technical overstatement and emphasise safeguards, human oversight, proportionality and public value.

The updated stakeholder mapping can also be expressed in terms of stakeholder function:

Table 5-2- Stakeholders function

Stakeholder function	Relevant groups	Purpose of engagement
Operational validation	Customs officers, customs authorities, airport operators, airport IT/security teams	Test usability, workflows, performance and deployment feasibility
Institutional adoption	National customs administrations, airport customs units, public authorities	Prepare procurement, governance and post-project uptake
Technical integration	Airport IT, system integrators, technology providers, cybersecurity stakeholders	Ensure interoperability, secure deployment and maintainability
Commercialisation	Industrial partners, system integrators, buyers, innovation networks	Refine business cases, licensing and service models
Regulatory assurance	Regulators, policy makers, data protection stakeholders, law enforcement authorities	Ensure legal, ethical, security and policy alignment
Standardisation	Standards Development Organisations, pre-standardisation bodies, technical working groups	Identify standardisation gaps and promote interoperability

Stakeholder function	Relevant groups	Purpose of engagement
Scientific sustainability	Universities, research centres, scientific communities	Support research dissemination, further projects and methodological development
Public legitimacy	Travellers, citizens, media, civil society	Promote transparency, trust and understanding of safeguards

6 IPR MANAGEMENT FINAL UPDATE

The management of Intellectual Property Rights (IPR) within BAG-INTEL aims to ensure that the ownership, use and protection of intellectual assets generated or contributed throughout the project are clearly identified and appropriately documented. Given the collaborative nature of the project and the involvement of multiple consortium partners, establishing transparent rules governing ownership, access rights, and the use of Background and Foreground Intellectual Property has been essential to support project implementation and provide legal certainty for all participants.

This section presents the final status of the project's intellectual property landscape. It includes an update of the declared Background Intellectual Property, the final inventory of the Foreground Intellectual Property (Results) generated during the project, and the corresponding IPR Matrix setting out ownership, applicable Background IP, licensing arrangements, protection mechanisms and access conditions. The section also summarises the final ownership arrangements and the measures adopted by the consortium to protect project results, in accordance with the GA and the CA.

Throughout the project, the consortium maintained an ongoing process for identifying and documenting intellectual property assets, enabling newly identified Background IP and project results to be incorporated as the project progressed. This approach supported consistent IPR management and a clear distinction between pre-existing assets and results generated within BAG-INTEL.

6.1 UPDATE ON BACKGROUND IP

Since submitting the previous version of this deliverable, the consortium has continued to monitor and document the IPR relevant to the BAG-INTEL project, in accordance with the project's IPR management strategy and the provisions of the GA. As the project progressed, consortium partners identified and formally declared two additional Background IP assets.

The declaration of these additional Background IP assets reflects the evolution of the project's technical activities and ensures a clear distinction between pre-existing intellectual property contributed by the partners and the results generated within BAG-INTEL. In line with the methodology adopted throughout the project, each Background IP declaration includes information on ownership, description, intended use within the project, and any applicable access conditions or restrictions.

Accordingly, the Background IP inventory has been updated with two additional entries, BG17 and BG18, which are presented below.

BG17 – Training Materials employed through Training Curricula Targeting the Needs of End-users ahead of and during the Use-Case Deployments (HfoeD): The background, owned by HfoeD, consists of training materials, including user guides, presentations and audiovisual material, developed to support the delivery of training curricula for end-users participating in the BAG-INTEL use-case deployments at Billund Airport and Thessaloniki "Makedonia" Airport. The materials provide technical guidance on the BAG-INTEL integrated platform, explain its key functionalities and operational capabilities, and support scenario-based exercises enabling end-users to interact with the platform in near-realistic operational conditions, such as baggage inspection and illicit goods detection. The background, as part of Task 5.4 – Development of Initial Training Material for End-users, aims to support on-site and online training activities. The project's technical partners and subject-matter experts reviewed and validated the training materials before making them available through the designated BAG-INTEL shared repositories. Access is limited to consortium members and authorised end-users participating in the project. No specific restrictions or additional conditions apply regarding the use or exploitation of this background beyond its use within the project.

BG18 – CI/CD Integration Framework and DevOps Methodology (INTRA): The background, owned by INTRA, consists of a pre-existing CI/CD integration framework and DevOps methodology, including automation methodologies, pipeline configuration patterns, deployment governance procedures, integration coordination practices, proprietary automation scripts, security policy frameworks and testing strategies developed through previous integration-intensive projects. The background does not include the underlying open-source software components (e.g., Jenkins, Docker, Harbor and Apache Kafka), which remain subject to their respective licences. The background, as part of Task 2.5, aims to design, configure, and operate the BAG-INTEL CI/CD pipelines; support the phased integration of platform components; perform interoperability testing; and manage controlled software releases across the project's deployment environments. The background is made available to consortium partners on a royalty-free basis solely for implementing the project and for its duration. Partners may use the CI/CD infrastructure and its outputs, including deployment packages and test results, but may not extract, reproduce or independently deploy INTRA's proprietary automation scripts, pipeline configurations or security policy templates outside the project context. INTRA retains full ownership of the background. Access for exploitation purposes by other consortium partners is subject to a prior written agreement under fair and reasonable conditions, in accordance with the Grant Agreement. The background may not be sublicensed, released as open source or incorporated into third-party products without INTRA's prior written consent. This background underpins ER11 but remains distinct from the foreground generated within BAG-INTEL and has been formally declared to clearly delineate the boundary between pre-existing background IP and project results.

6.2 FOREGROUND IP GENERATED DURING THE PROJECT

Foreground IP, referred to as Results under the Horizon Europe Grant Agreement, comprises all tangible and intangible outputs generated during the implementation of the BAG-INTEL project that may be eligible for protection, exploitation or further development. Throughout the project, consortium partners have continuously identified and assessed ERs in accordance with the project's exploitation strategy and the provisions of the GA.

The following section presents the final inventory of the Exploitable Results (ERs) generated during the project. For each result, a brief description is provided together with its ownership and its role within the relevant project activities.

ER1 – Multimethod Modelling: The result, owned by STAM, consists of the modelling methodology underpinning the BAG-INTEL digital twins. Developed within Tasks 2.6 and 4.4, it provides the methodological framework for modelling customs operations and supporting subsequent decision-support functionalities.

ER2 – Customs Management Decision Support System (CMDSS): The result, owned by STAM, consists of a Decision Support System based on the BAG-INTEL digital twin. Developed within Tasks 2.6 and 4.4, it supports customs authorities by assisting decision-making processes related to baggage inspection and operational management.

ER3 – Risk-based Decision Support for Customs and AI Vision-based Luggage Reidentification (AI4bagReID): The result, owned by LTA, combines AI-based luggage reidentification with risk assessment capabilities to support customs officers in selecting baggage for inspection. Developed within Task 3.3, it integrates bag risk assessment with visual reidentification techniques to improve the accuracy and efficiency of inspection decisions.

ER4 – Connection-analysis-based Risk Assessment (ConnRisk): The result, owned by LTA, consists of a software tool for assessing baggage-related risks using external data sources and connection analysis. Developed within Task 4.1, it identifies direct and indirect links between entities to support intelligence-driven customs inspections.

ER5 – Methodology for Operational BAG-INTEL (CustomsBagControl): The result, owned by LTA, consists of a methodology supporting the operational deployment of BAG-INTEL solutions. Developed within Task 4.3, it provides guidance for integrating the project's technologies into real-world customs operations, including real-time decision support.

ER6 – Customs Real-time Decision Support System (CRDSS): The result, owned by LTA, consists of a real-time decision support system designed to assist customs authorities during operational inspections. Developed within Task 4.3, it uses AI-driven analysis to support timely and informed inspection decisions.

ER7 – Advanced Detection Systems: The result, owned by SDE, consists of advanced contraband detection technologies combining high-resolution scanning and enhanced data collection capabilities. Developed within Tasks 2.4 and 3.2, it supports the identification of prohibited or illicit items in baggage.

ER8 – Knowledge Graph Database and Intelligent Analysis: The result, owned by UGR, consists of a knowledge graph methodology supporting intelligent data analysis and decision support. Developed within Tasks 2.4 and 4.5, it enables the integration and analysis of heterogeneous datasets for customs risk assessment.

ER9 – Integrated Customs Information System: The result, owned by LTA with contributions from INTRA, consists of an integrated software platform for the consolidation and management of customs-related information. Developed within Task 4.1, it facilitates the exchange and integration of data required for BAG-INTEL services.

ER10 – CCTV AI Detection Integrator: The result, jointly owned by CEA and PSI, integrates CCTV infrastructure with AI-based object detection technologies. Developed within Tasks 3.4 and 4.3, it supports automated monitoring and object recognition in customs environments.

ER11 – CI/CD Methodologies and Encryption Techniques for the Integrated BAG-INTEL System: The result, owned by INTRA, consists of secure software integration methodologies, CI/CD processes and encryption mechanisms supporting the development and deployment of the BAG-INTEL platform. Developed within Tasks 2.3 and 2.5, it ensures secure and efficient integration of the project's software components.

ER12 – Advanced Baggage Scanning System: The result, owned by SDE, consists of advanced baggage scanning hardware equipped with AI-assisted detection capabilities. Developed within Tasks 2.4 and 3.2, it enhances the identification of contraband through high-resolution imaging technologies.

ER13 – AI Tool for External-data-based Risk Assessment: The result, jointly owned by EXUS and UGR, consists of an AI-based software tool for extracting risk indicators from external data sources and producing baggage risk assessments. Developed within Tasks 4.1 and 4.5, it complements the overall customs risk analysis framework.

ER14 – Customs Bag-risk Management: The result, owned by LTA, consists of a software tool supporting the management of baggage-related risks throughout the customs inspection process.

Developed within Tasks 3.1, 4.1, 4.2 and 4.3, it assists customs authorities in prioritising inspections based on assessed risk levels.

ER15 – Training and Education Modules for Customs: The result, owned by HfoeD with contributions from several consortium partners, consists of training materials and educational modules supporting the use of BAG-INTEL technologies by customs authorities. Developed within Task 5.3, it provides guidance for the effective use of the project's tools and methodologies.

ER16 – Optimal Probabilistic Bijective Mapping (OPBM): The result, owned by INSA with contributions from CEA, consists of a probabilistic methodology for luggage reidentification based on matching scores across multiple baggage observations. Developed within Tasks 3.3, 4.1 and 4.2, it improves the accuracy of baggage matching within the BAG-INTEL framework.

ER17 – Multi-Risk Indicators Statistical Weighting and Aggregation of Qualitative and Quantitative Data: The result, owned by INSA with contributions from LTA and UGR, consists of a methodology for combining multiple qualitative and quantitative risk indicators into a global risk score. Developed within Tasks 4.1, 4.2 and 4.3, it supports inspection decision-making through integrated risk assessment.

ER18 – Providing CCTV for Object Detection: The result, owned by PSI with contributions from CEA, consists of a methodology for deploying CCTV systems in customs environments to support AI-based object detection. Developed within Task 3.3, it provides practical guidance for integrating video surveillance with intelligent detection capabilities.

ER19 – Secure-by-Design Scheme of the Architecture: The result, owned by ICCS with contributions from the consortium partners, consists of a Secure-by-Design methodology for the BAG-INTEL system architecture. Developed within Task 2.3, it establishes security principles and design requirements to support the secure development and integration of the platform.

ER20 – Luggage Reidentification: The result, owned by CEA, consists of an AI-based software solution for luggage reidentification, incorporating baggage detection, characterisation, tracking and reidentification functionalities. Developed within Task 3.3, it enables the reliable identification and tracking of baggage throughout the customs inspection process.

6.3 IPR MATRIX – FINAL VERSION

The final IPR Matrix presents the intellectual property information for all ERs identified during the BAG-INTEL project. It records the ownership of each result, the contributing partners, the applicable ownership model, any related Background IP, the relevant protection mechanism, licensing arrangements and the conditions governing access and use during and after the project.

The matrix has been prepared using the information provided by the consortium partners and reflects the final status of the project's intellectual property assets at the time of submission of this deliverable. It serves as the consortium's reference for the ownership, protection and management of project results and provides a clear overview of the arrangements established for each identified ER.

Table 6-1- BAG-INTEL's Final IPR Matrix

IPR	Exploitable Result (ER) name	ER category (please select from dropdown list)	ER short description	Name(s) of Owner(s) of this ER	Other Contributors to this ER	Type of Ownership (Single or Joint)	Related Background IP (if applicable)	Conflicting IP	Licence of ER	Type of protection (if applicable)	Conditions to use within the project	Conditions to use the result after the end of the project
ER1	Multimethod modelling	Methodology	The modelling methodology on which the digital twins are based on.	STAM	-	Single	BG8	-	-	None	Free to use	Consultancy fee
ER2	Customs Management Decision Support System (CMDSS)	Software	Decision Support System (DSS) based on the Digital Twin (developed in Task 2.6) for the customs	STAM	-	Single	BG8	-	AnyLogic, AnyLogic Private Cloud	None	Free to use	SaaS

ER3	Risk-based decision support for customs in selecting the best bags for inspection.	Software	Decision support for customs in selecting the best bags for inspection based on the overall bag risk assessment (including scanning results) and the reidentification results.	LTA	-	Single	-	-	-	None	Free to use	Depends on the case
ER4	Connection-analysis-based risk assessment (ConnRisk)	Software	Tool for deriving external-data-based bag risk assessment, based on suspicious connections (including indirect connections) identified in and	LTA	-	Single	BG2	-	Free use for European LEAs and customs authorities	Confidentiality agreement	Free to use	Free license for European LEAs and customs authorities to use it as it is. Consultancy for a fee.

			across the available databases, considering the strength and suspiciousness of the connections.									
ER5	Methodology for operational “BAG-INTEL”, including visualisation of real-time customs decision support (CustomsB agControl)	Methodology	Comprises methodology for implementing and operating “BAG-INTEL” solutions, hence bridging the gap between the BAG-INTEL proof-of-concept and operational “BAG-INTEL” solutions.	LTA	-	Single	-	-	-	None	Free to use	Consultancy fee



ER6	Customs Real-time Decision Support System (CRDSS)	Software	Enhances customs efficiency using AI for real time decision-making.	LTA	-	Single	-	-	-	Under definition	Free to use	Agreement
ER7	Advanced Detection Systems	Software	High-precision (extended data collection, as initially planned for in the GA required for "high-precision") contraband detection technology.	SDE	TOLD (data collection)	Single	n/a	n/a	Proprietary	Trademark	free to use	License Agreement (only specific SDE X-Ray Scanner model)
ER8	Knowledge Graph Database and Intelligent Analysis	Methodology	Using advanced data models for DSS and risk assesment	UGR	-	Single	n/a	n/a	Proprietary	None	Free to use	Consultancy fee

ER9	Integrated Customs Information System	Software	Unified platform for customs data integration.	LTA	INTRA	Single	n/a	n/a	-	-	Free to use	Consultancy fee
ER10	CCTV AI Detection Integrator	Software	Integrates CCTV Technology with AI Object Detection Modules	CEA, PSI	-	Joint	-	-	-	-	-	-
ER11	CI/CD methodologies and encryption techniques for the integrated BAG-INTEL system	Software	Encrypted integration between multiple components in a secure environment. Complementing this, it includes the robust Continuous Integration and Continuous Delivery (CI/CD)	INTRA	-	Single	N/A	-	Proprietary	Copyright (for proprietary automation scripts and configuration code) and trade secrets / confidential know-how (for the underlying CI/CD methodology, pipeline architecture, and	Available to all BAG-INTEL consortium partners on a royalty-free basis for project implementation purposes.	License Agreement

			methodologies and tools that govern the efficient development, integration, and deployment of the BAG-INTEL system's various software components.							integration coordination practices).		
ER12	Advanced Baggage Scanning System	Hardware	High-resolution scanners with integrated AI about contrabands	SDE	n/a	Single	n/a	n/a	Proprietary	Trademark	Free to use	Purchase of Hardware incl. relevant Algorithm Licenses
ER13	AI tool for external-data-based risk assessment	Software	Tool for extracting bag-risk indicators from external	EXUS, UGR	-	Joint	-	-	-	-	-	-

			data and for assessing the external-data-based bag-risk based on the extracted indicators									
ER14	Customs bag-risk management	Software	Tool for managing the risk of contraband in a bag	LTA	-	Single	n/a	n/a	Proprietary	Under definition	Free to use	Agreement
ER15	Training and Education Modules for Customs	Methodology	Training for customs officials to optimize operations.	HFOD	CEA, EXUS, INSA, LTA, SDE, STAM, PSI, UGR	Single	BG17	n/a	n/a	n/a	Free to use	In agreement with HfoeD (Task 5.4 leaders)
ER16	Optimal Probabilistic Bijective Mapping for the reidentification of luggage for customs	Methodology	Probabilistic bag-reidentification in the BAG-INTEL context - based on the matching	INSA	CEA	Single	BG16	n/a	open source	n/a	free to use	n/a

	inspection (OPBM)		scores of a collection of bags									
ER17	Multi-Risk Indicators Statistical Weighting and Aggregation of Qualitative and Quantitative Data	Methodology	Build up a Global Risk Indicators for Inspection Decision Making based on data mix of different nature	INSA	LTA, UGR	Single	-	n/a	open source	n/a	free to use	n/a
ER18	Providing CCTV for Object Detection	Methodology	Experiences in setting up CCTV in Custom zones for AI based object detection	PSI	CEA	Single	ER10	n/a	n/a	n/a	free to use	n/a
ER19	Secure-by-Design scheme of the architecture	Methodology	Secure-by-Design scheme of the architecture	ICCS	INSA, ALL	Single	-	-	-	-	-	-

ER20	Luggage reidentification	Software	AI tool dedicated luggage reidentification comprising 4 components : 1) luggage detection, 2) luggage characterisation, 3) luggage tracking and 4) bag-reidentification	CEA	-	Single	-	-	-	-	-	-
------	--------------------------	----------	---	-----	---	--------	---	---	---	---	---	---

6.4 OWNERSHIP AND LICENSING – FINAL ARRANGEMENTS

Ownership of the ERs generated during the BAG-INTEL project has been allocated in accordance with the GA and the CA. In general, each result is owned by the partner or partners that generated it. Where two or more partners have jointly developed a result and their respective contributions cannot be separated for the purposes of protection or ownership, the result is subject to joint ownership in accordance with the applicable provisions of the GA.

The final ownership arrangements are presented in the IPR Matrix (Section 6.3), which identifies the owner(s), contributing partners, the applicable ownership model (single or joint ownership) and, where relevant, the associated Background IP. This provides a clear record of the relationship between pre-existing intellectual property and the results generated within the project.

Access to Background IP and project Results has been governed by the access rights provisions of the GA and the CA. Throughout the project, the partners were granted access only to the Background IP and Results necessary for carrying out their assigned tasks and under the conditions agreed by the respective rights holders. Any use of project Results outside the scope of BAG-INTEL, including licensing to third parties, remains subject to the approval of the respective owner(s) and, where applicable, to separate contractual arrangements.

Background IP remains the property of the partner that declared it. The identification and declaration of additional Background IP during the course of the project ensured that pre-existing assets were clearly distinguished from the intellectual property generated within BAG-INTEL, providing transparency in the allocation and management of intellectual property rights across the consortium.

6.5 PROJECT RESULTS PROTECTION – FINAL STATUS

Throughout the BAG-INTEL project, the partners reviewed the project results to determine whether IP protection was appropriate, taking into account the nature of each result, its characteristics and the applicable legal framework. The choice of protection mechanism was made on a case-by-case basis by the respective owner(s), in accordance with the GA and the CA.

The protection status of the identified ERs is presented in the IPR Matrix (Section 6.3). Depending on the type of result, the applicable forms of protection include copyright, confidential know-how and trade secrets. Where appropriate, the respective owner(s) may decide to pursue additional forms of protection following the completion of the project, in accordance with their internal policies and applicable legislation.

Before any public dissemination of project results, partners considered whether the proposed disclosure could affect the protection of intellectual property. Where necessary, appropriate measures were taken to safeguard intellectual property rights prior to publication, in accordance with the procedures established under the GA and the CA.

The protection measures adopted throughout the project contributed to the clear identification of intellectual property, the preservation of ownership rights and the appropriate management of project results in accordance with the applicable contractual framework.

6.6 LESSONS LEARNED AND RECOMMENDATIONS FOR POST-PROJECT IPR MANAGEMENT

The implementation of the BAG-INTEL IPR framework confirmed the importance of managing intellectual property as an ongoing process throughout the project. Updating the Background IP declarations and the inventory of ERs at regular intervals allowed the consortium to accurately document ownership, clearly distinguish pre-existing intellectual property from project-generated results, and maintain an up-to-date record of the project's intellectual assets.

Another important outcome was the close cooperation between the technical, legal and project partners during the identification and documentation of intellectual property. Early discussions on ownership, contributions and the use of Background IP helped clarify responsibilities and facilitated the preparation of the final IPR Matrix.

Following the completion of the project, the owners of the identified results should continue to review their intellectual property portfolios and assess whether additional protection measures or ownership arrangements are required as the results evolve. Where results are jointly owned, any future use should be supported by clear agreements between the relevant parties. Similarly, any future dissemination or transfer of project results should take into account the existing ownership arrangements and ensure that confidential information and pre-existing intellectual property remain appropriately protected.

7 STANDARDISATION

7.1 LATEST DEVELOPMENTS IN STANDARDS AND STANDARDISATION ACTIVITIES CUSTOMS CONTROL OF AIRPORT ARRIVING PASSENGERS BAGGAGE

This Chapter focuses on standards related to customs and border-control for arriving passenger baggage, including the usage of CCTV, X-ray scanning, detection systems and artificial intelligence. Aviation-security screening standards, typically within the framework of ISO, IEC, CEN, CENELEC, DIN/DKE, WCO, ICAO, ECAC, EU and selected national frameworks, are included when they shape equipment performance, procurement, testing or interoperability.

The table below presents a mapping of the domain according to the relevant standards landscape.

Please note that although this research is extensive, there could be related or secondary standards that are not included due to the complexity and breadth of what exists.

Table 7-1: Relevant standards landscape by domain and issuing organisation

	ISO	IEC / CENELEC	CEN / DIN	WCO / ICAO / ECAC	EU / national
X-ray /CT equipment safety	ISO 12100 ISO 14971 analogy	IEC 61010-2-091 IEC 62463 IEC 62523	DIN EN IEC adoption	WCO NII Guidelines	Radiation laws
CCTV / video systems	ISO 22311 ISO/IEC 22989	IEC 62676 series	DIN EN IEC 62676	CAO Annex 17 context	GDPR / Policy rules
AI governance	42001 23894	IEC participation via JTC	CEN-CLC/JTC 21 DIN/DKE roadmap	WCO AI practice	EU AI Act
Customs risk & NII	ISO 31000 support	NII systems interfaces	Procurement specs	WCO SAFE + NII Data Model	WCC / national customs
Aviation screening performance				ECAC CEP EDS Standard 3/3 x EDSCB C1-C3	Reg. 2015/1998
Cybersecurity/privacy	ISO/IEC 27001 27701	IEC 62443	EN adoptions airport security programs	EN adoptions airport security programs	NIS2, CRA, GDPR

7.1.1 Standardisation Summary

The standardisation picture is not governed by a single airport customs baggage standard. It is a complex, layered regime:

- Customs administrations rely on WCO instruments for risk management, non-intrusive inspection (NII), data and mutual recognition;
- Safety and technical conformity of X-ray or CT equipment rely heavily on IEC/EN/DIN standards;
- CCTV and video-surveillance interoperability relies on ISO 22311 and the IEC 62676 family;
- AI governance increasingly relies on ISO/IEC JTC 1/SC 42 standards and European harmonised standards being prepared by CEN-CENELEC/JTC 21 under the EU AI Act.

The most important development since 2023 is the move from equipment-only specifications to system governance. The arrival of ISO/IEC 42001:2023 for AI management systems, ISO/IEC 23894:2023 for AI risk management, IEC 62676-5-1:2024 and IEC 62676-4:2025 for video surveillance performance and application guidance, and IEC 62463:2024 for X-ray personnel screening means that airport customs programmes now need auditable management systems, data-quality controls, monitoring of model drift, cybersecurity controls and human oversight - not only purchase specifications for scanners.

The second major development is the migration from 2D operator-reviewed X-ray images to CT, multi-view and AI-assisted image analytics. For customs, this does not replace officer discretion. The emerging good practice is to use AI as a decision-support layer that highlights anomalies, object classes or contraband patterns while preserving officer accountability, keeping audit logs and maintaining independent image review processes.

The third development is regulatory convergence. In Europe, AI systems used by or on behalf of public authorities for border-control risk assessment may fall within high-risk categories under the EU AI Act. CEN-CENELEC/JTC 21 is developing harmonised standards for risk management, quality management, data governance, transparency, human oversight, accuracy, robustness and cybersecurity. These standards are highly relevant even where the customs authority is outside the EU, because global scanner and analytics suppliers will increasingly design to these requirements.

Finally, customs requirements have become more security sensitive. Scanner images, CCTV streams, risk indicators and passenger data provide critical border-security data. Customs should require secure-by-design architecture, vulnerability management, logging, retention controls, model-performance evidence, open interfaces where feasible, and clear separation between aviation-security screening and customs enforcement use cases.

7.1.2 Key Findings

No single ISO, CEN or DIN standard fully specifies customs control of arriving passenger baggage; compliant systems are assembled from several standard families.

WCO SAFE and the WCO NII Guidelines remain the primary customs-specific standards for use of scanning technology and risk management.

IEC 61010-2-091 is central for cabinet X-ray equipment safety; IEC 62523 covers higher-energy cargo/vehicle systems; IEC 62463:2024 covers X-ray systems for screening persons.

IEC 62676 is the current anchor family for CCTV/video surveillance systems in security applications, with important 2024-2026 updates for camera performance, VMS/cloud profiles, application guidelines and intelligent video analysis.

AI deployments should be specified against ISO/IEC 22989, 23053, 23894 and 42001, and in Europe mapped to CEN-CENELEC/JTC 21 harmonised standards under the EU AI Act.

ECAC CEP and EU aviation-security rules are not customs standards, but they influence airport scanner capability, especially EDS Standard 3.x and EDSCB C1-C3 equipment

7.2 SCOPE AND OPERATING CONTEXT

Arriving-passenger baggage customs control is a border-control function. This control aims to detect undeclared or prohibited goods, narcotics, weapons, protected wildlife, food and agricultural items, currency, excise goods, sanctions-controlled goods and other contraband, as per country requirements. In an airport, this function intersects with but is not identical to aviation security. Aviation security normally screens passengers and cabin baggage before departure to protect civil aviation. Customs control on arrival normally selects passengers and baggage for inspection after landing and before exit from the customs-controlled area.

For standards purposes this distinction matters. Aviation security has detailed confidential performance standards for explosive detection and cabin baggage screening. Customs standards are more risk-management oriented and less prescriptive at the device-performance level. Customs administrations therefore combine customs instruments, radiation-safety standards, equipment-safety standards, privacy law, cybersecurity rules and procurement standards, (see Figure 7-1)

We are treating CCTV, X-ray scanning, detection systems and AI as parts of one socio-technical control system. In modern airports, the operational chain combines pre-arrival data, behavioral observation, queue and hall monitoring, green/red channel controls, image interpretation, trace detection, canine teams, hand search, seizure workflow and case-management systems. The trend is toward data fusion, automated triage and risk-based inspection, while maintaining human responsibility for coercive decisions.

Reference Architecture: customs control of arriving passengers baggage

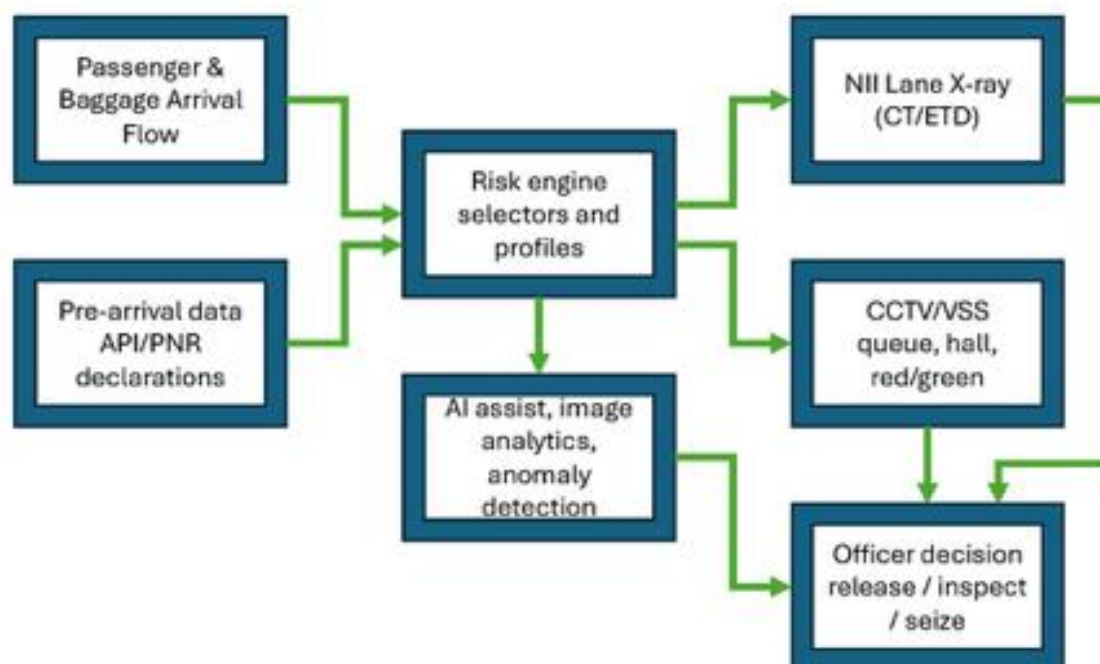


Figure 7-1: Reference Architecture for arriving passengers' baggage customs control

7.3 CUSTOMS-SPECIFIC STANDARDS AND GUIDANCE

7.3.1 WCO SAFE Framework and NII

The World Customs Organization (WCO) remains the central standards organisation for customs control. The SAFE Framework of Standards includes a standard on modern technology in inspection equipment, stating that non-intrusive inspection equipment and radiation detection equipment should be available and used for inspection. The framework is primarily designed for global supply-chain security, but its principles - risk management, advance information, customs-to-customs cooperation, and use of modern inspection technology - apply directly to airport baggage control when customs administrations select persons or baggage for inspection.

The WCO NII Guidelines, updated in 2025, define NII technology as equipment such as X-ray or gamma-ray imaging that allows inspection without opening cargo or unloading the means of transport. While the published definition is cargo-oriented, the operational principles are transferable to passenger baggage which entails needs assessment, procurement planning, performance evaluation, radiation safety, maintenance, training, image analysis, data handling, governance and lifecycle management. For customs programmes, the Guidelines are a practical bridge between high-level policy and equipment procurement.

7.3.2 WCO Data Model, API, PNR and Targeting

Arriving passenger baggage control increasingly begins before landing. API, interactive API and PNR data allow border authorities to perform risk assessment before the passenger reaches the customs

hall. The WCO Data Model provides harmonised data definitions and messages for customs and other cross-border regulatory agencies. IATA, ICAO and WCO passenger data standards are therefore relevant to baggage control because they shape the inputs to targeting engines that decide who or what will be scanned or inspected.

The standards issue is not simply message format. Customs authorities need data-quality controls, role-based access, retention periods, audit trails, and safeguards against discriminatory risk profiles. Where AI or machine learning is used to derive risk indicators, the system should be governed as an AI-supported risk-management process, not only as a database query.

7.3.3 Detection Systems Beyond X-Ray

Airport customs detection systems may include explosive trace detection, narcotics trace detection, radiation portal monitors, handheld isotope identifiers, metal detection, currency detection, chemical sensors, canine units and manual inspection tools. There is no single cross-modal customs standard for all such systems. Procurement usually references instrument-specific IEC, ISO, ASTM, national metrology or regulatory requirements, combined with local acceptance testing and customs operating procedures. The standardisation gap is strongest in AI-assisted contraband recognition for passenger baggage: common public benchmarks, data sets and acceptance metrics remain immature.

7.4 X-RAY, CT AND RADIATION-PROTECTION STANDARDISATION

7.4.1 Cabinet X-Ray Systems

For conventional baggage scanners, IEC 61010-2-091:2019 is a key equipment safety standard. It specifies particular safety requirements for cabinet X-ray systems and supplements IEC 61010-1. It is relevant to baggage and parcel scanners because these systems combine electrical, mechanical, conveyor and ionising-radiation hazards. European and national adoptions, such as EN IEC and DIN EN IEC versions, are usually the route through which the standard becomes embedded in procurement and conformity assessment.

Customs normally requires compliance evidence for electrical safety, radiation shielding, interlocks, emergency stops, conveyor safety, leakage radiation, warning indicators, servicing controls and operator documentation. Customs normally also requires acceptance testing after installation and periodic inspection under national radiation-protection law.

7.4.2 Personnel and Cargo/Vehicle Systems

IEC 62463:2024 concerns X-ray systems for the security screening of persons and provides radiation-protection requirements and test methods for persons screened, people nearby and operators. It is more relevant to body/person screening than baggage, but it matters where customs or border police consider backscatter, transmission or combined systems to detect concealed goods on persons. In Europe, use of ionising radiation on people is subject to strict justification and national law, so this standard does not itself authorise deployment.

IEC 62523:2010 applies to radiographic inspection systems with photon radiation energy of at least 500 keV for cargo, vehicles and cargo containers. Its direct relevance to passenger baggage is limited because airport baggage scanners are usually lower-energy cabinet systems. It is relevant at airports for air cargo, aircraft containers, vehicles and large consignments under customs control. A second edition project is visible in standards-development channels, suggesting continued evolution of this area.

7.4.3 CT and Multi-View Imaging

Computed tomography (CT) is the dominant advanced imaging trend. In aviation security it supports automated explosive detection and richer 3D operator review. In customs control it supports denser object separation, material discrimination and AI feature extraction. However, CT performance standards for customs contraband detection are not as public or mature as ECAC aviation-security performance standards.

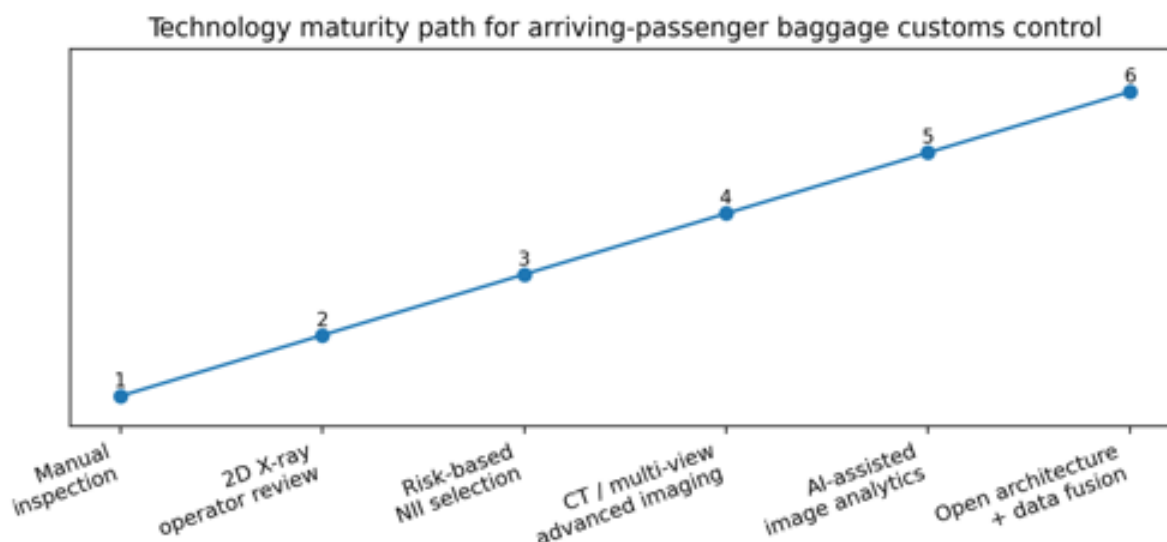


Figure 7-2: Maturity path from manual inspection to AI-assisted data fusion

7.5 AVIATION-SECURITY STANDARDS AFFECTING AIRPORT BAGGAGE SCANNERS

7.5.1 4.1 ECAC CEP and EDS/EDSCB

The European Civil Aviation Conference Common Evaluation Process (ECAC CEP) is a laboratory testing programme used by ECAC Member States to assess aviation-security equipment against ECAC/EU performance standards. It covers equipment such as explosive detection systems for hold baggage and explosive detection systems for cabin baggage. ECAC approval is not a customs approval, but it strongly influences the scanner market and the equipment installed in airports.

The key aviation-security categories are EDS for hold baggage and EDSCB for cabin baggage. EDS Standard 3 and newer 3.x levels concern hold-baggage explosives detection. EDSCB C1, C2 and C3 concern cabin-baggage screening. C3 systems are associated with advanced CT capability allowing large electronic devices and liquids to remain in bags under certain regulatory conditions.

7.5.2 EU Aviation-Security Implementing Rules

Commission Implementing Regulation (EU) 2015/1998 and associated confidential measures define common aviation-security measures in the EU, including methods for cabin-baggage screening such as hand search, X-ray equipment, EDS, explosive detection dogs and ETD equipment. These rules also include operational requirements for X-ray and EDS image review, such as limits on continuous image-review time in the public text.

7.6 CCTV AND VIDEO-SURVEILLANCE STANDARDISATION

7.6.1 ISO 22311 and Export Interoperability

ISO 22311:2012 specifies a common output file format for video-surveillance contents so that exported video, audio and metadata can be replayed and processed. Its importance for customs is evidential. CCTV footage from the baggage reclaim belt, customs channel, inspection bench or baggage X-ray lane may later be needed for prosecution, internal review or cooperation with police. Export interoperability reduces dependence on proprietary viewers and helps preserve context metadata.

7.6.2 IEC 62676 Family

The IEC 62676 series is the main international family for video surveillance systems used in security applications. Recent developments are particularly relevant. IEC 62676-2-11:2024 defines minimum profiles for video management systems and cloud video-surveillance-as-a-service systems. IEC 62676-5-1:2024 defines measurement methods for camera-equipment performance and image-quality tests. IEC 62676-4:2025 provides application guidelines for planning, design, installation, testing, commissioning and maintenance of video surveillance systems. IEC 62676-6:2026 addresses real-time intelligent video analysis in surveillance systems, including functions, performance, interfaces, environmental adaptability, test methods and grading rules.

For airports, these updates shift CCTV procurement from a camera-count exercise to a performance-based design exercise.

7.6.3 DIN and CENELEC Adoption

In many European countries, IEC surveillance standards are implemented through EN and national adoptions such as DIN EN IEC 62676. This matters for procurement: tenders should specify the exact edition and adoption path, for example DIN EN IEC 62676-4 for application guidance once adopted, not simply “CCTV to standard”. National data-protection and police/customs evidence rules must still be applied.

7.6.4 CCTV Analytics

Video analytics at customs arrival halls can support queue management, abandoned-object alerts, red/green channel monitoring, restricted-area intrusion detection and post-event investigation. Biometric identification or behavioral risk scoring is much more sensitive. Under European law and many national regimes, facial recognition, remote biometric identification or automated risk scoring in border-control contexts triggers high legal scrutiny. Standards can help specify quality and governance, but they do not remove the need for a legal basis, necessity and proportionality assessment, data protection impact assessment and human oversight.

7.7 ARTIFICIAL INTELLIGENCE STANDARDS AND AI STANDARDISATION ACTIVITY

7.7.1 ISO/IEC JTC 1/SC 42 Standards

The core AI standards for customs baggage-control systems are horizontal rather than airport-specific. ISO/IEC 22989:2022 establishes AI terminology and concepts. ISO/IEC 23053:2022 provides a framework for AI systems using machine learning. ISO/IEC 23894:2023 provides guidance on AI risk management. ISO/IEC 42001:2023 is the first AI management system standard and specifies

requirements for establishing, implementing, maintaining and continually improving an AI management system. These standards are directly relevant to AI-assisted image analytics, risk-scoring systems, CCTV analytics and data-fusion platforms used by customs.

For a customs authority, the practical value of ISO/IEC 42001 is that it creates an auditable management layer: AI policy, roles and responsibilities, risk assessment, impact assessment, data governance, supplier management, monitoring, incident handling and continual improvement. ISO/IEC 23894 complements this by giving risk-management guidance for AI-specific risks such as bias, data drift, lack of explainability, over-reliance by users, cyber manipulation, model degradation and emergent behavior.

7.7.2 CEN-CENELEC/JTC 21 and the EU AI Act

CEN-CENELEC/JTC 21 is developing European AI standardisation deliverables to support the EU AI Act. Its purpose is to produce standards for the European market, including harmonised standards that may provide presumption of conformity when cited in the Official Journal of the European Union. The standardisation request covers requirements such as risk management, data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness, cybersecurity and quality management. CEN and CENELEC announced measures in October 2025 to accelerate delivery of key standards under JTC 21 and the AI standardisation request.

The EU AI Act is relevant to customs because AI systems used by or on behalf of public authorities in migration, asylum and border-control management to assess risks posed by natural persons may be classified as high-risk. Even when a customs use case is framed as goods control, if the AI system evaluates a passenger for inspection, the fundamental-rights and border-control implications are clear. Procurement should therefore assume that AI-assisted passenger targeting and AI-assisted baggage image triage require high-risk-style controls unless legal analysis proves otherwise.

7.7.3 DIN/DKE AI Roadmap

DIN and DKE have developed a German Standardisation Roadmap on Artificial Intelligence. The roadmap addresses terminology, AI methods, imaging sensor technology, data quality, trustworthiness, ethics, safety and security. For customs this is useful because it highlights a practical standardisation gap: sector-specific AI quality requirements for sensor-driven inspection systems remain underdeveloped. Germany's roadmap approach supports the creation of use-case-specific profiles built on horizontal ISO/IEC and CEN-CENELEC standards.

7.7.4 NIST and Other Non-European Frameworks

NIST's AI Risk Management Framework is widely used and aligns conceptually with ISO/IEC 23894. It can help customs buyers structure governance around validity, reliability, safety, security, resilience, accountability, transparency, explainability, privacy and fairness.

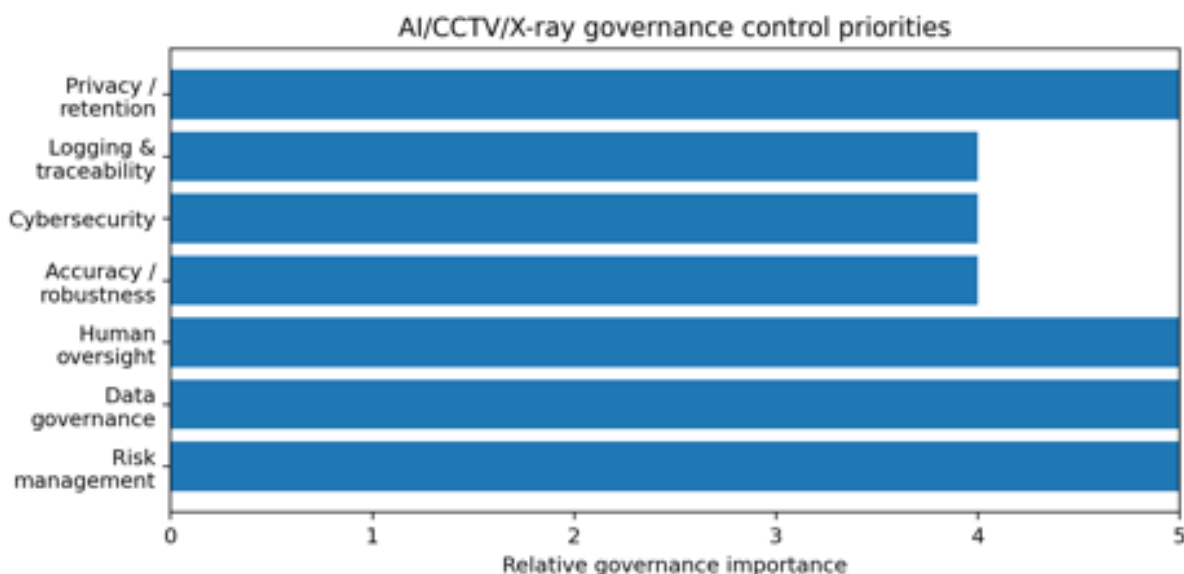


Figure 7-3: Governance control priorities for AI, CCTV and X-ray systems

7.8 STANDARDS MATRIX

Standard / instrument	Main subject	Use in airport-arrival customs baggage control
WCO SAFE Framework of Standards	Customs risk management and modern inspection technology	Primary customs framework; supports NII and radiation detection availability.
WCO NII Guidelines 2025	Non-intrusive inspection procurement, deployment and operation	Best available customs-specific guidance for scanner lifecycle and governance.
WCO Data Model	Standardized customs and border definitions/messages	Supports API/PNR/declaration integration and targeting data quality.
ICAO Annex 17 / Doc 8973 context	Aviation security safeguards	Relevant to airport environment; detailed security manual is restricted.
ECAC Common Evaluation Process	Testing aviation-security screening equipment	Important market and procurement influence; not customs contraband certification.
EU Reg. 2015/1998	Common aviation-security measures	Includes allowed cabin-baggage screening methods and operational controls.

Standard / instrument	Main subject	Use in airport-arrival customs baggage control
IEC 61010-2-091:2019	Cabinet X-ray equipment safety	Core for baggage/parcel scanner electrical, mechanical and radiation safety.
IEC 62463:2024	X-ray systems for screening persons	Relevant when customs considers person-screening systems using ionising radiation.
IEC 62523:2010	Cargo/vehicle radiographic inspection systems	Relevant for air cargo, vehicles and high-energy systems at airports.
ISO 22311:2012 / EN ISO 22311:2014	Video-surveillance export interoperability	Supports evidential export of CCTV/video with metadata.
IEC 62676-2-11:2024	VMS and VSaaS profiles	Supports interoperability of video management and cloud surveillance.
IEC 62676-5-1:2024	Camera performance measurement	Enables objective image-quality testing.
IEC 62676-4:2025	VSS application guidelines	Planning, design, installation, testing, commissioning and maintenance.
IEC 62676-6:2026	Intelligent video analysis	Emerging anchor for real-time intelligent video analytics performance.
ISO/IEC 22989:2022	AI concepts and terminology	Common vocabulary for AI procurements and policies.
ISO/IEC 23053:2022	ML-based AI system framework	Useful for documenting model components and lifecycle.
ISO/IEC 23894:2023	AI risk management	Risk identification, analysis, treatment and monitoring for AI.
ISO/IEC 42001:2023	AI management system	Auditable management system for organisations using or providing AI.
CEN-CENELEC/JTC 21 deliverables	European AI Act harmonised standards	Expected to shape high-risk AI conformity in Europe.

Standard / instrument	Main subject	Use in airport-arrival customs baggage control
ISO/IEC 27001 / 27701	Information security and privacy management	Baseline controls for scanner images, CCTV, targeting data and logs.
IEC 62443 series	Industrial automation/security controls	Useful where scanning equipment resembles networked operational technology.
GDPR / Law Enforcement Directive / national customs law	Privacy and law-enforcement data processing	Legal controls for CCTV, passenger data, biometric or AI-supported decisions.

7.9 PROCUREMENT AND ACCEPTANCE-TESTING IMPLICATIONS

Procurement should be written as a standards profile rather than a single compliance statement. The profile should separate mandatory legal conformity, desired interoperability, operational performance and governance evidence. For example, a baggage scanner tender can require IEC 61010-2-091 compliance, national radiation approval, cybersecurity hardening, image export format, operator training, maintenance support, AI model documentation, and local acceptance tests using customs target objects.

Acceptance testing should include factory acceptance, site acceptance, radiation survey, image-quality verification, throughput testing, fail-safe testing, network and logging checks, user-role tests, privacy configuration, and operational trials. For AI, it should also include baseline performance on representative local data, false-positive/false-negative analysis, subgroup or route bias review where passenger data is used, alert explainability, audit-log review, model version control and drift monitoring plan.

7.9.1 Recommended Tender Clauses for Customs

- Equipment shall comply with applicable IEC/EN/DIN safety standards, national radiation-protection law and airport safety requirements.
- Video systems shall support export interoperability and provide time-synchronised metadata suitable for evidence handling.
- AI-enabled functions shall be documented under an AI management and risk-management framework aligned with ISO/IEC 42001 and ISO/IEC 23894.
- The supplier shall provide model versioning, audit logs, performance evidence, known limitations, cybersecurity update processes and incident-reporting arrangements.
- The system shall preserve human authority: AI outputs are recommendations or cues unless a lawful automated decision basis is explicitly approved.

- The system shall support data minimisation, retention limits, role-based access, encryption in transit and at rest, and deletion/export logs.
- The authority shall have contractual rights to independent testing, vulnerability disclosure handling and post-deployment performance review.

7.10 DATA PROTECTION, FUNDAMENTAL RIGHTS AND EVIDENCE

CCTV footage, scanner images, risk scores, passenger declarations and officer notes can become personal data and law-enforcement data. Standards cannot replace legal basis, proportionality and necessity. In the EU and EEA context, customs and border authorities must map processing to the GDPR, Law Enforcement Directive implementation, customs legislation and national security exceptions. In Switzerland and other jurisdictions, equivalent national privacy and police/customs data laws apply.

The most sensitive deployments are biometric identification, behavior analytics, passenger risk scoring, and AI systems that recommend intrusive inspections. The safest design principle is “human-in-the-loop with accountable discretion”: AI may prioritise, highlight or support, but the officer records the grounds for action and remains able to disregard the AI output. This is also operationally sound because AI image classifiers can fail on new concealment techniques, novel packaging, adversarial placement and distribution shifts from local travel patterns.

For evidence, systems should preserve chain of custody. CCTV and scanner exports should include time stamps, device identity, operator identity, hash values or integrity controls, case number, export reason and retention metadata. ISO 22311 and IEC 62676 interoperability concepts should be treated as evidence-management requirements, not merely technical convenience.

7.11 STANDARDISATION GAPS AND EXPECTED DEVELOPMENTS

The main gap identified is the absence of a public, customs-specific, performance-based standard for AI-assisted contraband detection in passenger baggage. Aviation security has ECAC-style performance testing for explosives threats; customs contraband is more diverse and jurisdiction-specific. A future standard could define test-set governance, target categories, concealment scenarios, performance metrics, operational trial design, data protection controls and human oversight requirements.

A second gap is interface standardisation between scanner images, CCTV, targeting systems and case-management tools. Proprietary formats create lock-in and make cross-border cooperation harder. Open interfaces, standard metadata and export packages would improve auditability and evidence handling.

A third gap is post-market monitoring for AI in inspection systems. Customs authorities need practical metrics: model drift, false alarms by route or commodity, missed-detection review, operator override rates, alert fatigue, adversarial attempts, and retraining triggers. CEN-CENELEC/JTC 21 and ISO/IEC AI standards will help, but sector-specific profiles are still needed.

Expected developments through 2026-2028 include further European AI Act harmonised standards, national adoption of IEC 62676-4:2025 and IEC 62676-6:2026, continued CT deployment at airports, more AI-assisted X-ray analytics pilots by customs administrations, and stronger cyber/security scrutiny of scanner vendors and cloud-connected video platforms.

7.12 STANDARDISATION CONCLUSIONS

For airport arriving-passenger baggage customs control, the latest standards trend is convergence: customs risk management, X-ray/CT equipment safety, CCTV interoperability, AI governance, cybersecurity and data protection are becoming a single assurance problem. The strongest programmes will not simply buy better scanners. They will build a standards-based control ecosystem with auditable governance, trained officers, validated detection performance, secure data flows and continual improvement.

The recommended approach is to maintain a living standards profile. Start with WCO SAFE, WCO NII Guidelines and the WCO Data Model for customs control; IEC 61010-2-091, IEC 62463 and IEC 62523 for radiation and equipment safety; ISO 22311 and IEC 62676 for CCTV; ISO/IEC 22989, 23053, 23894 and 42001 for AI; CEN-CENELEC/JTC 21 and DIN/DKE activities for European AI standardisation ; and EU/national legal requirements for aviation security, privacy, radiation and border-control decisions. Then convert that profile into procurement clauses, acceptance tests, SOPs and audit evidence.

8 SECOND BAG-INTEL STANDARDS SURVEY

The BAG-INTEL project conducted a second stakeholder survey to further identify standards, standardisation gaps, and future priorities relevant to intelligence-led customs and law-enforcement activities – and this was designed as based upon the results of the first BAG-INTEL standards survey. This second survey is attached as Annex I. This report provides a comprehensive assessment of stakeholder responses regarding standards relevant to the BAG-INTEL project. The analysis identifies priority domains, standards gaps, emerging themes, and recommendations for future European standardisation activities.

8.1 OBJECTIVES OF THE SURVEY

The objective of this second survey was to gather feedback from the wide community of key stakeholders so as to:

- Identify standards currently used by stakeholders,
- Assess awareness of relevant standards,
- Identify areas where standards are missing or insufficient,
- Determine future priorities for standardisation ,
- Collect expert recommendations.

8.2 METHODOLOGY

8.2.1 Survey Design

The survey was designed to target the key stakeholder community. It was anonymous, short (7 questions) and it was created on the EU survey platform. This survey expanded the breadth and depth of the topic areas relevant to BAG-INTEL. The survey focused on standards associated with:

- Artificial Intelligence,
- Data Mining
- Knowledge Management,
- Risk Assessment,
- Detection Technologies,
- CCTV Systems
- Customs and Law Enforcement Data Exchange,
- Interoperability Frameworks.

8.2.2 Targetting the Stakeholder Community

The survey was widely circulated to the stakeholder groups as identified and described in detail in BAG-INTEL Deliverable D6.3, Section 6.1 and 6.2. In short, the stakeholder group included customs authorities, law enforcement agencies, government agencies, research institutes and universities, consultants, technology providers, EU policy makers and other stakeholders involved in security, customs and intelligence operations. The Survey, which was also distributed to all members of the Consortium, was widely distributed to focused contacts on Linked In, to EU customs authorities and BAG-INTEL contacts. The survey was launched on 23 March 2026 until 9 June 2026 and, in total, 88 replies were received.

8.2.3 Methodology for Analysis

Survey responses were reviewed question-by-question. Closed questions were analyzed quantitatively. Free-text responses were reviewed qualitatively to identify recurring themes, standards-reference extraction and recommendations.

Analysis separated the survey into five blocks: respondent profile, important areas, known/used standards, areas lacking standards, and standardisation efforts/status.

Interpretation focused on signals useful for project deliverables: priority setting, standards mapping, stakeholder engagement, and roadmap design.

The analysis combined:

- Descriptive statistics
- Comparative analysis
- Gap analysis
- Thematic coding of qualitative responses

8.3 ANALYSIS OF REPLIES TO SURVEY

8.3.1 Question 1 -Identifying the Type of Stakeholder Respondent

Survey Question 1: Identifying the respondents “What type of organisation do you represent?”

- Customs,
- Law Enforcement,
- Government Agency,
- Equipment Manufacturer,
- Technology Provider (including software),
- Consultant / Consulting,

- Services Provider,
- European Institutions (European Commission, etc. – which one (fill in)),
- Other (please note the type of organisation – fill in).

The stakeholder groups which responded to our second BAG-INTEL survey were composed of:

1. Customs (~26 respondents)
2. Law Enforcement (~14)
3. Technology Providers (~13)
4. Consultants (~12)
5. Government Agencies and EU institutions (~8)
6. Equipment Manufacturers (~7)
7. Services Provider (~3)
8. Other (~2)

Q1 respondent profile: broad but operationally weighted

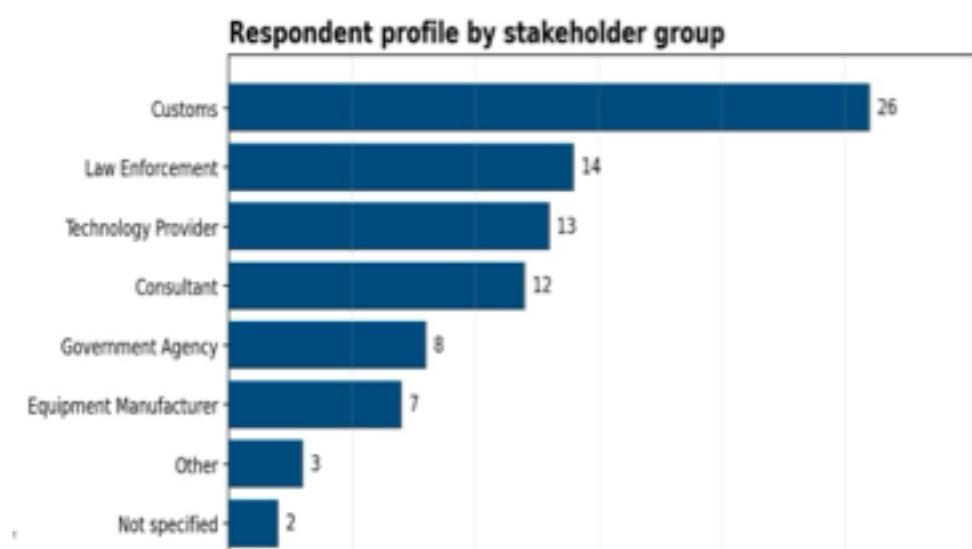


Figure 8-1: Replies received according to stakeholder group

From the replies,

- **Customs** was the largest respondent group representing a strong operational/end-user perspective.

- **Law enforcement, technology providers, consultants and equipment manufacturers** closely followed which had the value of adding implementation, supplier and advisory viewpoints
- **Government agencies and European institutions added the policy elements.**

Table 8-1: Stakeholder groups and their roles

Group	What they add
Customs	Operational pain points and cross-border needs
Law enforcement	Investigative and prosecutorial data-sharing needs
Technology providers / manufacturers	Implementation constraints, interfaces and product standards
Government / EU institutions	Policy alignment and regulatory legitimacy
Consultants and services providers	Market, compliance and process perspective
University	Research

The survey, thus, achieved broad representation across operational, technical, policy, and academic communities. This mix provided useful feedback in particular for standards work because it combined operational need, technical feasibility and policy relevance, i.e., the survey had sufficient operational input to support project-level standardisation recommendations.

8.3.2 Question 2 -Priority Areas for Standardization in Current Environment

Survey Question 2: In your opinion, standardisation is important in which of the following areas (more than one answer is possible):

- CCTV Systems and the images and files generated
- Artificial Intelligence Systems
- Data Mining / Knowledge Management / Data Processing Systems
- Detection / Scanning Technologies and Systems and the images and files generated
- Customs / Law Enforcement international data sharing
- Customs / Law Enforcement risk assessment
- Other areas (please name the area)

The highest priority areas for standardisation were in the areas below:

1. Customs / Law Enforcement international data sharing (~68 respondents)
2. Detection / Scanning technologies (~59)

3. Customs / Law Enforcement risk assessment (~53)
4. Artificial Intelligence systems (~44)
5. Data mining / knowledge management (~39)
6. CCTV systems (~38)

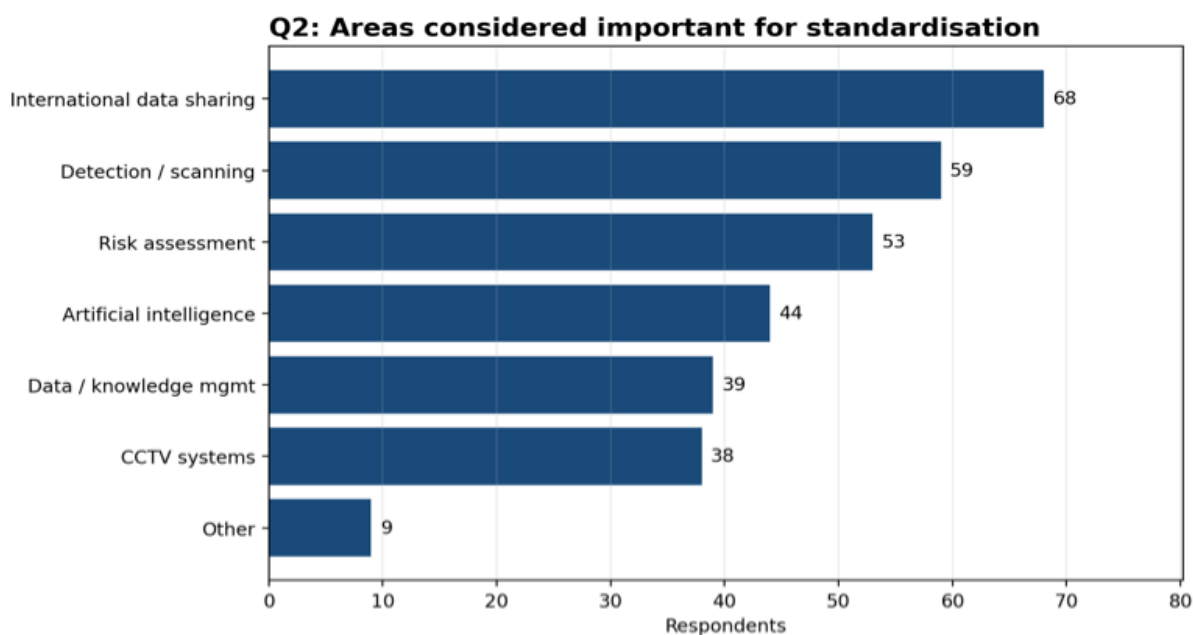


Table 8-2: Areas considered important for standardisation

Whilst the top-ranked area was customs/law-enforcement international data sharing (68), followed by Detection/scanning (59) and risk assessment (53) representing also high-priority operational areas, AI is a major priority (44) and it becomes even more important when combined with the standards-gap question.

The areas of international data sharing, risk assessment, AI systems, detection technologies and data-processing systems are central to future interoperability and intelligence capabilities.

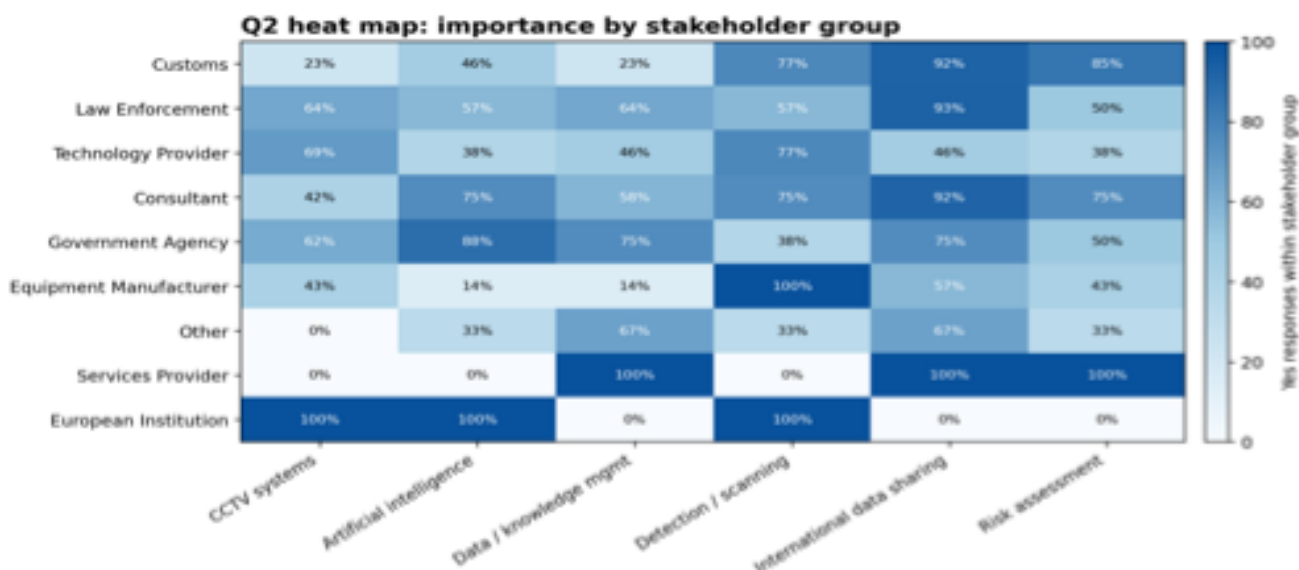


Figure 8-2: Stakeholder heat map showing the importance by stakeholder group

Stakeholders appear to view **cross-border interoperability and intelligence sharing** as the most urgent standardisation challenge, followed closely by technologies that generate **operational intelligence** (scanning, detection, and risk assessment).

The highest-value standardisation work should, therefore, support cross-border operational collaboration, not only stand-alone technical specifications.

Furthermore, detection/scanning standards are important because images, scanner outputs and metadata are core evidence and intelligence sources.

8.3.3 Question 3 -Maturity Awareness of Standards Baseline

Survey Question 3: In which areas do you know about specific standards and/or use standards:

The choice of answers to this question was:

- CCTV Systems and the images and files generated (if known, please name the standard(s))
- Artificial Intelligence Systems (if known, please name the standard(s))
- Data Mining / Knowledge Management / Data Processing Systems (if known, please name the standard(s))
- Detection / Scanning Technologies and Systems and the images and files generated (if known, please name the standard(s))
- Customs / Law Enforcement international data sharing (if known, please name the standard(s))
- Customs / Law Enforcement risk assessment (if known, please name the standard(s))

g. Customs / Law Enforcement other standards (if known, please name the standard(s))

h. Other areas (please name the area and please indicate the standard(s))

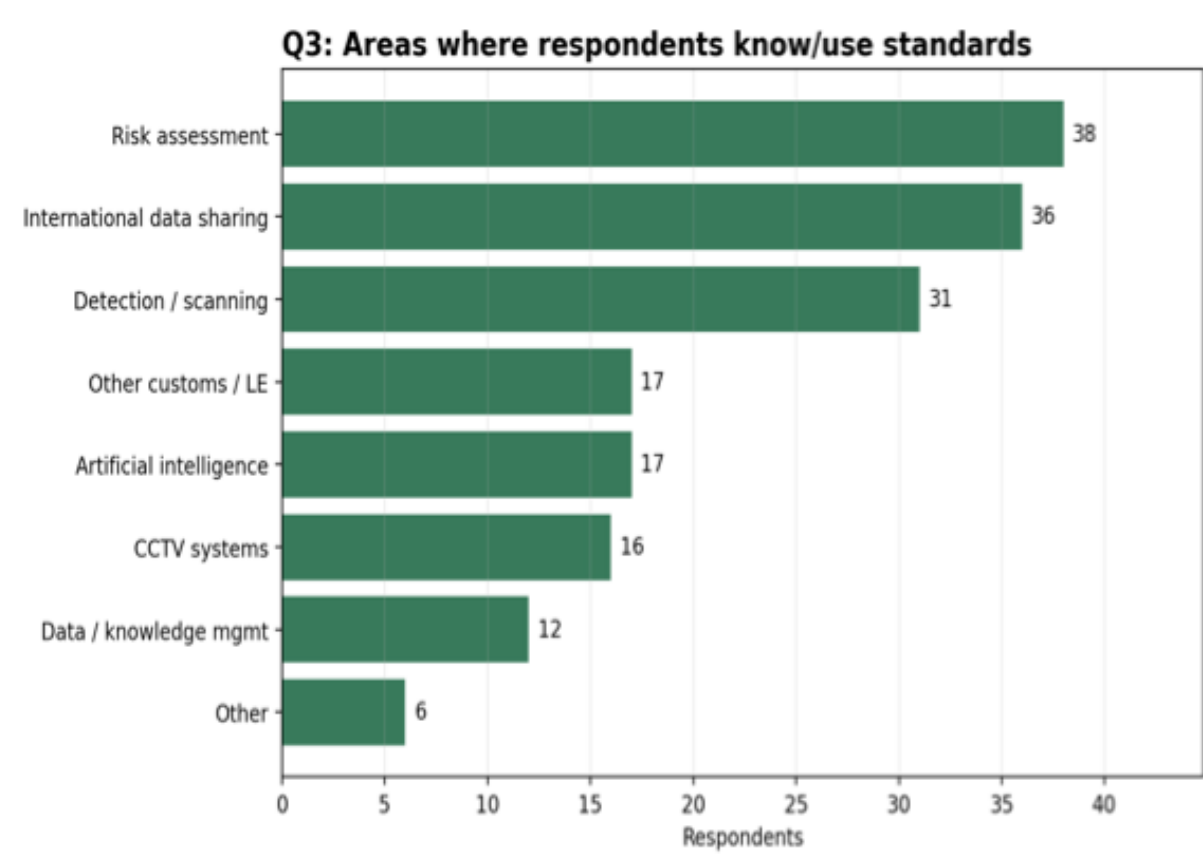


Figure 8-3: Maturity / awareness baseline according to stakeholders replies

Respondents referenced a mix of international standards, EU regulatory frameworks, operational guidance, technical data-exchange formats and sector-specific references. Existing awareness appears strongest in mature operational domains and weaker in AI governance as given in Table 8-3.

Table 8-3: Specific standards referenced by stakeholders

Reference	Mentions
GDPR	9
UFF	6
EU AI Act	5
WCO DM	5
HS Code	5
ISO/IEC 42001	4
CIRAM	4

Reference	Mentions
ECAC	4
SAFE	3
ISO/IEC 27001	3
DICOS	3
eTIR	2
ICS2	2
ISO/IEC 23894	2

Figure 8-3 indicates that:

- Risk assessment and international data sharing have the highest levels of standards awareness/use.
- Detection/scanning also shows meaningful standards awareness.
- AI and data/knowledge management show lower awareness/use compared with their strategic importance, indicating a maturity gap.

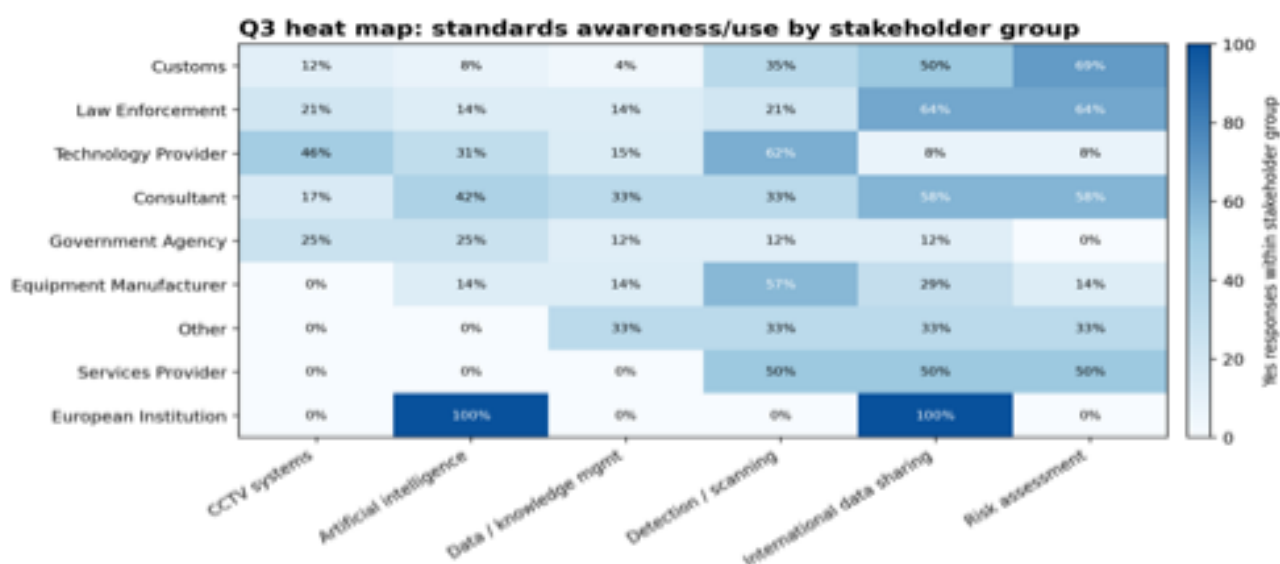


Figure 8-4: Heat map of Standards awareness and usage according to stakeholder group

Key finding Question 3:

Awareness is strongest in mature technical domains and weakest in emerging AI-related domains.

8.3.4 Question 4 -Areas in which Standards are Lacking

Question 4: In your opinion are there any standards that are currently missing from any of the topic areas below or otherwise? And is there any area lacking which needs more immediate attention?

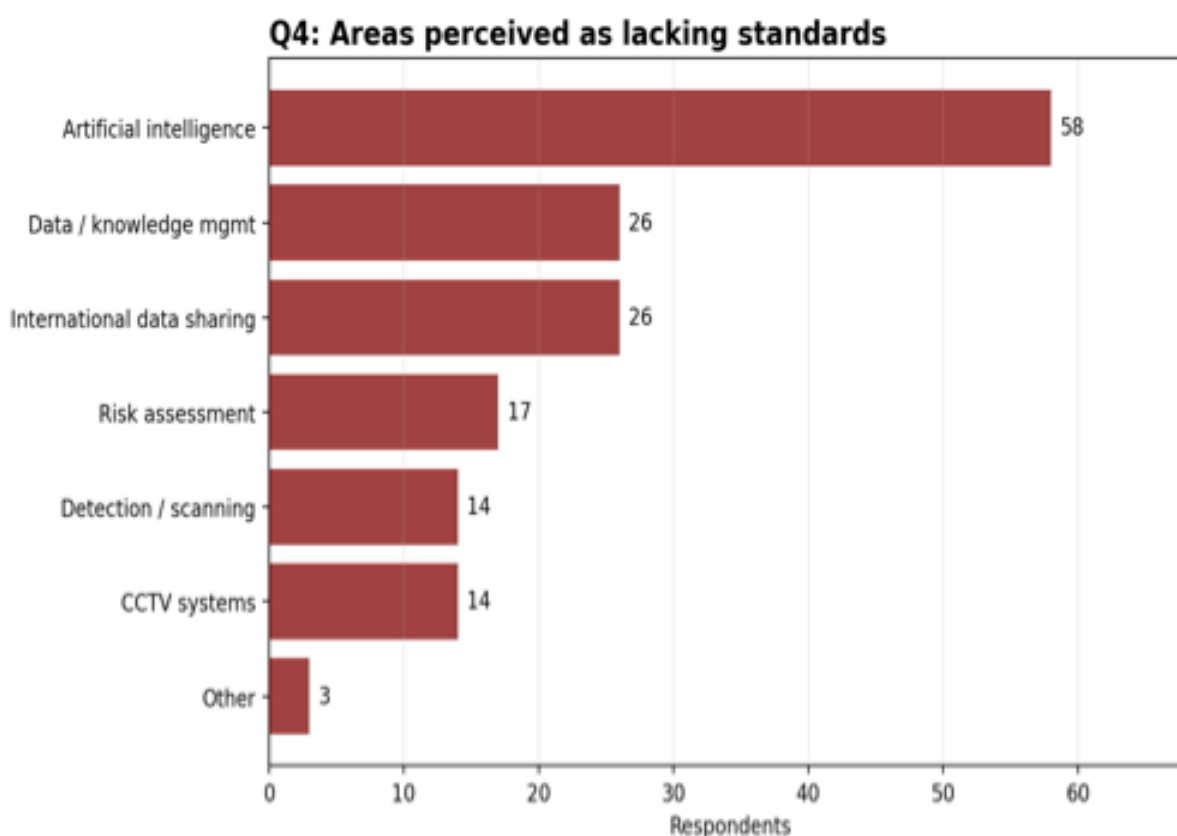


Figure 8-5: Stakeholders' perception of areas which lack standards

The results of the survey as given above indicate that

- AI is the dominant perceived gap (58 of 88), far ahead of every other area.
- Data/knowledge management and international data sharing form a second tier of standards gaps.
- CCTV, scanning and risk assessment are not absent from the gap list, but they are less urgent than AI and cross-border data governance.

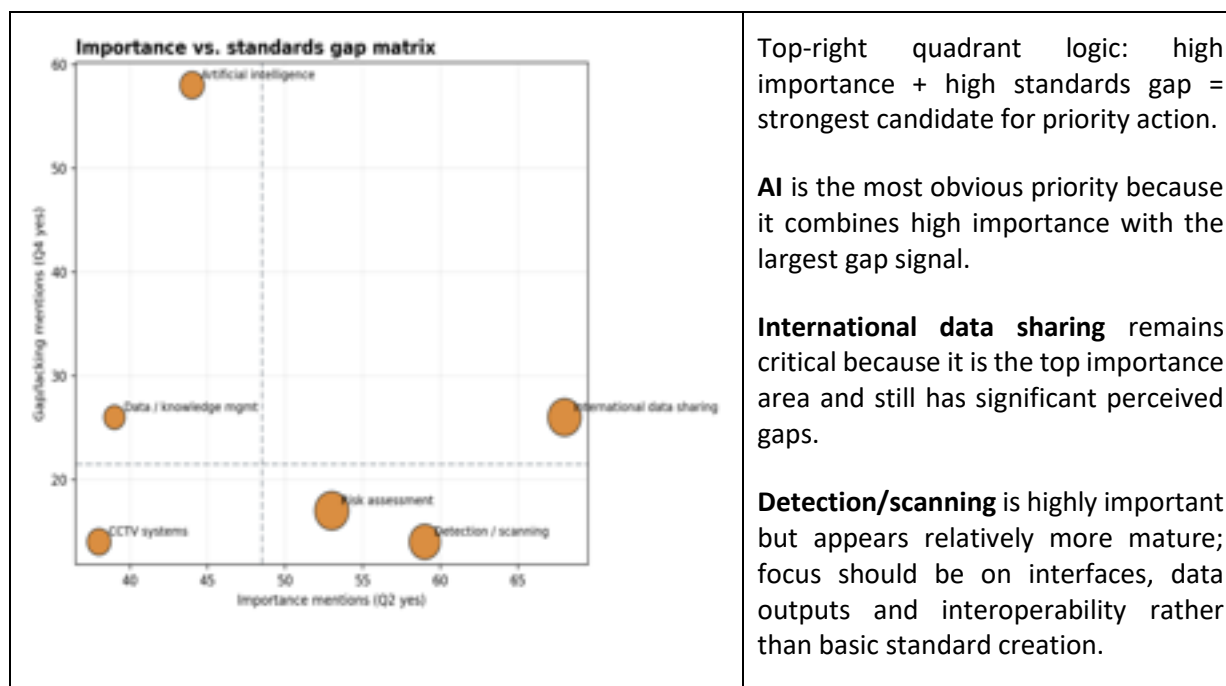
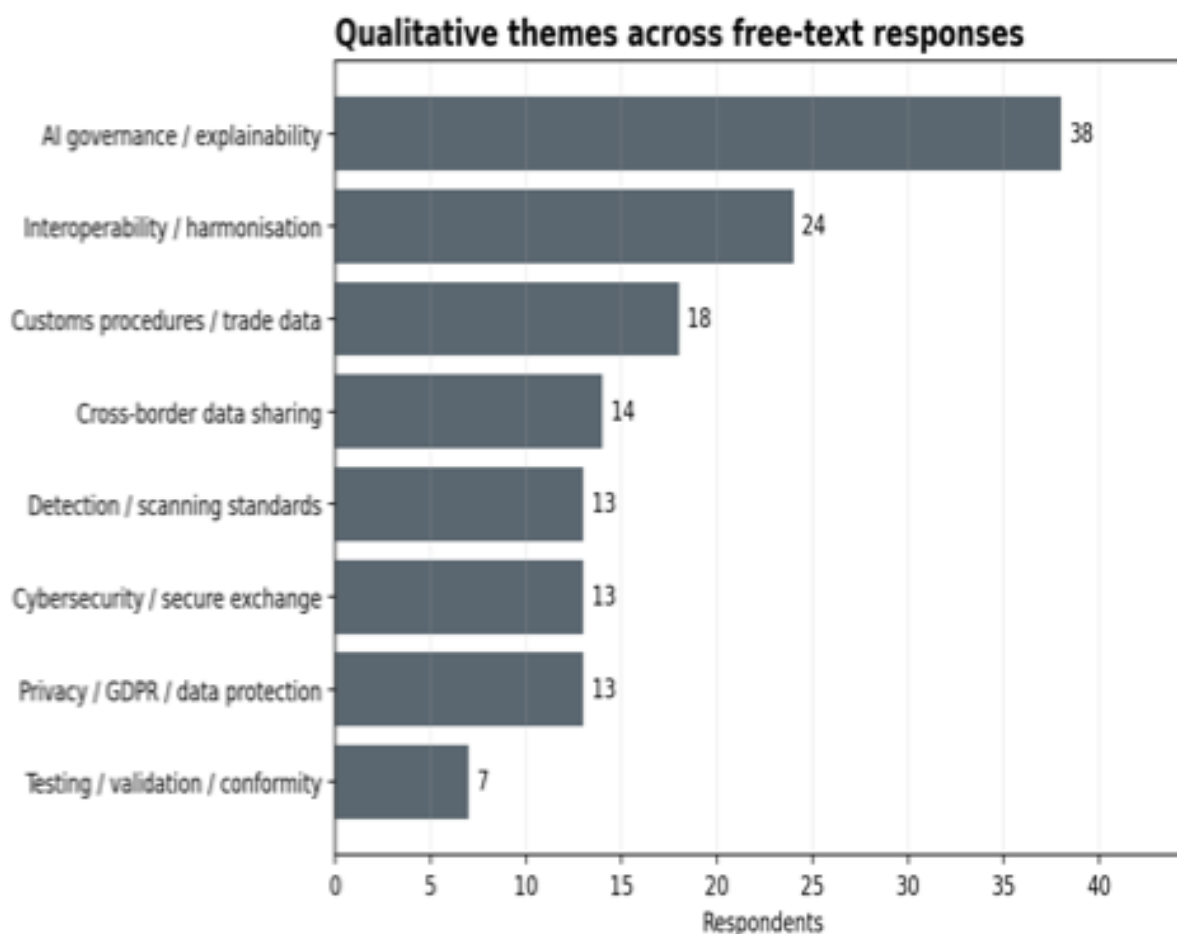


Figure 8-6: Importance vs standards gap matrix



*Figure 8-7: Qualitative themes emerging across the free-text responses***Key findings Question 4:**

- **Artificial Intelligence (AI)** was identified as the highest priority area requiring further standardisation, particularly for law enforcement and customs operations.
- There is a strong need for **harmonised standards** on explainable, transparent, auditable and accountable AI systems to support operational deployment.
- **Cross-border data sharing** between customs and law enforcement remains fragmented, requiring interoperable, secure and legally harmonised frameworks.
- **Common EU-wide risk assessment methodologies** are needed to improve consistency in threat identification and operational decision-making.
- Standards should ensure **vendor-neutral interoperability**, enabling platforms such as BAG-INTEL to integrate with different CCTV, scanner and security systems regardless of manufacturer.
- Additional guidance is needed on **algorithmic accountability, bias testing, human oversight, auditability and compliance** with the AI Act, GDPR, cybersecurity requirements and Fundamental Rights Impact Assessments (FRIAs).
- Respondents highlighted a current **gap in AI-specific customs standards**, noting that harmonised standards supporting the EU AI Act for high-risk customs AI systems are still under development.
- Greater standardisation is needed for **sector-specific data formats, communication protocols and cybersecurity safeguards**, particularly for customs, railway transport and specialized law enforcement equipment.
- Several respondents emphasized the importance of standards for **international trade compliance**, customs declarations, image sharing, transit goods controls, intellectual property protection and global trade management systems.

Overall, respondents agreed that **AI, data sharing, interoperability and risk assessment** represent the most urgent priorities for future European and international standardisation efforts supporting projects such as BAG-INTEL.

8.3.5 Question 5 - Known Areas of Standardisation Efforts

Question 5: Are you aware of and / or participate in any standardisation or pre-standardisation development efforts related to any of the topics and areas mentioned below? If so, name which topic areas are involved and if possible provide a very short sentence about the current status of these efforts.

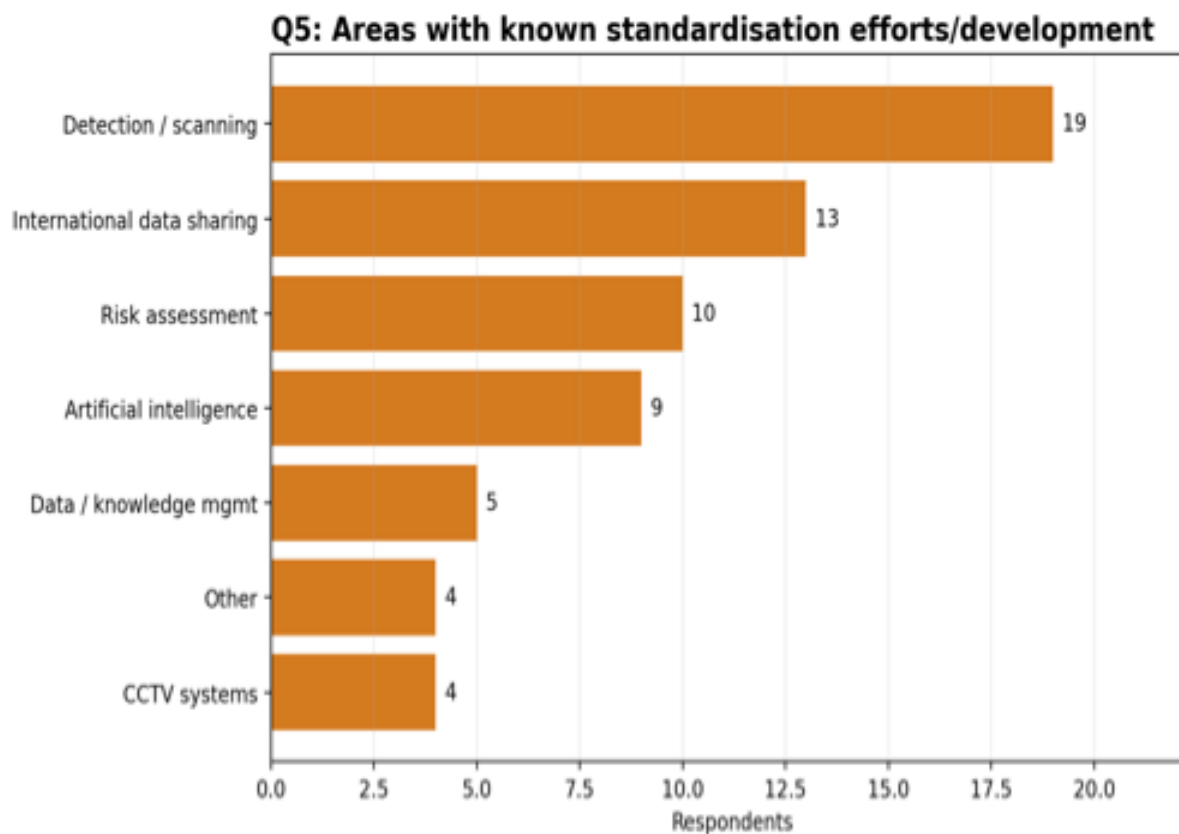


Figure 8-8: Known areas of standardisation efforts

The respondents replies indicated that:

- Detection/scanning and international data sharing show the strongest signals of ongoing or known standardisation activity.
- AI has a lower “in development” signal than its gap signal, suggesting uncertainty among stakeholders about emerging AI standardisation pathways.

Key finding Question 5:

Awareness is strongest in mature technical domains and weakest in emerging AI-related domains.

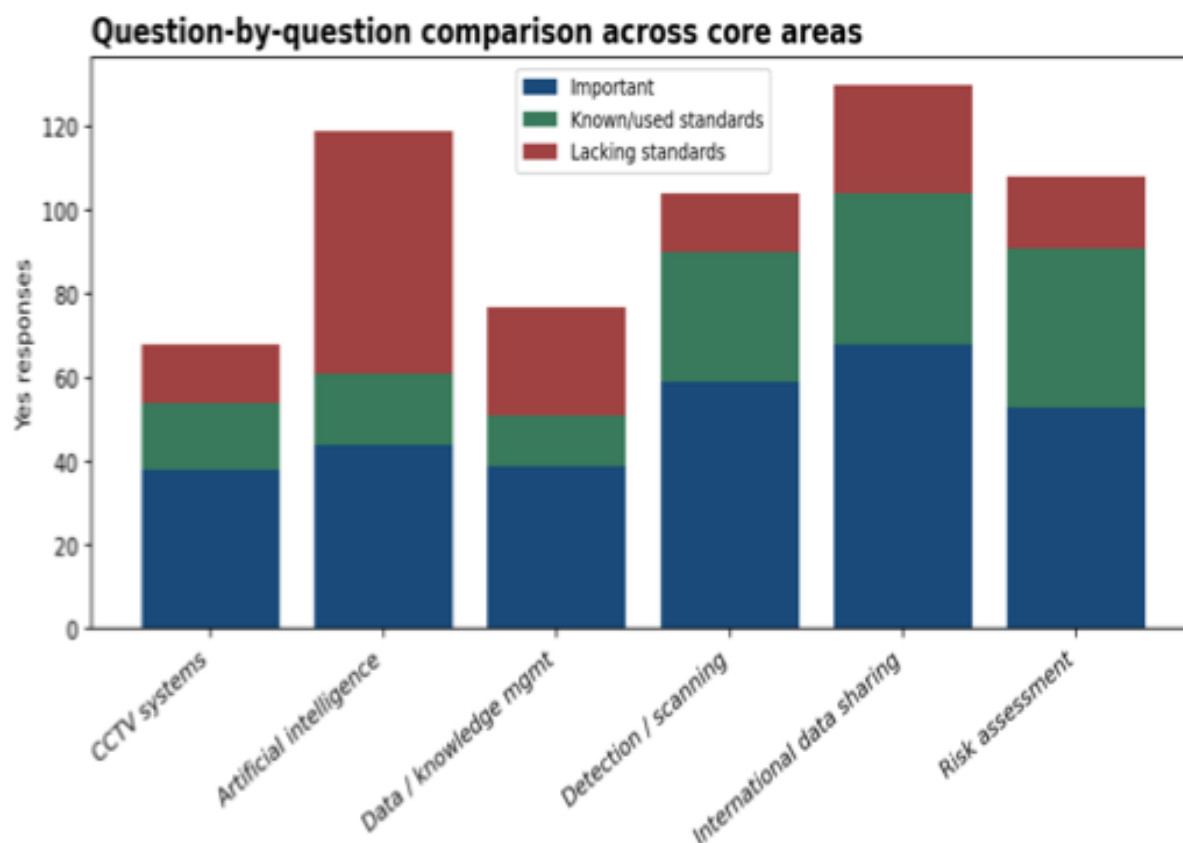


Figure 8-9: Comparison of standards needs across the core areas

A comparison made of the stakeholders requirements in standards illustrated that:

- **AI:** high importance, very high gap, weaker standards-awareness signal.
- **International data sharing:** highest importance, meaningful gap, relatively stronger standards awareness.
- **Detection/scanning:** high importance and stronger maturity signal; standards work should focus on BAG-INTEL integration points.
- **Data/knowledge management:** moderate importance but meaningful gap, especially when linked to AI governance and data quality.

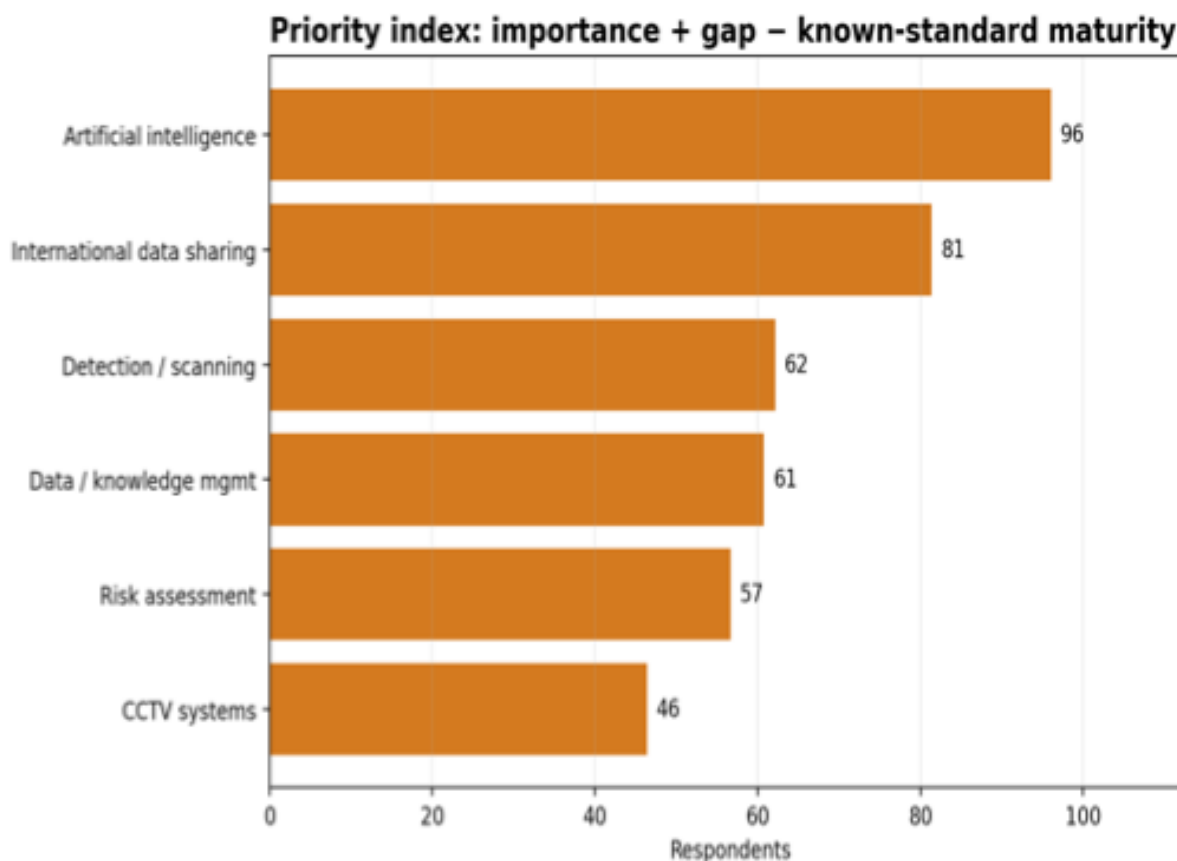


Figure 8-10: Stakeholders' priority index

8.3.6 Question 6 - Stakeholder Recommendations

Question 6: Do you have any specific recommendations with respect to the related standards, standardisation activities or European Union policy with respect to standardisation in these areas? (free text)

The free text recommendations resulted in the following four main recommendation priority areas:

Table 8-4: Four main priority area recommendations in standardisation activities

Recommended first priority:	AI governance for customs/law-enforcement intelligence systems.
Recommended second priority:	International data sharing and interoperability.
Recommended third priority:	Detection/scanning outputs and interfaces to feed a platform
Recommended enabling priority:	Data/knowledge management standards for quality, provenance, metadata and auditability.

On further analysis of the replies received, the following 10 recommendations are made to capture the key themes:

Table 8-5: Breakdown to define ten recommendations in key themes in standardisation

Recommendation 1	Strengthen harmonisation of standards across the EU to ensure consistent customs, border management and law enforcement practices and reduce fragmentation between Member States.
Recommendation 2	Prioritize interoperability by adopting common, technology-neutral standards that enable secure, real-time information exchange between customs, law enforcement and other competent authorities.
Recommendation 3	Accelerate the development of practical AI standards , focusing on explainability, transparency, accountability, traceability, human oversight, auditability and standardized AI risk management.
Recommendation 4	Establish a unified European framework for cross-border data sharing , including standardized data formats, communication protocols and secure exchange mechanisms to support more effective international investigations
Recommendation 5	Align technical standards with EU legislation and international frameworks , including the AI Act, GDPR, Union Customs Code (UCC), WCO Data Model, DICOS, ISO standards and other relevant global standards.
Recommendation 6	Support the deployment and certification of high-risk AI systems , such as BAG-INTEL, through harmonised conformity assessment procedures, accessible testing facilities and clearly defined validation methodologies.
Recommendation 7	Promote practical, operationally focused standards that support innovation, remain technology-agnostic, integrate with end-user operational environments and avoid unnecessary regulatory complexity.
Recommendation 8	Strengthen collaboration between customs authorities, law enforcement agencies, EU institutions, standards organizations, researchers, industry and international partners to ensure standards address real operational needs.
Recommendation 9	Simplify and standardize customs procedures and trade compliance requirements , reducing the complexity created by multiple bilateral agreements and improving consistency across international supply chains.
Recommendation 10	Improve access to standardized, high-quality datasets for AI development, risk assessment and X-ray image analysis, recognising that effective AI systems require broader cross-border data sharing than individual organizations can provide alone.

Table 8-6: Stakeholder group and top importance and gap signals

Stakeholder group	Top importance signals	Top gap signals
Customs	International data sharing, Risk assessment	Artificial intelligence, Data / knowledge management
Law Enforcement	International data sharing, CCTV systems	Artificial intelligence, International data sharing
Technology Provider	Detection / scanning, CCTV systems	Artificial intelligence, International data sharing

Stakeholder group	Top importance signals	Top gap signals
Consultant	International data sharing, Artificial intelligence	Artificial intelligence, Data / knowledge management
Government Agency	Artificial intelligence, Data / knowledge mgmt	Artificial intelligence, Data / knowledge mgmt
Equipment Manufacturer	Detection / scanning, International data sharing	Artificial intelligence, International data sharing

Harmonisation is a recurring strategic requirement: respondents want fewer fragmented national or sectoral approaches.

Interoperability is both a technical and governance problem: data formats, metadata, access rights, proportionality, security and evidentiary use all matter.

AI is not only a model-performance issue: respondents raised explainability, accountability, bias, auditability, human oversight and validation.

Technology-agnostic standards matter: several comments imply that BAG-INTEL should avoid dependence on a single scanner, CCTV or software supplier.

Practicality matters: respondents want standards that help end-users, testing centres, procurement and certification—not only high-level principles.

8.4 EVIDENCE-BASED CONCLUSIONS

Conclusion	Evidence
1. Interoperability is the dominant operational priority	68/88 selected international data sharing as important
2. AI is the largest perceived standards gap	58/88 selected AI as lacking standards; repeated free-text concern
3. Scanning/detection is important but more mature	59/88 selected scanning as important, with comparatively stronger standards awareness
4. Risk assessment remains strategically central	53/88 selected risk assessment as important; 38/88 know/use related standards
5. Standards need to be practical and sector-specific	Free text stresses testing, validation, interfaces and end-user integration

Table 8-7: Workstreams and recommended focus

Workstream	Recommended focus
AI governance	Explainability, auditability, human oversight, AI Act alignment

Workstream	Recommended focus
Data sharing/interoperability	Common formats, metadata, access controls, GDPR-compatible exchange
Scanning/CCTV integration	Technology-agnostic interfaces and output standards
Risk assessment	Transparent scoring, provenance, decision-support boundaries
Validation/testing	Benchmarks, acceptance criteria, pilot-site evaluation methods

8.5 PROPOSED STANDARDS ROADMAP FOR AFTER THE COMPLETION OF BAG-INTEL

Phase	Action
1. Inventory	Catalogue standards/frameworks mentioned by stakeholders and project partners
2. Gap analysis	Assess gaps against BAG-INTEL use cases and high-risk AI obligations
3. Alignment	Engage with CEN/CENELEC, ISO/IEC, WCO and relevant EU bodies
4. Pilot validation	Test interfaces, data quality, AI outputs and auditability in pilots
5. Dissemination	Publish guidance, recommendations and implementation checklist

Suggested principle: focus on “standards-to-practice” translation, because respondents want useful operational guidance rather than another abstract standards catalogue.

8.6 RECOMMENDATION OUTPUTS FROM THIS SURVEY

Standards landscape report: classify formal standards, EU regulations, operational frameworks and technical formats relevant to BAG-INTEL.

AI governance: explainability, risk management, bias testing, human oversight, auditability and high-risk AI conformity considerations.

Interoperability profile: proposed metadata, data-sharing and interface requirements for customs/law-enforcement use cases.

Pilot validation checklist: practical criteria for scanners, CCTV, data-processing systems and risk-assessment workflows.

Stakeholder engagement plan: targeted workshops with customs, law enforcement, technology providers and standards bodies.

Table 8-8: Key Standards Gap Importance Ranking

Area	Importance	Known	Gap	In development	Gap/Importance %
Artificial intelligence	44	17	58	9	132%
International data sharing	68	36	26	13	38%
Detection / scanning	59	31	14	19	24%
Data knowledge mgmt	39	12	26	5	67%
Risk assessment	53	38	17	10	32%
CCTV systems	38	16	14	4	37%

Table 8-9: Importance, Known, Lacking and In Development Rankings in Relation to Standards

Block	Area	Yes	Pct
Q2 Important	CCTV systems	38	43%
Q2 Important	Artificial intelligence	44	50%
Q2 Important	Data / knowledge mgmt	39	44%
Q2 Important	Detection / scanning	59	67%
Q2 Important	International data sharing	68	77%
Q2 Important	Risk assessment	53	60%
Q2 Important	Other	9	10%
Q3 Known/used	CCTV systems	16	18%
Q3 Known/used	Artificial intelligence	17	19%
Q3 Known/used	Data / knowledge mgmt	12	14%
Q3 Known/used	Detection / scanning	31	35%
Q3 Known/used	International data sharing	36	41%
Q3 Known/used	Risk assessment	38	43%
Q3 Known/used	Other customs / LE	17	19%
Q3 Known/used	Other	6	7%
Q4 Lacking	CCTV systems	14	16%
Q4 Lacking	Artificial intelligence	58	66%
Q4 Lacking	Data / knowledge mgmt	26	30%
Q4 Lacking	Detection / scanning	14	16%
Q4 Lacking	International data sharing	26	30%
Q4 Lacking	Risk assessment	17	19%
Q4 Lacking	Other	3	3%
Q5 In development	CCTV systems	4	5%
Q5 In development	Artificial intelligence	9	10%
Q5 In development	Data / knowledge mgmt	5	6%
Q5 In development	Detection / scanning	19	22%
Q5 In development	International data sharing	13	15%
Q5 In development	Risk assessment	10	11%
Q5 In development	Other	4	5%

8.7 BOTTOM LINE

The survey supports a follow-on to BAG-INTEL with standards agenda focused upon trusted AI, interoperable cross-border data sharing, technology-agnostic interfaces and practical validation methods.

The most compelling evidence-based message is that AI and international data sharing should be treated as joint priorities: AI cannot be trusted operationally without governance, and data sharing cannot scale without interoperable, legally robust standards.

The BAG-INTEL follow-on can add value by translating the emerging standards landscape into deployable guidance for customs, law-enforcement and technology partners.

8.8 CONCLUSIONS OF SURVEY

The survey demonstrates a strong consensus among stakeholders regarding the need for enhanced standardisation in AI, interoperability, and information sharing. While technical standards for operational technologies are relatively mature, governance-oriented standards remain underdeveloped.

The survey demonstrates strong consensus regarding the need for harmonised standards supporting interoperable, trustworthy and legally compliant intelligence ecosystems.

8.8.1 Key Findings

- Strong support exists for standards that facilitate **interoperability and international information sharing**.
- **Artificial Intelligence** emerged as the most significant standards gap.
- **Risk assessment, detection technologies, and data mining** are viewed as high-priority operational domains.
- Stakeholders favour **harmonised European approaches** rather than isolated national or sector-specific solutions.
- **Data governance, explainability, trust, and transparency** are becoming critical requirements for AI-enabled systems.

8.8.2 Strategic Implications

The survey demonstrated that future standardisation efforts should focus on trusted AI, cross-border information exchange, and interoperable intelligence ecosystems.

The survey demonstrates a strong consensus among stakeholders regarding the need for enhanced standardisation in AI, interoperability, and information sharing.

8.8.3 Potential Conclusions

Stakeholders are clearly indicating that:

- AI standardisation is not keeping pace with deployment.
- Governance, transparency, explainability, and interoperability standards remain underdeveloped.
- International information-sharing frameworks require further harmonisation.

This finding aligns well with current European priorities around the:

- EU AI Act
- Data Act
- Interoperability frameworks
- Trusted AI for public-sector applications

8.9 MESSAGES FROM THE STAKEHOLDER COMMUNITY

8.9.1 Message 1: Interoperability is the Dominant Concern

The survey suggests that stakeholders believe the greatest value from standardisation comes from enabling information exchange across customs, law-enforcement, and international agencies.

8.9.2 Message 2: AI is the Largest Standards Gap

While AI is seen as highly important, it is simultaneously viewed as the area most lacking mature standards.

8.9.3 Message 3: Operational Technologies are Ahead of Governance Technologies

Scanning, CCTV, and detection technologies already benefit from significant technical standards.

In contrast:

- AI governance
- Data governance
- Data sharing
- Explainability
- Privacy-preserving analytics

appear to require more development.

8.9.4 Message 4: Stakeholders want Harmonisation Rather than More Isolated Standards

Several free-text comments reference:

- interoperability
- harmonisation
- cross-border exchange
- GDPR compliance
- common frameworks

This suggests a preference for coordinated European approaches rather than sector-specific fragmentation.

9 CONCLUSIONS

The BAG-INTEL project has established a comprehensive technological and operational foundation for the modernisation of customs control of passenger baggage arriving on international flights. Its principal contribution lies not in the creation of a single detector, algorithm or software application, but in the integration of several complementary capabilities into a coherent customs intelligence environment. Advanced scanning, AI-assisted contraband detection, luggage re-identification, multi-source risk assessment, real-time decision support, knowledge representation, digital twin modelling, and secure system integration collectively address the complete operational chain, from the initial screening of baggage to the targeted intervention by customs officers.

This integrated approach responds to a structural challenge facing customs administrations. International passenger volumes and the complexity of smuggling methods are increasing, while customs authorities must operate within finite staffing, infrastructure and budgetary constraints. At the same time, customs control must remain proportionate and must not create unnecessary delays for compliant travellers. The BAG-INTEL concept addresses these competing requirements by seeking to improve the quality of inspection targeting, reduce dependence on random controls, preserve passenger flow and enable customs resources to be concentrated on baggage with stronger indications of risk.

The final exploitation assessment demonstrates that the project has generated a substantial and diverse portfolio of technological, methodological, operational and training-related results. Twenty Exploitable Results were assessed using a common framework that considered innovation, exploitability, and impact. The quantitative assessment provided an evidence-based indication of the results with the strongest combined performance, while the qualitative analysis considered maturity, architecture, ownership, operational relevance, integration needs, market positioning and dependencies.

The assessment confirmed that the strongest individual assets are centred on BAG-INTEL's core technological propositions. The highest-ranked Exploitable Results concerned risk-based decision support for selecting baggage for inspection, advanced baggage scanning, luggage reidentification, real-time customs decision support, advanced detection systems, digital twin-enabled customs management, probabilistic matching, and integrated customs information management. These findings demonstrate that the project's principal exploitation potential is distributed across four interdependent capabilities: detection, risk intelligence and decision support, reidentification, and system integration and deployment.

At the same time, the analysis confirmed that the exploitation value of BAG-INTEL cannot be adequately captured by a simple ranking of individual results. Several results that received lower individual scores perform indispensable enabling functions. CCTV integration and configuration, secure software deployment, data and knowledge management, operational methodology, training and system integration may not always constitute stand-alone commercial products, but they are required for the deployment and sustainable operation of the more visible AI and scanning components.

For this reason, the final strategy consolidated the individual results into four Key Exploitable Results. This represents one of the most significant developments in the final exploitation roadmap. The Key Exploitable Results are organised according to operational, and market needs rather than solely by the technical origin or ownership of each component.

The Customs Bag-Risk Assessment and Real-Time Decision Support Suite provides the analytical and operational capabilities needed to support more targeted inspection decisions. It combines real-time

decision support, bag-level risk management, risk indicators derived from external data, connection analysis, statistical weighting and aggregation, and the methodology required to configure and operate BAG-INTEL in a customs environment. Its main value lies in transforming fragmented risk signals into structured, traceable and operationally actionable information.

The AI-Based Luggage Reidentification and Tracking System addresses one of the project's most distinctive operational challenges. A bag flagged as suspicious during scanning must then be located when it reaches the baggage-claim or customs area. The system combines luggage detection, characterisation, tracking, probabilistic matching, CCTV integration and alerting to enable non-intrusive reidentification. This approach avoids visible physical tags or markings, does not alert passengers that their baggage has been selected for inspection, and preserves continuity between the scanning decision and the physical customs intervention.

The Advanced Contraband Detection System combines high-resolution baggage scanning with AI-assisted detection algorithms. It supports the identification of prohibited, restricted or undeclared goods in passenger baggage and provides key detection indicators to the wider BAG-INTEL risk and decision-support environment. Its exploitation potential is strengthened by its connection with an established detection-technology provider and by its relevance to a core customs-control function.

The Integrated Digital Twin, Knowledge and Secure Deployment Layer provides the cross-cutting capabilities required to transform the individual project components into a deployable and maintainable system. It combines the integrated customs information platform, digital twin-based management decision support, knowledge graph and intelligent analysis, and secure integration and delivery methodologies. Its value lies in data integration, airport-specific configuration, scenario simulation, knowledge representation, cybersecurity, maintainability and controlled system evolution.

Together, these four Key Exploitable Results establish an integrated operational logic. The Advanced Contraband Detection System identifies suspicious contents. The Customs Bag-Risk Assessment and Real-Time Decision Support Suite combines detection outputs with other indicators to support the inspection decision. The AI-Based Luggage Reidentification and Tracking System enables selected baggage to be in the customs area. The Integrated Digital Twin, Knowledge and Secure Deployment Layer connects the components, supports operational planning, and enables secure and sustainable deployment.

This interdependency leads to a clear commercial and operational conclusion: the strongest BAG-INTEL proposition is an integrated and modular solution rather than a collection of unrelated tools. The project results may be exploited separately where individual maturity, ownership, and market conditions permit, but their highest combined value is realised through joint deployment.

The full BAG-INTEL configuration can be positioned as an end-to-end customs baggage-control environment. However, a full deployment may require substantial investment, complex integration and a longer procurement process. The final roadmap therefore also supports modular entry packages. A customs authority may initially adopt the risk-assessment and decision-support capabilities, the detection and reidentification capabilities, or the digital twin and operational optimisation layer. Such phased deployment can reduce adoption barriers, generate operational evidence and establish the infrastructure required for later integration of additional components.

The business-case analysis confirms that national customs administrations and airport customs units are the principal customers and users of the BAG-INTEL results. Airport operators, airport IT and security departments, law-enforcement organisations, system integrators, equipment manufacturers and technology providers also have important roles as buyers, beneficiaries, infrastructure providers, delivery partners or commercial channels.

The public-sector nature of the market significantly shapes the exploitation strategy. Customs authorities do not purchase technologies solely based on novelty or theoretical performance. Procurement decisions require evidence of operational effectiveness, legal compliance, cybersecurity, interoperability, reliability, support capacity and value for money. Technologies must align with existing customs procedures, national legislation, airport infrastructure and institutional accountability requirements.

Accordingly, the transition from a successful research result to a market-ready solution requires additional activities beyond technical development. Each Key Exploitable Result will need a clear product or service definition, supported configurations, technical documentation, performance evidence, integration specifications, training materials, support arrangements, and lifecycle management procedures. Buyers must be able to understand precisely what is being procured, which organisation is responsible for delivery, how the system will be maintained and what happens when algorithms, data sources or operational requirements change.

The most suitable commercial model is likely to be mixed. Depending on the Key Exploitable Result and the adopting authority, revenues may arise from hardware sales, software licences, algorithm licences, site-based platform licences, subscriptions, AI-as-a-Service, professional services, system integration, customisation, consultancy, digital twin modelling, training, maintenance, model retraining, cybersecurity updates and managed services. On-premises and hybrid deployment models are likely to remain particularly important because customs data and airport security environments may be subject to strict sovereignty, confidentiality, and operational control requirements.

The return on investment for public authorities should not be evaluated only in conventional financial terms. BAG-INTEL can create value through improved inspection targeting, increased detection effectiveness, better allocation of customs personnel, reduced manual analysis, fewer unnecessary controls, improved traceability, stronger management information and smoother passenger flows. These benefits should be translated into measurable operational indicators during subsequent pilots and deployments.

From the perspective of technology owners and service providers, commercial viability will depend on the extent to which core components can be reused across different airports while allowing for necessary local adaptation. Excessive customisation for every implementation could limit scalability and increase support costs. The future exploitation model should therefore distinguish between a reusable core product or reference architecture and site-specific services, including data connectors, CCTV configuration, scanner integration, user interfaces, risk policies, and operational workflows.

A further conclusion concerns the allocation of exploitation roles. The Key Exploitable Results are composite assets and may involve several owners and contributors. It cannot be assumed that the technical owner of each component will also possess the resources, market presence or contractual capacity required to sell and support a complete solution. Joint exploitation will therefore require a clear distinction among the Owner, the Service Provider and the Seller or Business Champion.

The Owner retains and manages the relevant intellectual property and technical component. The Service Provider undertakes activities including deployment, integration, customisation, hosting, training, maintenance and support. The Seller or Business Champion leads customer engagement, tender participation, contract management and revenue distribution. These roles may be performed by the same organisation in some cases, but they should be explicitly allocated before joint market engagement begins.

The consortium should avoid proceeding with joint commercialisation without clear agreements on licensing, commercial leadership, liability, maintenance responsibilities, revenue sharing, support

obligations, and decision-making. The absence of such arrangements could delay procurement discussions and create uncertainty for prospective customers.

The analysis also confirms that BAG-INTEL remains at a stage where further operational validation is essential. The technical results provide a credible basis for continued development, but deployment in customs and airport environments requires evidence generated under realistic conditions.

For luggage reidentification, performance must be assessed across different camera positions, lighting conditions, airport layouts, crowd densities, luggage types, trolley use, partial visibility and occlusion. The system must manage uncertainty and communicate confidence appropriately. False matches may cause unnecessary interventions, while missed matches may prevent the inspection of suspicious baggage. Validation should therefore consider both algorithmic accuracy and the operational consequences of system errors.

For contraband detection, further work is needed on representative datasets, relevant contraband categories, concealment scenarios, image quality, detection probability and false-alarm management. Smuggling methods evolve, and the performance of a model trained on one dataset cannot be assumed to remain stable indefinitely. Continued access to suitable data, controlled retraining and post-deployment monitoring are therefore necessary for sustainability.

For risk assessment and decision support, the principal dependencies are lawful access to external data, data quality, interoperability and institutional acceptance. The value of multi-source risk analysis will be diminished if the relevant information cannot be accessed in a timely and lawful manner. Future deployments should therefore begin with a detailed mapping of available data sources, access rights, purposes of processing, retention requirements, responsibilities and technical interfaces.

Human oversight must remain a fundamental design and operational principle. BAG-INTEL is intended to support customs decision-making, not to replace accountable professional judgement. The system may prioritise baggage, identify patterns, present risk indicators and recommend action, but customs officers must retain the authority and responsibility to accept, question or disregard the recommendation. The grounds for intervention should be documented, and the system should preserve sufficient evidence to support audit, review and accountability.

User acceptance is also a condition of successful exploitation. Even a technically accurate system may fail if it disrupts established workflows, produces opaque alerts or requires excessive additional effort. Customs officers and managers should continue to participate in system configuration, validation and evaluation. Interfaces, thresholds, alert presentation and escalation procedures should be designed with users rather than imposed upon them.

Training should therefore be an integral part of each deployment. Users need to understand the system's purpose, capabilities, and limitations; how to interpret confidence values; the appropriate response to alerts; the possibility of errors; and the procedures for reporting or correcting problematic outputs. Management and technical personnel also require training in data governance, cybersecurity, model monitoring, and system maintenance.

The stakeholder engagement analysis confirms that sustained collaboration is required across the entire innovation and deployment ecosystem. Customs authorities and operational officers are essential for validation and adoption. Airport operators and airport IT departments are required for infrastructure access, system integration, CCTV configuration and operational continuity. Law-enforcement and border-management organisations may provide relevant data, analytical expertise and adjacent use cases. Technology providers and system integrators are required for commercial packaging, deployment and support. Policymakers, regulators and data-protection authorities

influence the legal and institutional acceptability of the solutions. Research organisations support further technological maturation, while standardisation bodies provide the mechanisms for consolidating interoperability and assurance requirements.

Stakeholder engagement after the project should therefore remain targeted and results oriented. Generic dissemination will not be sufficient. Each engagement activity should have a clear objective, such as validating a performance requirement, preparing a pilot, defining procurement criteria, resolving an integration issue, establishing a commercial partnership, or contributing to a standardisation initiative.

The Intellectual Property Rights analysis provides a final, structured reference for the protection and exploitation of BAG-INTEL results. The project has updated the inventory of Background Intellectual Property, identified the Foreground Intellectual Property generated during implementation, and consolidated ownership, contributions, access rights, restrictions, and exploitation intentions in the final IPR Matrix.

The principal IPR conclusion is that effective exploitation depends on result-specific rather than generic arrangements. Different outputs require different protection and licensing strategies. Software may be protected through copyright, confidential source code and proprietary or open-source licences. Algorithms and methodologies may be protected through copyright, trade secrets, know-how or, where justified, patent protection. Training materials may be made available under open licences where wider uptake is the principal objective. Data may be reusable only under defined legal, ethical and contractual conditions.

Jointly developed results require particular attention. Where contributions cannot be separated, partners should agree in writing how the result will be protected, licensed, maintained and exploited. The agreement should address decision-making, costs, licensing authority, enforcement, revenue distribution, and each owner's right to use the jointly owned result independently.

Background Intellectual Property must also be distinguished carefully from the Foreground generated during the project. The exploitation of a project result may depend on proprietary software, datasets, patents, methodologies or know-how held by one partner before the project. A prospective customer or commercial partner must understand whether the complete solution can be licensed and supported without infringing those pre-existing rights.

The protection of project results should not be interpreted as requiring maximum restriction. The appropriate approach is to protect what must remain proprietary while enabling access and reuse where this advances research, standardisation, training or market adoption. Decisions concerning openness should reflect the nature of the result, commercial objectives, security requirements, data protection obligations, and the interests of the relevant owners.

Standardisation is another decisive factor in the future uptake of BAG-INTEL. The analysis demonstrates that arriving-passenger baggage control is governed by a complex, layered set of standards. Customs risk management, non-intrusive inspection, baggage-scanning equipment, radiation safety, CCTV, Artificial Intelligence, cybersecurity, data protection and evidence management are increasingly interconnected.

The principal conclusion is that these domains should no longer be treated as separate compliance questions. For an AI-enabled customs-control system, they constitute a single assurance problem. A deployment cannot be considered trustworthy merely because the scanner complies with equipment-safety standards or because the AI model demonstrates high laboratory accuracy. Trustworthiness depends on the interaction of validated performance, secure data flows, lawful processing,

interoperable interfaces, trained users, human oversight, evidence integrity and continuous monitoring.

No single standard currently covers the complete BAG-INTEL environment. A living standards profile is therefore required. Such a profile should combine customs-specific instruments, equipment, and radiation-safety requirements; video-surveillance standards; Artificial Intelligence governance standards; cybersecurity frameworks; and applicable legal obligations. The profile should be reviewed before each deployment and updated as standards and regulations evolve.

The practical value of standardisation lies in its translation into procurement and operational practice. Standards should inform technical specifications, tender clauses, supplier evidence, acceptance-testing procedures, standard operating procedures, training, audit trails and lifecycle monitoring. Merely citing a list of standards in procurement documentation is insufficient unless the buyer defines how compliance will be demonstrated and tested.

The second BAG-INTEL standards survey provides substantial evidence concerning stakeholder priorities. The survey received 88 responses from customs, law enforcement, government, industrial, research, and consultancy stakeholders. International data sharing was identified as important by 68 respondents, making interoperability the dominant operational priority. Detection and scanning were identified as important by 59 respondents, while risk assessment was selected by 53 respondents. Artificial Intelligence was identified as lacking adequate standards by 58 respondents, considerably more than any other domain.

These results lead to four central conclusions. First, interoperability is not only a technical interface problem. It also concerns metadata, data quality, access rights, security, proportionality, evidentiary use and legal responsibility. Second, Artificial Intelligence is being deployed more rapidly than sector-specific governance and assurance standards are developing. Third, operational technologies such as scanners and CCTV are supported by comparatively mature technical standards, while governance technologies concerning AI, data and integrated decision support remain less developed. Fourth, stakeholders favour harmonisation and practical European or international frameworks rather than fragmented national or vendor-specific approaches.

The standardisation roadmap should consequently focus on trusted AI, interoperable cross-border data exchange, technology-neutral interfaces and practical validation methodologies. Artificial Intelligence and data sharing should be addressed together. AI cannot be trusted operationally without appropriate governance, while cross-border information exchange cannot scale without legally robust and interoperable standards.

A major gap remains the absence of a public, customs-specific performance framework for AI-assisted contraband detection in passenger baggage. Future work should consider test-set governance, contraband categories, concealment scenarios, performance metrics, operational trial design, data protection controls, and human oversight.

A second gap concerns the interfaces among scanner systems, CCTV, risk engines, decision-support tools and case-management environments. Proprietary formats increase integration costs and create the risk of vendor lock-in. Technology-neutral interfaces, common metadata and standard export packages would support portability, evidence handling, auditability and competitive procurement.

A third gap concerns post-deployment monitoring. Customs authorities need practical metrics for model drift, false alarms, missed detections, officer overrides, alert fatigue, adversarial attempts and retraining triggers. Horizontal AI standards provide an important foundation, but customs-specific profiles and implementation guidance remain necessary.

The future standardisation strategy should therefore emphasise the translation of standards into practice. The objective should not be to produce another abstract catalogue of standards, but to help customs authorities, technology providers and system integrators apply the emerging framework in real systems, tenders, pilots and operational procedures.

The overall sustainability of BAG-INTEL depends on the coordinated management of technical, operational, commercial, institutional, legal and knowledge-related factors. Technical sustainability requires maintainable software, documented interfaces, cybersecurity, controlled releases and model monitoring. Operational sustainability requires integration with real-world customs processes, user acceptance, training and evidence of performance. Commercial sustainability requires clear products, viable pricing, competent service providers and credible market channels. Institutional sustainability requires ongoing engagement with public authorities and alignment with policy and procurement priorities. Legal and ethical sustainability requires lawful data use, human oversight, fairness, proportionality and accountability. Knowledge sustainability requires documentation, research continuity, training, standardisation and technology transfer.

The post-project pathway should therefore be phased. The immediate priority is to preserve and consolidate the project assets. This includes finalising ownership and licensing arrangements, maintaining technical documentation, preserving relevant data and models, recording known limitations and identifying the partners responsible for each result.

The second priority is further validation and maturation. The Key Exploitable Results should be tested under realistic, diverse airport conditions, with performance measured against clear operational and governance criteria. Validation should cover not only technical accuracy but also integration, usability, decision quality, passenger-flow implications, cybersecurity and maintainability.

The third priority is market and procurement preparation. The results should be converted into clearly defined, modular and supportable offerings. Reference architectures, deployment requirements, service descriptions, indicative pricing models, support conditions and acceptance criteria should be prepared. Engagement with system integrators and prospective Business Champions should be intensified.

The fourth priority is the development of pilot-to-procurement pathways. Follow-on pilots should be designed not merely as additional research demonstrations, but as reference implementations capable of producing the evidence required for public procurement. They should involve end users, procurement authorities, technology providers, IT and security stakeholders from the beginning.

The fifth priority is continued stakeholder and standardisation engagement. The project's findings should be communicated to relevant European and international organisations, technical committees, customs networks and future research initiatives. Particular emphasis should be placed on AI governance, cross-border data exchange, interfaces, validation and procurement guidance.

The conclusion is that BAG-INTEL has generated a credible portfolio of results with significant potential to support a more intelligence-led, efficient and accountable model of customs baggage control. The project has demonstrated the strategic value of connecting detection, risk assessment, decision support, reidentification and operational optimisation. It has also clarified that the transition to deployment depends on more than technological performance.

Successful exploitation will require continued validation, high-quality and lawfully accessible data, interoperable and secure architectures, clear Intellectual Property Rights arrangements, competent commercial and service-delivery structures, procurement readiness, training, human oversight and

long-term lifecycle support. Standardisation must connect these dimensions and provide a practical assurance framework rather than operate as a separate technical exercise.

If these conditions are addressed systematically, BAG-INTEL can progress from a European research and innovation project to a modular, scalable foundation for future customs control solutions. Its results can support more targeted inspections, better use of customs resources, improved detection of contraband, stronger operational traceability and reduced disruption for compliant passengers. The project therefore provides not only a portfolio of technologies, but also a structured basis for future deployment, commercial collaboration, policy development, standardisation and continued innovation in European customs and border management.

REFERENCES

- [1] World Customs Organization, SAFE Framework of Standards, <https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/safe-framework-of-standards.pdf>
- [2] World Customs Organization, Guidelines for the Procurement and Deployment of Scanning/NII Equipment, June 2025, https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/nii-guidelines-2025/nii-guidelines-en_june-2025.pdf
- [3] World Customs Organization, WCO Data Model, <https://www.wcoomd.org/DataModel>
- [4] WCO News, Artificial intelligence-based X-ray image analytics solution: India's experience and key takeaways, 2026, <https://mag.wcoomd.org/magazine/wco-news-109-issue-1-2026/artificial-intelligence-based-x-ray-image-analytics-solution-indias-experience-and-key-takeaways/>
- [5] ISO, ISO/IEC 42001:2023 Artificial intelligence management system, <https://www.iso.org/standard/42001>
- [6] ISO, ISO/IEC 23894:2023 Artificial intelligence - Guidance on risk management, <https://www.iso.org/standard/77304.html>
- [7] ISO, ISO/IEC 22989:2022 Artificial intelligence concepts and terminology, <https://www.iso.org/standard/74296.html>
- [8] ISO, ISO/IEC 23053:2022 Framework for AI systems using machine learning, <https://www.iso.org/standard/74438.html>
- [9] ISO, Artificial intelligence top standards, <https://www.iso.org/sectors/it-technologies/ai>
- [10] CEN-CENELEC/JTC 21, European AI Standardisation , <https://jtc21.eu/>
- [11] CEN-CENELEC, Artificial Intelligence area of work, <https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/>
- [12] CEN-CENELEC, Update on decision to accelerate AI standardisation , 23 October 2025, <https://www.cencenelec.eu/news-events/news/2025/brief-news/2025-10-23-ai-standardisation/>
- [13] European Commission, Standardisation of the AI Act, <https://digital-strategy.ec.europa.eu/en/policies/ai-act-standardisation>
- [14] European Commission, AI Act regulatory framework, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- [15] DIN, Artificial Intelligence standardisation , <https://www.din.de/en/innovation-and-research/artificial-intelligence>
- [16] DIN/DKE, German Standardisation Roadmap AI, <https://www.din.de/en/innovation-and-research/artificial-intelligence/ai-roadmap>
- [17] IEC, IEC 61010-2-091:2019 Cabinet X-ray systems, <https://webstore.iec.ch/en/publication/33872>
- [18] IEC, IEC 62463:2024 X-ray systems for security screening of persons, <https://webstore.iec.ch/en/publication/73407>
- [19] IEC, IEC 62523:2010 Cargo/vehicle radiographic inspection system, <https://webstore.iec.ch/en/publication/7155>
- [20] IEC, IEC 62676-4:2025 Video surveillance application guidelines, <https://webstore.iec.ch/en/publication/83425>
- [21] IEC, IEC 62676-5-1:2024 Camera equipment performance measurement, <https://webstore.iec.ch/en/publication/62442>
- [22] IEC, IEC 62676-2-11:2024 VMS and VSaaS profiles, <https://webstore.iec.ch/en/publication/66755>
- [23] IEC, IEC 62676-2-31:2019 Video transmission protocols, <https://webstore.iec.ch/en/publication/61227>
- [24] IEC, IEC 62676-6:2026 Intelligent video analysis, <https://webstore.iec.ch/en/publication/59704>
- [25] ISO, ISO 22311:2012 Video-surveillance export interoperability, <https://www.iso.org/standard/53467.html>

- [26] ECAC, Common Evaluation Process of security equipment, <https://www.ecac-ceac.org/activities/security/common-evaluation-process-cep-of-security-equipment>
- [27] ECAC, CEP test request form, June 2023, https://www.ecac-ceac.org/images/activities/security/ECAC-CEP_test_request_form-final.pdf
- [28] UK Department for Transport, EDSCB C3 approvals, 2025, <https://www.gov.uk/government/publications/explosive-detection-systems-for-cabin-baggage-edscb-c3-approvals>
- [29] ACI EUROPE, Changes to EU regulation restrict use of new generation baggage scanners, 31 July 2024, <https://www.aci-europe.org/press-release/504-changes-to-eu-regulation-restrict-the-use-of-new-generation-baggage-scanners-at-europe-s-airports.html>
- [30] TSA, Emerging Technology - Security Screening, <https://www.tsa.gov/travel/security-screening/emerging-technology>
- [31] DHS, TSA AI Use Case Inventory, Accessible Property Screening, 2024, <https://www.dhs.gov/ai/use-case-inventory/tsa>
- [32] ACI, Smart Security, <https://aci.aero/airport-advocacy/airport-security/smart-security/>
- [33] IATA, Passenger Data, <https://www.iata.org/en/programs/passenger/passenger-facilitation/passenger-data/>
- [34] European Commission/Eur-Lex, Commission Implementing Regulation (EU) 2015/1998 public annex references, accessible consolidated public copies.
- [35] Bundesamt fuer Strahlenschutz, Security screening of hand baggage using X-ray scanners, <https://www.bfs.de/EN/topics/ion/daily-life/cabin-luggage/hand-baggage.html>

ANNEXES

ANNEX 1 - BAG-INTEL STANDARDISATION QUESTIONNAIRE SURVEY

Disclaimer

The European Commission is not responsible for the content of questionnaires created using the EUSurvey service - it remains the sole responsibility of the form creator and manager. The use of EUSurvey service does not imply a recommendation or endorsement, by the European Commission, of the views expressed within them.

Anonymous mode

The anonymous option has been activated. As a result, your contribution to this survey will be anonymous as the system will not save any personal data such as your IP address.

Survey with a Focus on BAG-INTEL Technology Components, Systems and Solutions, Standardisation Efforts and Policy Recommendations (if any)

This survey is part of the work of the BAG-INTEL Horizon Europe project (<https://bag-intel.eu/>). BAG-INTEL aims to address the needs of the border and customs authorities at inland border airports in the area of development of new tools to increase the effectiveness and efficiency of baggage customs controls.

We thank you in advance for your support in completing this survey which is voluntary by nature.

1. What type of organisation do you represent?

Single Choice Question

- a. Customs
- b. Law Enforcement
- c. Government Agency
- d. Equipment Manufacturer
- e. Technology Provider (including software)
- f. Consultant / Consulting
- g. Services Provider
- h. European Institutions (European Commission, etc.) Which institution/organization? Please fill in free text below:
- i. Other Please fill in free text below:

Enter here the name of organization or institution (see last two options above):

2. In your opinion, standardisation is important in which of the following areas (more than one answer is possible):

Multiple Choice Question

- a. CCTV Systems and the images and files generated
- b. Artificial Intelligence Systems
- c. Data Mining / Knowledge Management / Data Processing Systems
- d. Detection / Scanning Technologies and Systems and the images and files generated
- e. Customs / Law Enforcement international data sharing
- f. Customs / Law Enforcement risk assessment
- g. Other areas (please name the area)

Please here enter the additional areas which you deem important in standarization:

3. **In which areas do you know about specific standards and/or use standards (more than one answer is possible):**

Multiple Choice Question

- i. CCTV Systems and the images and files generated (if known, please name the standard(s))
- j. Artificial Intelligence Systems (if known, please name the standard(s))
- k. Data Mining / Knowledge Management / Data Processing Systems (if known, please name the standard(s))
- l. Detection / Scanning Technologies and Systems and the images and files generated (if known, please name the standard(s))
- m. Customs / Law Enforcement international data sharing (if known, please name the standard(s))
- n. Customs / Law Enforcement risk assessment (if known, please name the standard(s))
- o. Customs / Law Enforcement other standards (if known, please name the standard(s))
- p. Other areas (please name the area and please indicate the standard(s))

Please here enter the area and name of the specific standards known or used:

4. **In your opinion are there any standards that are currently missing from any of the topic areas below or otherwise (more than one answer is possible)? And is there any area lacking which needs more immediate attention? Please note and explain in the free text area below.**

Multiple Choice Question

- a. CCTV Systems and the images and files generated
- b. Artificial Intelligence Systems
- c. Data Mining / Knowledge Management / Data Processing Systems
- d. Detection / Scanning Technologies and Systems and the images and files generated
- e. Customs / Law Enforcement international data sharing
- f. Customs / Law Enforcement risk assessment

- g. Other areas (please name the area)

If there is any area lacking which needs more immediate attention, please note and explain in the free text option below:

5. **Are you aware of and / or participate in any standardisation or pre-standardisation development efforts related to any of the topics and areas mentioned below (more than one answer is possible)?**

If so, in the free text option below, name which topic areas are involve and if possible provide a very short sentence about the current status of these efforts.

Multiple Choice Question

- a. CCTV Systems and the images and files generated
- b. Artificial Intelligence Systems
- c. Data Mining / Knowledge Management / Data Processing Systems
- d. Detection / Scanning Technologies and Systems and the images and files generated
- e. Customs / Law Enforcement international data sharing
- f. Customs / Law Enforcement risk assessment
- g. Other areas (please name the area)

Free text to enter known status of standardisation efforts and or other areas in development.

6. **Do you have any specific recommendations with respect to the related standards, standardisation activities or European Union policy with respect to standardisation in these areas? (free text)**

Free text option

7. Please send an email to survey@conceptivity.ch if you would like to be connected and to receive more information about the BAG-INTEL project.