BAG-INTEL

D6.3: Standardisation, Exploitation and Sustainability Strategy and Plan

Revision: v3.0

Work package	WP6 - Dissemination, Communication, Exploitation
Task	Tasks 6.3 and 6.4
Due date	28/02/2025
Submission date	21/02/2025
Deliverable lead	CONCEPTIVITY
Version	1.0
Authors	Victoria Menezes Miller (CPT), Mark Miller (CPT), Erika Nika (DBC)
Reviewers	Hassane Essafi (CEA
Abstract	This deliverable represents a report on exploitation and standardisation aspects covering the first period of the BAG-INTEL Project. The report includes inputs, feedback and results and conclusions. A second deliverable will be issued toward the end of the project in order to track all elements and to provide a full and final update on standardisation and exploitation.
Keywords	Standardisation, Exploitation, Sustainability

Grant Agreement No.: 101096649
Call: HORIZON-CL3-2022-BM-01

Topic: HORIZON-CL3-2022-BM-01-04
Type of action: HORIZON-RIA

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	10/12/2024	1st edit	Erika Nika (DBC)
V0.2	15/12/2024	2nd edit	Mark Miller (CPT), Victoria Menezes Miller (CPT)
V0.2	16/01/2025	3rd edit	Mark Miller (CPT), Victoria Menezes Miller (CPT)
V0.3-5	15/01/2025	Revisions Chapter 8	Mark Miller (CPT), Victoria Menezes Miller (CPT)
VO.6	04/02/2025	Chapters 1-7	Erika Nika (DBC)
V0.7	04/02/2025	Incorporate Part 1 (Chapter 1-7)	Victoria Menezes Miller (CPT)
V0.8	04/02/2025	Additions to Chapter 8	Mark Miller (CPT)
V0.9-V0.12	05/02/2025-06/02/2025	Revisions Chapter 8-12	Mark Miller (CPT), Victoria Menezes Miller
V0.13	10/02/2025	Final edits Part 1	Erika Nika (DBC)
V0.14	10/02/2025	Sent to Reviewer	Mark Miller (CPT)
V0.15	21/02/2025	Comments from reviewer integrated	Erika Nika (DBC)
V0.16	21/02/2025	Finalised for transfer for final review	Mark Miller (CPT), Victoria Menezes Miller

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

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

The BAG-INTEL project aims to revolutionize customs security and baggage control through AI-powered risk assessment, digital twin technology, and real-time decision-support systems. As global trade and air travel expand, customs authorities face increasing challenges in detecting contraband, streamlining baggage inspections, and ensuring regulatory compliance. The project develops cutting-edge AI-driven solutions to address these issues, optimizing operational efficiency, reducing manual workload, and enhancing security screening accuracy.

This deliverable, D6.3: Standardisation, Exploitation, and Sustainability Strategy and Plan, outlines the roadmap for ensuring the long-term impact and adoption of BAG-INTEL solutions. It presents a comprehensive market analysis, identifying key trends such as the rise of AI and machine learning in customs control, increasing regulatory scrutiny, and the growing need for automated security solutions. A competitive landscape assessment highlights BAG-INTEL's positioning relative to established security technology providers, AI startups, and government-backed initiatives. The project differentiates itself through AI-powered baggage reidentification, risk-based decision support systems, and digital twin modeling—offering a more adaptive and scalable approach than traditional solutions.

The deliverable focuses on exploitable results and commercialization strategies. The document details specific Key Exploitable Results (KERs), including AI-driven contraband detection algorithms, digital twin-based customs simulations, and secure data-sharing systems for customs authorities. The Intellectual Property Rights (IPR) management strategy ensures that these innovations are protected, while the exploitation plan defines pathways for commercial uptake, licensing agreements, and integration into existing customs infrastructures.

Despite its technological advancements, BAG-INTEL faces several market entry challenges, including regulatory compliance, data privacy concerns, integration complexities, and competition from established industry leaders. To address these, the project proposes strategic policy engagement, pilot implementations, and modular deployment models that facilitate adoption while reducing transition costs for customs agencies.

The socioeconomic analysis within this deliverable evaluates the political, economic, social, technological, legal, and environmental (PESTLE) factors influencing BAG-INTEL's implementation. It is accompanied by a SWOT analysis that identifies key strengths, weaknesses, opportunities, and threats. The project's approach to stakeholder engagement is structured around collaboration with customs authorities, airport security agencies, technology providers, and regulatory bodies, ensuring broad support for its deployment.

The deliverable concludes with individual and joint exploitation plans detailing how project partners will commercialize and sustain BAG-INTEL results beyond the project's duration. By aligning with EU policy frameworks, international security regulations, and industry best practices, BAG-INTEL is positioned to become a leading AI-driven solution in next-generation customs control and border security operations.

Furthermore, this deliverable also covers the issues in looking at the standards currently addressing customs controls of passenger baggage including the equipment, the operational activities, the additional controls involved and sharing of data.

A key part of the deliverable is the results of survey undertaken in order to look at potential areas that could be addressed via standardisation, in addition to touching upon the Standards Development Organisations (SDOs) that are relevant to this. It is clear that a full standardisation effort would not be

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

possible within the timeframe of the BAG-INTEL project, however, there can be potential some early identification and pre-standardisation activities undertaken if there is sufficient “critical mass” and impetus to move forward.

It is important to mention that this deliverable is the first in the series of two deliverables within the BAG-INTEL project addressing both Exploitation and Standardisation, with the final deliverable occuring toward the very end of the project.

This deliverable also “points the way” for the future, both in terms of the final deliverable and with respect to the future of “after the end of the project”.

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

TABLE OF CONTENTS

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

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

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

LIST OF FIGURES

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

LIST OF TABLES

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

ABBREVIATIONS

AI	Artificial Intelligence
API	Application Programming Interface
APSS	Accessible Property Screening System
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
EDS	Explosive Detection System
EDSCB	Explosive Detection Systems for Cabin Baggage
EOS	European Organisation for Security
EU	European Union
GDPR	General Data Protection Regulation
HFOD	Hochschule für den Öffentlichen Dienst in Bayern
IATA	International Air Transport Association

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

IBM	Integrated Border Management
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
NEMA	National Electrical Manufacturers Association
NIS	Network and Information Security
OA	Open Architecture
OH&S	Occupational Health and Safety
PESTLE	Political, Economic, Social, Technological, Legal, and Environmental
ROI	Return on Investment
SDE	Smiths Detection Germany
SDO	Standards Development Organisation
SERI	State Secretariat for Education, Research, and Innovation (Switzerland)

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

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

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

1 INTRODUCTION

1.1 PURPOSE AND SCOPE

The BAG-INTEL project aims to enhance customs security and operational efficiency through AI-driven solutions, digital twin technologies, and real-time decision-support systems. The project responds to the growing need for automated customs risk assessment, baggage reidentification, and contraband detection in European airports and border control points. By integrating advanced AI methodologies, the project seeks to streamline customs operations, reduce the workload on human personnel, and improve detection accuracy. This deliverable, D6.3: Standardisation, Exploitation, and Sustainability Strategy and Plan, outlines the project's market positioning, competition analysis, and long-term exploitation plans. It provides a structured framework for ensuring BAG-INTEL's technological solutions' sustainability and commercial viability.

Furthermore, this deliverable is designed to address the key aspects of existing relevant standards, the key standards development organisations and very clear stakeholder input and feedback is looking at potential gaps and opportunities to develop and / or utilise standards in addressing important aspects of customs security and control of passenger baggage.

1.2 PURPOSE AND SCOPE

This deliverable aims to define the strategic roadmap for the standardization, exploitation, and sustainability of the BAG-INTEL project outcomes. It aims to identify key exploitable results developed within the project and assess their commercialization potential. A preliminary market and competition analysis is conducted to evaluate market dynamics, key players, and the competitive advantages of BAG-INTEL technologies. The document also defines challenges to market entry, including regulatory barriers, integration constraints, and financial limitations. Additionally, it establishes a sustainability and exploitation plan to ensure the long-term adoption and scalability of BAG-INTEL's technologies. The deliverable provides a structured framework for stakeholders, industry partners, and policymakers to understand the project's commercial and operational impact and to support its successful deployment in the security and customs sectors.

In addition, this deliverable seeks to also identify aspects that could be managed via the development of further standards, while at the same time charting those standards which are clearly in us.

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

This deliverable, D6.3: Standardisation, Exploitation, and Sustainability Strategy and Plan, is part of Work Package 6 (WP6: Dissemination, Communication, Exploitation, and Sustainability). WP6 plays a crucial role in ensuring that the technological advancements of the BAG-INTEL project transition beyond research and development into market-ready solutions. It defines the framework for dissemination, stakeholder engagement, exploitation, and long-term sustainability strategies that will drive the adoption of AI-powered customs control technologies. The deliverable focuses on standardization efforts, market positioning, business models, and regulatory considerations for integrating BAG-INTEL solutions into customs and security operations across European and international markets.

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

WP6 is directly connected to other work packages, as its exploitation and standardization efforts are based on the results generated across the project lifecycle. WP1 (Project Coordination and Management) provides oversight, ensuring alignment between project objectives and execution. WP6 utilizes insights from WP1 to structure the exploitation strategy by the overall project vision.

BAG-INTEL's technological foundation is developed in WP2 (System Architecture and Technology Development) and WP3 (Core System Development and Integration), which deliver the AI-powered customs security tools, digital twin models, and decision-support systems that form the basis for the project's marketable outputs. The exploitable results identified in this deliverable are derived from the advancements made in these work packages. WP6 ensures these technologies are positioned correctly in the market, with sustainable business models and industry adoption strategies.

WP4 (Pilot Implementation and System Validation) is critical in informing this deliverable's exploitation and sustainability strategy. The real-world deployment and validation of BAG-INTEL solutions in selected airports provide crucial data on performance, regulatory alignment, and user acceptance. WP6 integrates these findings into the market entry and competition analysis, ensuring that lessons learned from pilot deployments shape the commercial roadmap.

WP5 (Standardization, IPR, and Ethics) is another key contributor to WP6. The legal, ethical, and intellectual property (IPR) frameworks developed in WP5 influence how BAG-INTEL solutions can be commercialized and integrated into existing regulatory structures. The findings from WP5 regarding compliance with EU customs policies, AI ethics, and data governance are incorporated into this deliverable to ensure that market adoption strategies align with legal requirements and best practices in AI governance.

The relationship between WP6 and these work packages ensures that the project outcomes are effectively positioned for market adoption. The insights gathered from WP2, WP3, WP4, and WP5 contribute directly to the strategic planning of WP6, shaping the recommendations for standardization, business models, and regulatory compliance. This deliverable synthesizes findings from across the project to provide a comprehensive exploitation and sustainability strategy, ensuring that BAG-INTEL solutions can be successfully deployed in real-world customs security operations.

1.4 METHODOLOGY AND STRUCTURE OF THE DELIVERABLE

The methodology used in this deliverable combines qualitative and quantitative approaches to assess the market, competitive landscape, and strategic opportunities for the BAG-INTEL project. The analysis is based on data collected from industry reports, regulatory frameworks, expert consultations, and prior research conducted within the project. Assessing key market trends and drivers relies on industry insights, trade statistics, and technological adoption studies. The competitive landscape analysis includes benchmarking against existing customs control technologies, examining strengths, weaknesses, and differentiators. Market entry challenges are studied by regulatory compliance requirements, technological integration constraints, and financial considerations that impact the adoption of AI-driven customs security solutions.

The deliverable is structured to provide a clear progression from market analysis to implementation strategies. The introduction outlines the purpose, scope, and approach taken within Work Package 6, highlighting its relation to other work packages. The following section presents an analysis of key market trends and growth drivers that influence the adoption of AI-powered customs security solutions. This is followed by assessing the competitive landscape, identifying key players, existing solutions, and BAG-INTEL's competitive positioning. The document then examines market entry

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

challenges, discussing regulatory barriers, operational constraints, and financial considerations. The following section focuses on the strategic implications and recommendations, outlining exploitation, commercialization, and standardization pathways. The deliverable also includes an analysis of the socio-economic impact of BAG-INTEL, incorporating a PESTLE and SWOT analysis to evaluate external factors influencing the project's implementation and sustainability. The stakeholder identification and engagement strategy section provides insights into the key actors involved in adopting and implementing BAG-INTEL's solutions. Finally, individual and joint exploitation plans are presented, detailing how project partners intend to commercialize and sustain the project outcomes. The document concludes with a summary of findings and recommendations for ensuring the long-term impact and market success of BAG-INTEL technologies.

A second major part of the deliverable is dedicated to the standardisation question including the identification of standards in use, the relevant standards development organisations and looking at potential opportunities for useful standardisation in the future. Again, and a key part of this is the results from the survey that was conducted with a broad set of important stakeholders' groups, especially focused upon the end users in BAG-INTEL (namely customs organisations). Furthermore, the stakeholders involved in the survey have included, but are not limited to: Law Enforcement, Government Agencies, Equipment Manufacturers, Technology Providers (including software technology), Consultants / Consulting Organisations, Services Providers, and as previously mentioned Customs Organisations. A number of conclusions with respect to standardisation have been drawn from the results and these are clearly explained in the later part of this deliverable.

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

2 EXPLOITABLE RESULTS DESCRIPTION

The BAG-INTEL project is designed to generate various exploitable results (ERs) that contribute to the modernization and efficiency of customs control operations through AI-powered solutions, digital twins, and advanced security technologies. These results are critical for enhancing contraband detection, baggage reidentification, and customs risk assessment, ultimately supporting the project's goal of optimizing customs procedures in European airports.

This section presents a comprehensive overview of the exploitable results collected from project partners. It highlights the technological advancements developed within the project, their Technology Readiness Levels (TRLs), commercialization potential, and market applications. The results include software solutions for AI-driven risk analysis, digital twin modeling for customs decision-making, AI-enhanced baggage screening technologies, and secure communication systems for data exchange.

By systematically identifying and categorizing these key exploitable results (KERs), the project ensures that innovations are effectively transitioned from research to practical implementation and commercial exploitation. These ERs are assessed for their business potential, alignment with regulatory frameworks, and integration into broader security ecosystems, ensuring long-term sustainability and impact within customs, airport operations, and border security.

2.1 EXPLOITATION PLANNING OF THE BAG-INTEL PROJECT

The BAG-INTEL project is designed with a robust exploitation plan to ensure that the project results are effectively transitioned into practical applications with lasting impact. The exploitation planning framework addresses market needs, stakeholder engagement, and sustainability, providing a comprehensive roadmap for maximizing the value of the project outcomes.

Exploitation Plan and Strategy

The project incorporates a detailed exploitation plan, which defines the market strategies, return on investment (ROI) projections, and actionable steps required to sustain the results during and beyond the project lifecycle. This plan is essential for aligning BAG-INTEL's technological innovations with real-world needs, ensuring they can be successfully introduced to relevant markets. Building an initial business model, the plan evolves dynamically based on ongoing project insights and stakeholder feedback, reflecting a strong focus on aligning the outcomes with tangible market opportunities.

Joint Exploitation Agreement

A core component of the exploitation planning is developing a joint exploitation agreement among the project partners. This agreement complements the Consortium Agreement and lays out clear guidelines on intellectual property rights (IPR) management and the responsibilities of each partner. It also facilitates joint and individual exploitation of the results, ensuring that all partners can effectively benefit from and contribute to the exploitation process. This agreement creates a cohesive framework for the project's sustainability by defining clear roles and responsibilities across different exploitation channels.

Market and Business Model Analysis

The project analyses market opportunities, stakeholder ecosystems, and value chains to ensure successful market adoption. These analyses aim to identify key segments and evaluate the competitive

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

landscape, helping refine strategies for introducing BAG-INTEL solutions. The business model also considers the evolving needs of stakeholders, such as customs authorities and airport operators, enabling the project to tailor its approach to specific industry requirements.

Return on Investment (ROI) Analysis

A comprehensive ROI analysis evaluates the expected benefits of adopting BAG-INTEL solutions. This analysis goes beyond financial gains, incorporating social and safety aspects such as improved efficiency in customs operations, enhanced security, and reduced risks for citizens. By quantifying these benefits, the ROI analysis helps validate the project's impact and strengthens its value proposition for stakeholders.

Stakeholder Involvement

Engaging external stakeholders is a vital part of exploitation planning. Tailored activities are initiated to involve potential end-users, industry experts, and market participants. These efforts include leveraging pilot implementations to validate the exploitation plan, demonstrating the effectiveness of the solutions, and gathering valuable feedback. This active involvement ensures that the exploitation strategies are aligned with real-world needs and priorities, increasing the likelihood of adoption.

Exploitation Pathway and Milestones

The exploitation planning is structured into three distinct phases, each with specific milestones to guide the transition of project results to the market. These phases ensure a systematic approach to deployment, beginning with early-stage exploitation activities and culminating in a go-to-market strategy that extends beyond the project's duration. This phased approach provides a clear timeline for implementation and allows for adjustments based on ongoing feedback and market developments.

Roles and Responsibilities in Exploitation

Given BAG-INTEL's complex ecosystem, specific roles are assigned to project partners to streamline the exploitation process. Partners are categorized as sellers, service providers, or owners, each with distinct responsibilities. Sellers focus on marketing and commercial activities, service providers handle deployment and maintenance, and owners are responsible for developing and delivering specific components. This clear definition of roles ensures accountability and efficiency throughout the exploitation process.

Delivery and Deployment Models

BAG-INTEL considers two primary delivery models: on-premises and off-premises (as-a-service). The on-premises model involves hosting the software solution on customer premises, which is often preferred by authorities due to security and legal constraints—the off-premises model leverages cloud-based solutions, offering scalability, flexibility, and reduced capital investment. The choice of model depends on customer requirements and regulatory considerations, ensuring that BAG-INTEL solutions can adapt to diverse deployment scenarios.

Licensing and Pricing Policies

Licensing and pricing strategies are designed to maximize accessibility while ensuring sustainability. Licensing options include usage-based models, such as concurrent users or the number of cases handled, while pricing policies prioritize simplicity, fairness, and future-proofing. These strategies are

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

developed to align with industry the best practices and provide flexibility for various stakeholder needs.

Individual Exploitation Plans

In addition to the overarching exploitation strategy, each consortium partner develops individual exploitation plans tailored to their specific objectives. Industry and SMEs focus on integrating project results into market-ready solutions and enhancing their position in the security sector. Law enforcement agencies and customs authorities prioritize operational improvements and continued evaluation of project outputs. Research and academic institutions leverage the results to enhance their research capacities, integrate findings into educational programs, and foster technology transfer initiatives.

Impact Assessment and Standardization Activities

The impact of BAG-INTEL solutions is assessed across social, security, and economic dimensions. This includes evaluating improvements in customs operations, citizen safety, and reducing illegal activities. Furthermore, the project explores opportunities for pre-standardization activities, aiming to align the solutions with existing standards and influence the development of new ones. This focus on standardization enhances the long-term applicability and scalability of the project outcomes.

The exploitation planning framework of BAG-INTEL reflects a strategic and dynamic approach to ensuring that the project's innovative solutions achieve their full potential during and after completion.

2.2 EXPLOITABLE RESULTS (ERS) GATHERED FROM PROJECT PARTNERS

As part of the BAG-INTEL project, we collected and analysed Exploitable Results (ERs) submitted by the project partners to highlight the innovative outputs and their potential impact. This structured effort aimed to ensure that all results produced during the project were effectively aligned with its goals, assessed for readiness, and prepared for practical application or commercialization.

The collection process involved a specially designed exploitation tool (Exploitation Tool) based on Excel, which provided a unified framework for partners to submit detailed information about their contributions. Each partner was asked to complete a comprehensive set of fields, including the ER's name, category, short description, progression of the Technology Readiness Level (TRL), strengths, weaknesses, market opportunities, risks, and the envisioned path to market.

A key focus was understanding how these results could be leveraged within the organizations involved, such as extending product portfolios, developing new solutions, or addressing specific market needs. Additionally, the data provided insights into the ERs' competitive positioning, highlighting areas of innovation and identifying potential challenges, such as market competition or resource dependencies.

This initial evaluation is a preliminary approach to collecting and organizing Key Exploitable Results (KERs). A detailed assessment of all ERs will be conducted in a subsequent phase to finalize the selection of KERs. This phased process ensures a thorough and strategic review, allowing for the identification of results with the highest potential for impact and scalability.

Below, we present the Exploitable Results (ERs) collected from the project partners for a detailed review.

ER1 - Multimethod Modelling.

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

Multimethod modeling is a methodology on which the digital twins are based. Suggested and owned by STAM, this methodology is associated with Tasks 2.6 and 4.4 and started and ended the project at TRL 8. Its commercial exploitation is categorized as a business opportunity due to its versatility and ease of reproducibility in various contexts. The methodology excels in replicating the behavior of different systems involving flows such as people, vehicles, materials, and products. However, its implementation and validation can be time-consuming. With a wide potential market due to its scalability, it is threatened by the increasing adoption of AI in similar fields. While competition exists, this methodology is one of the most comprehensive available. It targets markets where understanding complex systems' interactions and dynamics is crucial and has already been applied commercially. The expected ROI depends on the solutions developed, ranging from €30-80 million depending on the solution built on the basis of the methodology. This methodology is already embedded in STAM's workflow and is considered a Key Exploitable Result (KER).

ER2 - DSS for Customs.

The DSS for Customs is a Decision Support System based on the Digital Twin developed under BAG-INTEL. Suggested and owned by STAM, it is linked to Tasks 2.6 and 4.4, starting the project at TRL 4 and reaching TRL 6. Classified under commercial exploitation, the DSS operates in a highly competitive market with diverse approaches but stands out due to customizable KPIs and the ability to perform "what-if" scenarios. While these strengths improve system awareness, the DSS requires further enhancements to be more competitive. Opportunities lie in its adaptability to multiple stakeholders in critical infrastructure sectors like airports. However, the lack of stakeholder interest or support threatens its adoption. Competitively, the DSS offers tailored solutions to project stakeholders, targeting airport managers, security, and police. With an estimated time to market of 1 year, its expected ROI is €30-80k, plus annual fees of 5%. This DSS is already part of STAM's portfolio and is considered a KER.

ER3 - AI-Vision-Based Reidentification of Luggage for Customs Inspection (AI4bagReID).

AI4bagReID focuses on bag reidentification and supporting customs in identifying high-risk luggage. Suggested by LTA and INSA and owned by LTA, this software solution is tied to Tasks 3.3 and 4.2. It has significant commercial potential, starting at TRL 4 and ending at TRL 6, as no similar solutions currently exist in airports. Its ability to reidentify bags and identify high-risk ones is a key strength, although achieving satisfactory reidentification levels remains uncertain. AI4bagReID can collaborate with any scanner provider, meeting customs requirements, offering broad compatibility. Potential risks include failing to reach expected performance levels and RFID tagging, while an alternative poses operational challenges. Customs agencies are the primary market, with an estimated time to market of 1-3 years and expected costs of €50-100k, including maintenance fees. By extending LTA's portfolio, this tool is considered a KER.

ER4 - Connection-Analysis-Based Risk Assessment (ConnRisk).

ConnRisk is a tool for deriving risk assessments based on suspicious connections across databases, suggested and owned by LTA. Associated with Tasks 4.1 and 4.2, it started at TRL 5 and reached TRL 7 by the project's end. Its commercial exploitation potential is significant, especially within the BAG-INTEL ecosystem. ConnRisk's strength lies in its ability to derive connections from diverse data sources. However, restricted access to law enforcement databases could limit its utility. Opportunities include investigative applications in organized crime and fraud cases, while risks stem from database restrictions. With no current competition, ConnRisk targets customs within the BAG-INTEL framework, with a time to market of less than 1 year. While not marketed separately, it is integrated into BAG-INTEL solutions, and its development for operational use makes it a KER.

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

ER5 - Methodology for Operational BAG-INTEL (CustomsBagControl).

The CustomsBagControl methodology provides a framework for implementing and operating BAG-INTEL solutions. Suggested and owned by LTA, it relates to Task 4.3, starting at TRL 4 and concluding at TRL 6. This business-oriented methodology is crucial for airport operational setups and has significant market potential due to its role in sustainable luggage reidentification and customs control. Its strength lies in addressing all operational issues for configuration and operation, although it faces challenges as no similar methodologies currently exist. Targeting EU and global customs agencies, the methodology is expected to reach the market within 1-3 years. Although the ROI remains undefined, it will be marketed as a comprehensive enterprise for BAG-INTEL. Establishing a production and commercialization team is part of the path to market, and it is considered a KER.

ER6 - AI-Powered Decision Support System (DSS).

The AI-powered DSS enhances customs efficiency through AI-driven decision-making capabilities. Owned by LTA and associated with Tasks 2.1, 3.3, and 4.1, this system shows high adaptability and excels in real-time data processing. However, its dependence on data for effective operation is a critical weakness. Opportunities for expansion into global customs systems highlight its scalability, while the potential risks tied to data dependency remain a challenge. The primary targeted markets are customs and logistics, with a time to market estimated at 1 year. This DSS is designed to address operational needs but was not explicitly marked as a Key Exploitable Result (KER) in the provided dataset.

ER7 - Advanced Detection Systems.

This hardware solution offers high-precision contraband detection technology and is linked to Tasks 2.4 and 3.2. Its superior detection accuracy represents a significant strength, but the high implementation costs pose a challenge. Opportunities exist in partnerships with global airports, while market threats center around affordability and competition. The targeted customers include customs and airport operators, with a time to market of 2 years. While details on ROI or explicit KER designation were not provided, the system offers considerable potential to modernize detection capabilities in security contexts.

ER8 - Knowledge Graph Database and Intelligent Analysis.

This methodology leverages advanced data models for DSS and risk assessment, suggested by UGR and linked to Tasks 2.4 and 4.5. Starting at TRL 4 and reaching TRL 6, it provides significant knowledge support across airport systems, with exploitation opportunities in consulting, research, and licensing services. Strengths include a robust research foundation, but real data privacy limitations present weaknesses. Opportunities involve licensing to analytics companies, while threats include data availability challenges. Its targeted market spans EU customs agencies, global software developers, and associated industries. The estimated time to market is 3 years, with pathways to collaboration with industry partners and participation in innovative ecosystems. This methodology is considered a KER.

ER9 - Integrated Customs Information System.

The Integrated Customs Information System is a software solution providing a unified customs data integration platform. It is owned by LTA and is associated with Tasks 3.2 and 4.1. It offers high scalability as a strength but faces complexity in integration as a weakness. Opportunities exist for expansion into other hubs and logistics networks, but the dataset lacks specific information on threats. The targeted customers include customs and logistics companies, with a time to market of 2 years.

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

Although ROI estimates and KER status were not provided, the system aligns well with broader modernization goals in customs operations.

ER10 - CCTV AI Detection Integrator.

This software integrates CCTV technology proposed by PSI and AI object detection modules developed by CEA. It is tied to Tasks T3.1, 3.4 and 4.3, starting at TRL 3 and reaching TRL 6. Its versatility and scalability make it a strong contender in diverse airport environments, while high customization efforts pose challenges. Opportunities include expansion into additional airports, while threats arise from varying environmental demands and potential operational limitations. The targeted customers include customs and airport operators, with an estimated time to market of 2 years. Specific ROI figures were not detailed, but the tool holds potential as part of broader modernization efforts.

ER11 - Secure Communication Systems.

This software ensures secure data sharing in customs operations and is owned by ICCS, connected to Tasks 3.5 and 4.2. The system is built on robust encryption, a key strength, but potential integration hurdles could slow its adoption. Opportunities exist in broader security applications, extending beyond customs to other sectors requiring secure communication. The targeted market includes customs and security agencies, with an estimated time to market of 1 year. The tool is considered a Key Exploitable Result (KER), highlighting its strategic importance in the project's objectives.

ER12 - Advanced Baggage Scanning System.

This hardware solution introduces high-resolution scanners integrated with AI for enhanced baggage scanning. Proposed and owned by SDE, the system is associated with Tasks 2.4 and 3.5, starting at TRL 6 and advancing to TRL 7. Its leading detection accuracy is a significant strength, though the high implementation cost is a notable weakness. Opportunities include expanding into global security markets, with potential benefits from additional training data. The competition contains other security CT vendors and adjacent technologies like X-ray diffraction. Targeted customers are airports and customs agencies, with a time to market of 1-2 years. ROI depends on the availability and completeness of training data. The system will extend SDE's product portfolio with new detection algorithms, which are considered a KER.

ER13 - AI-Based Risk and Decision Support Tool.

This software offers intelligence for decision-making in customs operations, developed by EXUS and linked to Tasks 4.1 and 4.5. Its ability to provide actionable intelligence is a significant strength, but its dependency on data for training presents a challenge. Opportunities for expansion into other sectors highlight its adaptability, though threats were not specified in the dataset. The target market is customs, with an estimated time to market of 2-3 years. While the dataset does not explicitly state if this is a KER, the tool aligns with the project’s broader goals of enhancing customs efficiency.

ER14 - Customs Bag-Risk Management.

This software tool is designed to manage the risk of contraband in luggage, suggested and owned by LTA. Associated with Tasks 3.1, 4.1, and 4.2, it started at TRL 4 and concluded at TRL 6. The tool fuses risk indicators for comprehensive bag-risk assessment, a clear strength. However, its dependency on real-time data represents a challenge. Opportunities include general customs and security risk assessment applications, targeting government and customs markets. The tool has a time to market of 2 years and is initially marketed as part of BAG-INTEL solutions. It is considered a KER, emphasizing its role in advancing risk management capabilities.

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

ER15 - Training and Education Modules for Customs.

These modules provide comprehensive training for customs officials to optimize operations, proposed by HFOD and associated with Task 5.3. The modules offer detailed educational content, a significant strength, but they rely heavily on continuous content updates, posing a challenge. Opportunities exist to expand into global customs training programs. However, the low degree of readiness of technical solutions developed by partners may pose a threat. The targeted market includes customs authorities, with an estimated time to market of 1 year. The modules are considered a KER, showcasing their critical role in enhancing the skills of customs officials.

ER16 - Optimal Probabilistic Bijective Mapping (OPBM) for Luggage Reidentification.

This methodology focuses on probabilistic bag reidentification based on matching scores for a collection of bags. Proposed and owned by INSA, it is associated with Tasks 4.2, 4.1, and 3.3, starting at TRL 4 and ending at TRL 6. The originality and portability of the mathematical method offer significant potential for applications in airports and other engineering sectors. Its strength lies in optimizing reidentification processes, though its success rate depends on practical implementation and performance targets (expected at 80%). Opportunities exist for implementation in AI-based photo-identification systems, but the method's performance depends on the uncertainty of matching scores. Currently, no direct competition exists in the field of random bijective mapping. The targeted market includes customs agencies as part of BAG-INTEL solutions and academic sectors for risk modeling and analysis. The time to market is estimated at 1-3 years, with potential for enhancing INSA's R&D in engineering applications. This methodology is considered a Key Exploitable Result (KER).

ER17 - Multi-Risk Indicators Statistical Weighting and Aggregation of Qualitative and Quantitative Data.

This methodology focuses on building a global risk indicator system for inspection decision-making by integrating data of different natures. It is suggested by INSA, with contributions from LTA and UGR, though detailed task associations, TRL levels, and commercial pathways were not fully provided in the dataset. The methodology holds potential for advancing customs operations by improving risk assessment capabilities, offering new opportunities for collaborative innovation. However, further details are needed to evaluate its competitive positioning and specific exploitation strategies. The dataset did not explicitly confirm its status as a KER.

ER18 - Providing CCTV for Object Detection.

This methodology involves setting up CCTV systems in customs zones for AI-based object detection. Proposed by PSI with contributions from CEA, it is linked to Tasks T3.1, 3.4 and 4.3, starting at TRL 2 and reaching TRL 6. The methodology stands out by addressing the unique needs of providing video data for AI detection modules instead of human-monitored systems. Its strength lies in the flexibility to adapt to various interior and exterior environments, though practical implementation in diverse airport settings remains challenging. Opportunities include expanding its use to other airports, targeting customs and airport operators. The estimated time to market is 1-2 years, with the potential for learning and optimizing deployment configurations. While the dataset does not explicitly list this methodology as a KER, it significantly advances customs efficiency through technology integration.

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

3 IPR MANAGEMENT

Effective Intellectual Property Rights (IPR) management is crucial for ensuring the protection, ownership, and sustainable exploitation of the innovations and technological advancements developed within the BAG-INTEL project. Given the diverse contributions of consortium partners, a clear and structured IPR framework is essential to define ownership, access rights, licensing strategies, and commercialization pathways for the project's results.

This section outlines the IPR management strategy adopted in BAG-INTEL, detailing the identification of Background and Foreground Intellectual Property, the allocation of ownership, and the mechanisms for safeguarding and exploiting key innovations. It also establishes a framework for collaborative exploitation, ensuring that all partners benefit equitably from the project's outputs while complying with European regulatory frameworks on intellectual property, data security, and AI ethics.

By implementing a comprehensive IPR strategy, BAG-INTEL aims to protect proprietary technologies, facilitate knowledge transfer and commercialization, and ensure the long-term sustainability of AI-powered customs solutions across European and global markets.

3.1 BACKGROUND IP

In the context of the project BAG-INTEL, identifying and managing Background Intellectual Property (IP) is crucial for ensuring that the participating partners' existing knowledge, technologies, and methodologies are effectively utilized in developing and implementing the project's objectives. Background IP refers to pre-existing data, know-how, technologies, or tools brought into the project by the partners and are essential for achieving project deliverables, particularly for generating new results and innovations.

Data was collected using a standardized methodology to facilitate a comprehensive understanding and proper management of Background IP. Each project partner was requested to provide detailed information about their existing Background IP relevant to the project's scope. This information was gathered using a structured questionnaire, which included the following fields: the Background IP number, name of the technology or know-how, ownership details, a description of the Background IP, its intended use within the project, and any specific restrictions or conditions for its use or exploitation. This approach ensured consistency and completeness in documenting the contributions of all partners.

The data collected has been carefully analyzed to identify the relevance and applicability of each Background IP to the project activities. This section provides a detailed account of the Background IP contributed by the partners, categorized from BG1 to BG16. Each entry includes the background number, name, owner, description, project utilization, and any associated restrictions or conditions for use and exploitation. The following analysis forms the foundation for effectively integrating Background IP into the BAG-INTEL project and ensures compliance with intellectual property management protocols:

BG1 - AI technology for visual baggage reidentification (AI4bagID): The background, owned by LEGIND TECHNOLOGIES AS (LTA), is a technological solution at TRL 3. It uses advanced deep learning technologies to measure the similarity between observed luggage and those selected for inspection. The process involves segmenting images, extracting identifying signatures for visual reidentification, and tracking luggage based on camera images. It will be utilized within Task 3.3 of the project. Background is provided solely for use within the project, with access granted only to necessary information for project activities. Access to the software source code will not be granted. Exploitation

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

outside the project requires agreement with LTA, and the source code will remain inaccessible in all cases.

BG2 - Graph technology for finding connections in large datasets (ConFind): LEGIND TECHNOLOGIES AS (LTA) owns this background, a TRL 7 software tool for identifying direct and indirect connections between entities in large datasets. It calculates the overall certainty of these connections. The project will be used in Task 4.1 to detect connections between travelers and organized crime and assess risks associated with such connections. The background is available for project use only, with access limited to necessary information. Source code access is excluded. For exploitation purposes, agreements with LTA are required, and access to the source code will not be permitted.

BG3 - PIXANO: Owned by CEA, PIXANO is software for image annotation with registered versions and licenses under CeCILL-C and BSD-3. Other parties do not need the background for their project actions, and access rights will not be granted unless mutually agreed upon. Use in exploitation scenarios requires a separate license agreement, with no access to source or object code provided. Restrictions also apply based on third-party contracts.

BG4 - UDA-ReID: CEA-owned UDA-ReID includes software components for training neural networks for object reidentification using unsupervised domain adaptation. Other parties do not require the background for implementing actions within the project, and no access rights will be granted unless agreed otherwise. Exploitation requires a separate license agreement, with no access to source or object code granted. Limitations related to third-party rights apply.

BG5 - UDA-HP: CEA owns UDA-HP, which consists of software components for training neural networks for human parsing through unsupervised domain adaptation. Similar to BG4, other parties do not need this background for project actions, and access will not be granted without specific agreements. Exploitation scenarios require a separate license agreement; source or object code access will not be provided. Conditions based on third-party agreements are applicable.

BG6 - HPTR: Owned by CEA, this background involves software for human parsing registered under APP No. iddn.fr.001.050008.000.S.P.2022.000.20900. Other project parties do not require the background to implement their actions, and access rights will not be granted unless mutually agreed upon. A separate license agreement is needed for exploitation; no source or object code access will be provided. Restrictions related to third-party contracts apply.

BG7 - "Apprentissage automatique sans annotation amélioré par regroupements adaptatifs en ensemble ouvert de classes": This French patent, owned by CEA, was filed on June 4, 2021, under No. FR2105890 (published as No. FR3123748). The background is unnecessary for other parties' project actions, and access will not be granted unless otherwise agreed. Exploitation requires a separate license agreement, with no source or object code access provided. Third-party rights and agreements impose specific limitations.

BG8—Expertise and know-how: STAM owns expertise and know-how in multi-method and agent-based simulation models of complex systems, processes, and flows. This background will be used to develop digital twins and decision support systems for customs in Tasks 2.6 and 4.4. Access is limited to project use, and knowledge cannot be transmitted outside project activities. Exploitation requires legal consent from STAM, with possible financial or copyright terms to be discussed.

BG9—Software components, applications, and libraries: PSI owns this background, which consists of software components, applications, and libraries previously developed by PSI Software. Use is limited to project implementation under existing PSI licensing terms. Access to source code is excluded, and

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

any conflicts with PSI software licensing terms will favor PSI's conditions. Exploitation is subject to existing licensing terms and specific agreements, with restricted source code access.

BG10 - PSI know-how and expertise: PSI has expertise in software implementation, including analysis, design, development, testing, training, and technical support, as well as AI and baggage handling systems. This know-how will be available for consulting, usage, and adaptation within the project. Access is strictly limited to the project period, and exploitation beyond this period is not allowed. Intellectual property rights for modifications made during the project will remain with PSI.

BG11 - IAPR (Independent Authority for Public Revenue) part: The background, owned by IAPR, includes expertise and processes of the Hellenic Customs, focusing on customs, tariff, and tax legislation, as well as rules related to Excise Duty and VAT. Access rights must be requested and are only granted in duly justified cases. No personal or commercial data will be transmitted, and all data must be anonymized. These restrictions also apply to exploitation purposes, ensuring that data remains anonymized and protected.

BG12 - Customs Authority / End User: AEAT owns this background, which provides expertise and know-how on customs processes and flows within a Customs Area. According to Article 95 of the Spanish General Tax Law, the use and transfer of data with tax significance are restricted, as such data is classified as reserved. These restrictions apply to project implementation and exploitation activities, in compliance with data protection regulations.

BG13 - Information and data concerning current systems, possible threats, and identified gaps: This background is owned by the Ministerio del Interior (Guardia Civil, GUCI) and comprises information and data on current systems, threats, and gaps based on GUCI's expertise. Without written permission, data cannot be transferred to third parties or used beyond the project's scope. For exploitation, explicit written permission is also required to use GUCI's data, name, or logo for commercial purposes.

BG14 - Information and data for real scenarios testing definition and actual exercises: Owned by GUCI, this background consists of data used for accurate scenario testing and exercises. Like BG13, GUCI's data cannot be transferred or used outside the project without explicit permission. Permission is also required for commercial exploitation, including using GUCI's data, name, or logo.

BG15 - Information and data to share: This background, owned by GUCI, consists of anonymized data from open sources. No data or information from open or closed operations will be shared. These restrictions ensure that only anonymized, non-sensitive data is utilized within the project. The same restrictions apply to exploiting this data and maintaining strict confidentiality.

BG16 - Optimal Probabilistic Bi-jective Mapping for the reidentification of luggage for customs inspection (OPBM): Owned by INSA, this background provides a method for bag reidentification within the BAG-INTEL context, based on matching probabilities of a collection of bags. It will be implemented in the risk-based inspection decision support tool of BAG-INTEL. Access is required to the matching scores determined by the AI-based reidentification module. There are no specific restrictions or conditions for exploitation of this background.

3.2 TYPES OF KNOWLEDGE

The BAG-INTEL project generates diverse types of knowledge that are essential for its success and sustainability. These include scientific, technological, operational, market, and societal expertise and insights into ethical and legal frameworks. Scientific knowledge is derived from the research and development of AI-powered tools, methodologies, and algorithms designed explicitly for customs

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

control and contraband detection. This knowledge underpins the technical advancements achieved by the project and serves as the foundation for further innovation.

Technological knowledge encompasses the system architectures, software algorithms, and digital twin technologies developed within the project. These technologies provide innovative solutions for baggage reidentification and contraband detection, enabling customs authorities to enhance efficiency and accuracy. Operational knowledge is gained through deploying and optimizing the BAG-INTEL system in real-world settings, such as pilot demonstrations in selected airports. This includes understanding the workflows, resource allocation, and system integration required for effective implementation.

Market and societal knowledge focus on end-user requirements, societal impact, and market strategies. This type of knowledge is informed by engagement with stakeholders, including customs authorities, airport operators, and industry experts, to ensure that the solutions developed address real-world challenges and priorities. Additionally, the project contributes to ethical and legal knowledge by adhering to privacy-by-design principles, ensuring data protection compliance, and integrating ethical guidelines for AI technologies. This holistic approach to knowledge generation and management ensures that the project's outcomes are robust, impactful, and aligned with the needs of stakeholders and society.

3.3 RECORD OF INTELLECTUAL PROPERTY ASSETS

The BAG-INTEL project has established a structured framework for cataloging and managing its intellectual property (IP) assets. This systematic approach ensures that all innovations and contributions from the consortium partners are appropriately documented, protected, and utilized effectively.

The project's intellectual property assets are broadly categorized into background IP and foreground IP. Background IP consists of preexisting methodologies, datasets, and tools brought into the project by the consortium partners. These include proprietary software algorithms, AI frameworks, and domain-specific expertise that provide the foundation for the project's innovations. For instance, partners have contributed specialized knowledge in digital twin modeling, contraband detection techniques, and image processing algorithms that have been adapted and enhanced during the project.

Conversely, foreground IP encompasses all new and original outputs generated directly from the project activities. This includes advanced detection algorithms, decision-support systems tailored to airport environments, and digital twin technologies explicitly designed for baggage management. Additionally, training modules for customs authorities and new methodologies for risk assessment and luggage reidentification represent significant IP assets developed during the project.

To ensure effective management, all IP assets are recorded in a centralized database maintained by the consortium. This database includes detailed descriptions of each asset, its owner(s), associated background IP, and any dependencies. For example, each partner has provided information on their contributions' technology readiness levels (TRLs), highlighting their potential for exploitation and further development.

A key component of the IP asset record is classifying assets by their potential applications and market relevance. This allows the consortium to prioritize results with the highest impact and scalability, such as AI-powered tools that address customs challenges and operational inefficiencies. Moreover, the

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

project's IP management framework ensures compliance with ethical, legal, and regulatory requirements, providing clear data protection and usage rights guidelines.

3.4 OWNERSHIP SCHEMAS

The ownership schemas within the BAG-INTEL project have been meticulously defined to ensure clarity and fairness in the management and exploitation of intellectual property (IP). These schemas are grounded in the Consortium Agreement and aim to delineate ownership rights, responsibilities, and access conditions for Background and Foreground IP.

Ownership of project results is categorized as follows:

1. **Sole Ownership**: When a result is generated exclusively by one partner without significant contributions from others, that partner retains sole ownership of the result. This is applicable, for instance, to proprietary algorithms or software components developed independently by a single partner during the project. The owner can exploit these results commercially or otherwise, provided it does not conflict with the obligations outlined in the Consortium Agreement.

2. **Joint Ownership**: For results developed collaboratively by multiple partners, ownership is shared among the contributors based on their respective input levels. Jointly owned results require precise usage, exploitation, and licensing agreements. Typically, the joint owners grant each other non-exclusive, royalty-free licenses for internal research and development purposes. Any commercial exploitation of such results requires consent from all joint owners and fair and equitable benefit-sharing arrangements.

3. **Access Rights**: To facilitate the project's objectives and ensure smooth collaboration, partners are granted access rights to Background and Foreground IP under specific conditions:

    - **Background IP**: Access is provided royalty-free for research activities directly related to the project. For commercial purposes, access is granted under fair and reasonable terms.

    - **Foreground IP**: Access rights are granted to all partners for internal research and development activities. Commercial access follows a similar model to Background IP, ensuring fair compensation for the owning partner(s).

4. **Third-Party Access**: Third parties such as subcontractors or external stakeholders may sometimes require access to specific IP. Strict confidentiality agreements govern such access and must comply with the project's IP management framework.

The ownership schemas also address scenarios involving potential disputes or ambiguities. A designated IP management team oversees conflict resolution, ensuring alignment with the Consortium Agreement and the project's overarching goals. This structured approach to ownership ensures transparency, fosters collaboration, and maximizes the impact of BAG-INTEL's innovations.

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

3.5 IPR MATRIX

The IPR Matrix below provides a detailed overview of intellectual property ownership, access rights, and exploitation plans within the BAG-INTEL project. This structured framework ensures clarity and facilitates effective collaboration and commercialization.

Table 3-1: BAG-INTEL's IPR Matrix

Result	Owner(s)	Background used	Access Rights	Exploitation Plan
Digital Twin Technology	STAM	Proprietary modeling methods	Research: Royalty-free, Commercial: Negotiable	Licensing to airport operators, inclusion in service packages
Contraband Detection Algorithm	SDE	AI datasets, imaging frameworks	Research: Royalty-free, Commercial: Licensing	Commercialization via software licenses
Training Modules for Customs Officials	HFOD	Educational content templates	Open access under Creative Commons	Deployment in training programs for EU customs officials
AI-Powered Reidentification Tools	LTA	AI image processing techniques	Research: Royalty-free, Commercial: Fair terms	Integration with security systems for airports
Knowledge Graph Database	UGR	Semantic data frameworks	Research: Royalty-free, Commercial: Licensing	Consulting and licensing to analytics companies
Secure Communication Protocols	ICCS	Encryption technologies	Research: Royalty-free, Commercial: Negotiable	Integration into broader customs IT frameworks
Advanced Baggage Scanning Systems	SDE	High-resolution scanning methods	Research: Royalty-free, Commercial: Licensing	Sales of hardware solutions to airport authorities

This matrix aligns with the project's IP strategy and ensures all partners benefit equitably from the results while maintaining compliance with the BAG-INTEL Consortium Agreement

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

3.6 INSTRUMENTS FOR PROJECT RESULTS PROTECTION

A comprehensive suite of protection instruments safeguards the valuable results of the BAG-INTEL project, ensuring both legal and practical safeguards. These instruments align with international intellectual property standards and are tailored to the specific needs of the consortium partners.

1. **Patent Applications**: Innovative solutions such as contraband detection algorithms and advanced baggage scanning technologies are protected through patents. This ensures exclusivity for their commercial exploitation and prevents unauthorized use by third parties. Depending on the ownership schema, the patent process is managed by individual partners or jointly, with costs shared as per the Consortium Agreement.

2. **Copyright Protections**: Software, training modules, and other written outputs are secured under copyright laws. This applies to digital twin documentation, AI-based reidentification tool designs, and educational content. Copyright ensures recognition and control over the distribution and reproduction of these assets.

3. **Trademarks**: Distinctive logos, names, and branding associated with BAG-INTEL deliverables are protected through trademarks. This enhances the visibility and recognizability of project outputs while preventing misuse or misrepresentation by competitors.

4. **Licensing Agreements**: Tailored licensing frameworks govern the use and commercialization of project outputs. For instance, software tools may be licensed to airport authorities under fair and reasonable terms, while training materials could be disseminated via open-access platforms to maximize societal impact.

5. **Data Management and Security**: The project adheres to stringent data protection protocols, ensuring compliance with GDPR and other relevant regulations. Sensitive datasets, such as those used for algorithm training, are anonymized and stored in secure repositories with controlled access.

6. **Consortium Agreement Clauses**: The Consortium Agreement includes specific provisions for IP management, dispute resolution, and benefit sharing. This ensures all partners are aligned on the protection and exploitation strategies from the outset.

7. **Monitoring and Enforcement Mechanisms**: Continuous monitoring of project outputs and their usage ensures compliance with agreed-upon terms. In unauthorized use or infringement cases, enforcement mechanisms, including legal recourse, are activated to protect the consortium's interests.

These instruments collectively provide a robust framework for protecting the BAG-INTEL project results, ensuring their value is preserved and maximized for both societal benefit and commercial exploitation.

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

3.7 MANAGEMENT OF KNOWLEDGE

The BAG-INTEL project employs a comprehensive knowledge management framework designed to maximize the value of the knowledge generated and ensure its effective utilization throughout the project lifecycle. Knowledge management encompasses collecting, organizing, sharing, and applying knowledge to achieve the project's objectives and foster long-term innovation and impact.

The framework includes the following key components:

1. **Centralized Knowledge Repository**: All project-related knowledge, including datasets, algorithms, documentation, and deliverables, is stored in a secure, centralized repository. This repository ensures easy access and retrieval for all consortium members while maintaining strict data protection standards.

2. **Knowledge Classification and Tagging**: To facilitate efficient retrieval and application, knowledge assets are systematically classified based on categories such as domain (e.g., AI algorithms, operational workflows), type (e.g., datasets, publications), and relevance (e.g., high-impact results). Tagging ensures that knowledge can be cross-referenced and used effectively across work packages.

3. **Knowledge Sharing Protocols**: Regular consortium-wide meetings, workshops, and webinars are organized to share insights, lessons learned, and emerging innovations. These events foster collaboration and ensure all partners align with the project's objectives and advancements.

4. **Stakeholder Engagement**: External stakeholders, including customs authorities, airport operators, and policymakers, are engaged throughout the project to validate and refine knowledge outputs. Feedback from stakeholders ensures that the knowledge generated is practical, relevant, and impactful.

5. **Continuous Monitoring and Assessment**: The project employs performance indicators to monitor the usage and impact of knowledge assets. For example, tracking how algorithms improve detection accuracy or how customs authorities adopt training modules helps assess the effectiveness of knowledge dissemination and application.

6. **Open Access and Dissemination**: Wherever feasible, knowledge outputs such as research publications, datasets, and software tools are accessible. This aligns with the project's commitment to the FAIR principles (Findability, Accessibility, Interoperability, and Reusability) and enhances the project's broader societal impact.

7. **Long-Term Sustainability**: The knowledge management framework includes provisions for ensuring the sustainability of project outputs. Key deliverables are integrated into long-term operational systems for customs control, while repositories remain accessible for future research and innovation efforts.

Through this comprehensive knowledge management strategy, the BAG-INTEL project ensures that the knowledge generated is preserved and leveraged to drive innovation, improve customs operations, and deliver societal benefits.

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

3.8 PROJECT RESULTS PROTECTION

The BAG-INTEL project employs a robust and multifaceted strategy for protecting its results, ensuring the long-term sustainability and impact of the outcomes. This protection framework encompasses legal, technical, and procedural measures designed to secure the project's intellectual property, safeguard sensitive information, and support effective exploitation by consortium partners.

1. **Legal Protections**:
    - Results generated by the project are protected under relevant intellectual property laws, including patents, copyrights, and trademarks. These measures prevent unauthorized use and ensure that the rights of consortium partners are upheld.
    - Clear ownership agreements, as outlined in the Consortium Agreement, delineate the rights and responsibilities of partners, fostering transparent and equitable management of project results.
2. **Data Security and Privacy**:
    - Sensitive data and information produced during the project are secured using advanced encryption methods and secure storage systems. These measures comply with GDPR and other applicable regulations, ensuring data privacy and confidentiality.
    - Specific protocols are in place for sharing and transferring data, limiting access to authorized individuals and partners.
3. **Technology-Specific Protections**:
    - The software, algorithms, and digital solutions developed by BAG-INTEL are safeguarded through tailored licensing agreements. These licenses specify the conditions under which the tools can be used, ensuring controlled dissemination and preventing misuse.
    - A combination of open and proprietary licensing models balances broad societal impact and commercial viability.
4. **Monitoring and Enforcement**:
    - A structured monitoring system is in place to track the usage of project results and detect any unauthorized access or use. Consortium partners collaborate to enforce protections and address potential infringements.
    - Periodic reviews are conducted to evaluate the effectiveness of protection measures and update strategies as needed.
5. **Stakeholder Engagement and Awareness**:
    - Training sessions and workshops are organized to inform stakeholders, including end-users and policymakers, about the importance of protecting project results and the mechanisms in place.

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

- Stakeholders are encouraged to report any observed misuse or infringement, fostering a collaborative approach to safeguarding results.

6. **Long-Term Sustainability**:

   - Key project outcomes are integrated into existing frameworks and systems to ensure their continued use and development beyond the project's lifecycle.

   - Plans for ongoing maintenance and updates of software and tools are established and supported by commercial and institutional partners.

Through this comprehensive approach, the BAG-INTEL project ensures that its results are protected against unauthorized use and positioned for sustained impact in customs operations and border security.

3.9 RISKS AND MITIGATION MEASURES

3.9.1 Conflict resolution

In order to conduct an appropriate IPR allocation plan, a proactive plan to anticipate any potential conflicts are foreseen. As a starting point, in compliance with the provisions of article 11.8 of the project's Consortium Agreement ("Settlement of disputes"), according to which "*the Parties shall endeavor to settle their disputes amicably",* in case any issues are identified, DBC will engage to discussions with the partners involved in order for the potential dispute to be settled. Information related to each partners contribution are considered vital in this task, alongside the provided background and potentially each partner's person months, during the IPR allocation process and the relevant discussions.

If this procedure is deemed unsuccessful, the Consortium Agreement's internal mediation process will be initiated. Should issues persist, a formal mediation process will follow, aligned with WIPO Mediation Rules. Up to this point though, conflicts regarding IPR rights among partners have not arisen in BAG-INTEL and we can safely assume that the consortium will not face such issues.

3.9.2 Mitigation of third-party IP dependencies

In the context of BAG-INTEL, mitigating risks associated with dependencies on third-party IP is crucial to maintaining the integrity and continuity of project outcomes. A proactive approach will involve conducting due diligence to identify any external IP that the project may rely on to develop its foreground results. Partners must indicate any third-party IP relevant to their contributions, and the project team will assess licensing agreements to ensure compliance and avoid infringement risks. Additionally, and if required for future exploitation, strategies will be developed to negotiate necessary licenses with third-party IP holders, allowing for unhindered access and use of their technologies.

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

4 PRELIMINARY MARKET & COMPETITION ANALYSIS

4.1 KEY MARKET TRENDS AND GROWTH DRIVERS

The market for AI-powered customs control and baggage security solutions is undergoing rapid transformation, driven by increasing global trade, heightened security threats, and advancements in artificial intelligence (AI) and digital twin technologies. The **BAG-INTEL project** is positioned within this dynamic landscape, leveraging innovative AI-driven risk assessment, baggage reidentification, and contraband detection to enhance the efficiency of customs operations. This section outlines the key market trends and growth drivers shaping the adoption and expansion of BAG-INTEL solutions.

4.1.1 Market Trends:

1. **Increasing Air Passenger and Cargo Volumes.** The air travel industry continues to expand, with global air passenger traffic expected to double over the next two decades. This surge necessitates more **efficient and automated customs screening solutions** to handle increased baggage loads while maintaining security compliance. Similarly, international cargo volumes are rising, prompting **greater demand for AI-powered customs clearance technologies**.

2. **Stricter Border Security and Compliance Regulations.** Governments worldwide are tightening regulations on cross-border trade and security screening, increasing the need for **advanced customs control technologies**. The EU's Integrated Border Management (IBM) Strategy emphasizes AI adoption, risk-based screening, and real-time data analytics to streamline operations while reducing smuggling risks.

3. **Adoption of AI and Machine Learning in Customs Operations.** AI and machine learning-driven automation are becoming the standard for customs security, risk assessment, and baggage reidentification. AI-powered object recognition in X-ray and CT scans, real-time video analytics for suspicious behavior detection, and automated decision-support systems are key market demands that BAG-INTEL technologies address.

4. **Growth of Digital Twin Technology in Security and Logistics.** The integration of digital twin models in airport and customs security is gaining traction, enabling real-time simulation, predictive analytics, and process optimization. This trend aligns with BAG-INTEL's AI-powered customs control framework, which leverages digital twin modeling to optimize inspection workflows.

5. **Expansion of Smart Border Initiatives.** Smart border technologies, including biometric verification, real-time customs risk assessment, and AI-powered screening, are expanding across European, North American, and Asia-Pacific regions. Initiatives such as EU Smart Borders, US CBP (Customs and Border Protection) AI screening, and automated customs clearance in major hubs reinforce the relevance of BAG-INTEL solutions.

4.1.2 Growth Drivers:

1. **Regulatory Push for AI-Based Customs Modernization**

    - **European Union:** EU customs authorities are mandating the adoption of AI and data-driven customs risk management, reinforcing the demand for BAG-INTEL's AI-driven screening solutions.

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

- **US and Asia-Pacific:** Governments invest in AI-based baggage scanning, automated risk analysis, and cross-border data-sharing initiatives.

2. **Need for Efficiency in Customs Inspections.** With limited human resources, customs agencies require automated and AI-enhanced solutions to increase efficiency while maintaining high detection accuracy. AI-powered baggage reidentification and contraband detection reduce operational workload and improve processing times.

3. **Increasing Investment in Airport Security Technologies.** Global investments in airport security solutions are expected to surpass $20 billion by 2030, focusing on AI-driven screening and digital border management systems. BAG-INTEL's customs AI decision-support system aligns with this investment trend.

4. **Demand for Seamless Passenger Experience.** As airports and governments seek to enhance passenger convenience while improving security, AI-driven baggage tracking and risk-based customs inspections minimize random checks, false alarms, and unnecessary passenger delays.

5. **Adoption of AI for Fraud and Contraband Detection.** The rise in organized crime and smuggling activities has increased demand for AI-powered fraud detection, contraband identification, and real-time customs risk analytics. BAG-INTEL's advanced detection algorithms and AI-enhanced customs support systems cater directly to this need.

4.2 COMPETITIVE LANDSCAPE

The market for AI-powered customs control and baggage security solutions is increasingly competitive, with various technology providers, security agencies, and AI-driven risk assessment platforms offering solutions to enhance border security, baggage screening, and contraband detection. The BAG-INTEL project operates within this evolving landscape, leveraging cutting-edge AI, machine learning, and digital twin technologies to optimize customs procedures. This section provides an overview of the key competitors, alternative solutions, and market positioning of BAG-INTEL.

1. Key Competitors and Alternative Solutions

The competitive landscape in AI-powered customs and security screening solutions is dominated by established technology providers, emerging AI startups, and security-focused research consortia. The following categories outline major competitors:

A. Established Security Technology Providers

1. **Smiths Detection**

   - A global leader in baggage screening and contraband detection, Smiths Detection specializes in computed tomography (CT), X-ray, and AI-enhanced threat detection solutions[1] .

[1] Smiths Detection. (2023). X-ray and CT scanning solutions for customs control. Retrieved from https://www.smithsdetection.com.

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

- The company's technologies focus on real-time threat identification, competing with BAG-INTEL's AI-powered contraband identification system.

2. **Rapiscan Systems**
   - Rapiscan provides advanced security screening for airports, customs, and border control[2].
   - Its real-time AI-powered baggage analysis competes with BAG-INTEL's AI-driven reidentification and decision-support system.
3. **Leidos Security & Detection Systems**
   - Leidos specializes in AI-enhanced risk assessment, X-ray scanning, and baggage tracking[3].
   - The company integrates big data analytics for customs operations, positioning itself as a competitor to BAG-INTEL's predictive analytics and risk modeling capabilities.

B. AI Startups and Emerging Technology Providers

1. **Cognitec & NEC Corporation** (AI-based facial recognition and tracking)
   - These companies focus on AI-powered passenger and baggage tracking[4].
   - BAG-INTEL competes by offering AI-driven baggage reidentification and tracking through visual analytics.
2. **Evolv Technology** (AI-based security scanning)
   - Evolv specializes in real-time AI-powered threat detection solutions[5].
   - Competes with BAG-INTEL's AI-based customs risk detection and contraband analysis.
3. **SeeTrue AI** (Automated baggage security)
   - Focuses on real-time AI-powered baggage screening for explosives and contraband[6].
   - Direct competitor to BAG-INTEL's AI-enhanced detection system.

[2] Rapiscan Systems. (2022). Advanced security screening technologies for border control. Retrieved from https://www.rapiscansystems.com.

[3] Leidos. (2023). AI-driven security solutions for customs and border control. Retrieved from https://www.leidos.com.

[4] Cognitec. (2022). AI-based facial recognition solutions for border security. Retrieved from https://www.cognitec.com; NEC Corporation. (2023). AI and biometric verification for customs and border control. Retrieved from https://www.nec.com.

[5] Evolv Technology. (2023). AI-powered security screening solutions. Retrieved from https://www.evolvtechnology.com.

[6] SeeTrue AI. (2022). Automated baggage security through AI-powered detection systems. Retrieved from https://www.seetrue.ai.

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

C. Government and Research Consortiums

1. **European Customs AI Initiatives (DG TAXUD & FRONTEX)**
    - The EU supports research in AI-driven customs risk assessment, contraband detection, and automated customs processing[7].
    - BAG-INTEL offers an integrated AI ecosystem covering risk detection, baggage tracking, and decision support.
2. **U.S. CBP (Customs and Border Protection) AI Pilots**
    - U.S. authorities are piloting AI-powered baggage analysis and contraband detection[8].
    - BAG-INTEL competes by providing customizable AI-powered customs control solutions adaptable across multiple jurisdictions.
3. **International Air Transport Association (IATA) Smart Border Initiative**
    - IATA promotes seamless border control through AI, biometrics, and risk assessment systems[9].
    - BAG-INTEL aligns with IATA's vision but provides a more focused AI-driven customs control model.

2. Competitive Positioning of BAG-INTEL

The BAG-INTEL project stands out in the competitive landscape due to its holistic AI-powered approach integrating contraband detection, risk assessment, and baggage tracking. The key differentiators include:

1. **AI-Driven Baggage Reidentification**
    - Unlike competitors focusing solely on scanning and object detection, BAG-INTEL employs AI-powered visual tracking to reidentify high-risk baggage across multiple airport zones.
2. **Customs-Specific Digital Twin Technology**
    - BAG-INTEL integrates real-time simulation and predictive analytics, unlike competitors relying on standard scanning technologies.
3. **Risk-Based Customs Decision Support System (DSS)**

[7] European Commission. (2023). Customs risk assessment and AI-driven border security initiatives. Retrieved from https://ec.europa.eu.

[8] U.S. CBP. (2023). AI pilots in customs risk assessment and baggage security. Retrieved from https://www.cbp.gov.

[9] IATA. (2022). Smart border technologies for aviation security. Retrieved from https://www.iata.org.

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

- Offers a customized AI-driven risk assessment engine that enhances customs efficiency, setting it apart from competitors focusing only on standalone screening technologies.

4. **Modular and Scalable Deployment Model**

   - Unlike large-scale proprietary solutions (e.g., Smiths Detection, Rapiscan), BAG-INTEL is designed for modular deployment and scalability across various customs environments.

4.3 COMPETITIVE ADVANTAGES OF BAG - INTEL TECHNOLOGIES

The BAG-INTEL project brings a transformative approach to customs security, baggage screening, and risk assessment by integrating artificial intelligence (AI), machine learning (ML), digital twin technology, and real-time decision-support systems. Unlike existing market solutions, BAG-INTEL's unique technological innovations enhance customs control efficiency, accuracy, and adaptability. This section highlights the key competitive advantages of BAG-INTEL's technologies over traditional and competing solutions.

1. AI-Powered Baggage Reidentification and Tracking

One of the most significant differentiators of BAG-INTEL is its ability to perform AI-driven baggage reidentification across multiple airport zones.

- Unlike traditional tracking systems that rely on barcodes or RFID scanning[10], BAG-INTEL utilizes computer vision and deep learning to recognize baggage across locations.
- The system eliminates reliance on physical tags, often subject to damage or tampering, ensuring higher tracking accuracy in high-security zones.
- Competitors like Smiths Detection and Rapiscan provide X-ray and CT scanning but do not offer continuous baggage tracking through AI-based visual recognition[11].

2. Digital Twin Technology for Real-Time Customs Simulation

BAG-INTEL integrates digital twin technology, a feature not widely adopted by traditional baggage screening providers.

- What makes it unique? Unlike static risk models, BAG-INTEL's digital twin creates a real-time virtual replica of customs operations, allowing for scenario analysis, process optimization, and predictive analytics[12].

[10] Leidos. (2023). AI-driven security solutions for customs and border control. Retrieved from https://www.leidos.com.

[11] Smiths Detection. (2023). X-ray and CT scanning solutions for customs control. Retrieved from https://www.smithsdetection.com.

[12] European Research Executive Agency. (2023). Horizon Europe customs security projects. Retrieved from https://rea.ec.europa.eu.

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

- Competing solutions like Leidos and Rapiscan focus on enhancing scanning accuracy but do not provide full-scale customs simulations for risk-based decision-making[13].

- This predictive analytics approach helps customs authorities allocate resources efficiently, reducing false positives and unnecessary manual inspections.

3. AI-Driven Risk-Based Customs Decision Support System (DSS)

BAG-INTEL introduces an advanced AI-powered Decision Support System (DSS) that analyzes multiple data sources to assess risk in real-time.

- Unlike conventional systems that depend on predefined risk assessment matrices, BAG-INTEL dynamically adapts to new threat patterns using machine learning[14].

- While U.S. CBP's AI pilots and EU customs security initiatives focus on enhancing risk detection, they do not offer integrated AI-driven decision-making that continuously learns and adapts to new risks[15].

- The system is designed to work seamlessly with existing customs frameworks, allowing for faster decision-making while maintaining compliance with international security regulations[16].

4. AI-Powered Contraband Detection Beyond Conventional Screening

BAG-INTEL's contraband detection algorithms go beyond standard X-ray and CT-based scanning by incorporating:

- AI-enhanced object recognition identifies anomalies in baggage contents more accurately than traditional imaging systems[17].

- Multi-source data fusion integrates passenger risk profiles, travel history, and scanning results to improve customs efficiency[18].

- In contrast, Rapiscan, Leidos, and Evolv Technology primarily rely on predefined contraband signatures rather than self-learning AI models that continuously update based on real-world data[19].

5. Seamless Integration with Existing Customs Infrastructure

[13] Leidos. (2023). AI-driven security solutions for customs and border control. Retrieved from https://www.leidos.com.

[14] European Commission. (2023). Customs risk assessment and AI-driven border security initiatives. Retrieved from https://ec.europa.eu.

[15] U.S. CBP. (2023). AI pilots in customs risk assessment and baggage security. Retrieved from https://www.cbp.gov.

[16] IATA. (2022). Smart border technologies for aviation security. Retrieved from https://www.iata.org.

[17] Smiths Detection. (2023). X-ray and CT scanning solutions for customs control. Retrieved from https://www.smithsdetection.com.

[18] European Commission. (2023). Customs risk assessment and AI-driven border security initiatives. Retrieved from https://ec.europa.eu.

[19] Leidos. (2023). AI-driven security solutions for customs and border control. Retrieved from https://www.leidos.com; Rapiscan Systems. (2022). Advanced security screening technologies for border control. Retrieved from https://www.rapiscansystems.com.

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

BAG-INTEL is designed for modular deployment, allowing customs authorities to integrate AI-driven analytics without replacing existing infrastructure.

- Compared to large-scale proprietary solutions from Smiths Detection and Rapiscan, BAG-INTEL enables incremental deployment, reducing cost and operational disruptions.
- The system is adaptable to various airport sizes and operational structures, making it scalable for large international hubs and smaller regional airports[20].

6. Enhanced Passenger Flow and Reduced Delays

A key advantage of BAG-INTEL is its ability to streamline customs operations without causing unnecessary delays for passengers.

- AI-driven risk-based screening ensures that only high-risk baggage is flagged for secondary inspection, unlike conventional systems that rely on randomized manual checks[21].
- Competitors in the customs security sector primarily focus on detection accuracy, but BAG-INTEL balances security with operational efficiency, improving traveler experience without compromising safety.

7. Compliance with International Security Standards and Regulations

BAG-INTEL aligns with EU and global regulatory frameworks, ensuring seamless adoption across customs agencies worldwide.

- The project complies with EU Integrated Border Management (IBM) Strategy, GDPR, and Schengen customs security standards[22].
- Unlike closed-source AI security solutions, BAG-INTEL emphasizes data transparency, regulatory compliance, and ethical AI implementation.

4.4 MARKET ENTRY CHALLENGES

Despite the technological and operational advantages of BAG-INTEL's AI-driven customs security solutions, penetrating the highly regulated and security-sensitive customs control and border management market presents several challenges. These challenges stem from regulatory compliance, market adoption barriers, integration complexity, financial constraints, and competition from established players. This section analyzes the primary obstacles to BAG-INTEL's market entry and strategic deployment.

1. Regulatory and Compliance Barriers

A. Strict Security and Customs Regulations

[20] European Research Executive Agency. (2023). Horizon Europe customs security projects. Retrieved from https://rea.ec.europa.eu,

[21] IATA. (2022). Smart border technologies for aviation security. Retrieved from https://www.iata.org.

[22] European Commission. (2023). Customs risk assessment and AI-driven border security initiatives. Retrieved from https://ec.europa.eu.

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

- Customs and border control are heavily regulated sectors governed by strict national and international security frameworks, such as the EU Integrated Border Management (IBM) Strategy, the General Data Protection Regulation (GDPR), and the WCO SAFE Framework of Standards[23].

- New AI-driven security systems, like those proposed by BAG-INTEL, require extensive regulatory approvals and validation trials, potentially delaying deployment in international markets[24].

B. Ethical and Data Privacy Concerns

- AI-based customs control systems rely on large-scale data processing, including passenger information, baggage scans, and behavioral analytics. Compliance with GDPR, U.S. CBP regulations, and other regional data protection laws poses a challenge[25].

- Transparency, bias mitigation, and AI ethics must be demonstrated to regulatory bodies before approval, requiring additional compliance investments and legal oversight[26].

2. Market Adoption and Stakeholder Resistance

A. Resistance from Customs and Airport Authorities

- Customs authorities and airport operators often rely on existing, well-established security solutions[27].

- Resistance to adopting new AI-driven models stems from concerns about technological reliability, potential disruptions to operations, and the need for additional training.

- Many authorities hesitate to transition from manual or semi-automated screening processes to fully AI-powered systems due to lack of familiarity and operational inertia[28].

B. Training and Workforce Adaptation

- Implementing BAG-INTEL requires customs officers and security personnel to undergo specialized training in AI-powered risk assessment, digital twins, and advanced screening methodologies.

[23] European Commission. (2023). Customs risk assessment and AI-driven border security initiatives. Retrieved from https://ec.europa.eu; World Customs Organization. (2022). SAFE Framework of Standards to Secure and Facilitate Global Trade. Retrieved from https://www.wcoomd.org.

[24] European Research Executive Agency. (2023). Horizon Europe customs security projects. Retrieved from https://rea.ec.europa.eu.

[25] U.S. CBP. (2023). AI pilots in customs risk assessment and baggage security. Retrieved from https://www.cbp.gov.

[26] European Commission. (2023). Customs risk assessment and AI-driven border security initiatives. Retrieved from https://ec.europa.eu.

[27] Leidos. (2023). AI-driven security solutions for customs and border control. Retrieved from https://www.leidos.com; Smiths Detection. (2023). X-ray and CT scanning solutions for customs control. Retrieved from https://www.smithsdetection.com.

[28] Rapiscan Systems. (2022). Advanced security screening technologies for border control. Retrieved from https://www.rapiscansystems.com.

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

- Limited technical expertise among customs personnel can hinder adoption and necessitate additional investment in training programs, delaying widespread implementation.

3. Integration Complexity and Technological Challenges

A. Compatibility with Existing Infrastructure

- Many airports and customs facilities operate on legacy security screening systems that do not natively support AI-driven analytics and digital twin modeling.
- Ensuring seamless integration of BAG-INTEL with X-ray scanners, CT imaging, and automated border control systems requires customized solutions, increasing deployment costs and time.

B. Real-Time AI Decision-Making Constraints

- Customs control is a high-stakes environment where false positives or AI misjudgments could result in operational inefficiencies, passenger delays, and legal challenges.
- AI models require continuous retraining and validation to minimize false detection rates while ensuring compliance with security protocols.
- The demand for low-latency AI decision-making in busy airports poses computational challenges, requiring high-performance infrastructure and cloud-edge integration.

4. Financial Barriers and Funding Constraints

A. High Initial Investment Costs

- The transition to AI-driven customs control demands significant upfront investment in hardware, software, AI model training, and staff training programs.
- Many customs agencies operate on fixed budgets, making it challenging to secure funding for next-generation security solutions.
- BAG-INTEL must demonstrate strong cost-benefit projections to convince government authorities, investors, and funding agencies of its long-term financial viability.

B. Limited Government Funding for AI-Based Customs Modernization

- Government funding for AI in customs security remains limited, with most budgets allocated to traditional security measures such as physical screening infrastructure.
- BAG-INTEL must compete with established players for limited Horizon Europe, EU Innovation Fund, and national security funding opportunities.

5. Competition from Established Security Technology Providers

- Global security giants such as Smiths Detection, Rapiscan, and Leidos have long-standing contracts with governments and airport authorities, making it challenging for new entrants to secure market share.

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

- These companies already offer well-established, AI-augmented baggage screening technologies, requiring BAG-INTEL to differentiate itself through superior capabilities, modular deployment, and cost efficiency.

- BAG-INTEL must overcome vendor lock-in effects, as many customs agencies prefer continuing contracts with existing providers rather than investing in new technologies.

6. Interoperability and International Standardization Challenges

- Customs security technologies must be interoperable across different jurisdictions to facilitate seamless cross-border security coordination[29].

- The lack of global standardization in AI-driven customs control complicates adoption, as different regions enforce distinct security compliance frameworks[30].

- BAG-INTEL must align with international standardization efforts, collaborating with IATA, WCO, and EU security regulators to enhance global adoption[31].

4.5 STRATEGIC IMPLICATIONS AND RECOMMENDATIONS

The successful adoption, deployment, and market penetration of BAG-INTEL's AI-driven customs control technologies require a strategic approach that addresses regulatory, operational, financial, and competitive challenges. The project operates within a highly regulated environment where compliance with international customs security frameworks is crucial. Additionally, the presence of strong competitors with established solutions necessitates differentiation through advanced technological capabilities, cost-effectiveness, and seamless integration with existing infrastructure. Financial sustainability and adoption incentives will also be key in securing government and industry partnerships for widespread implementation.

1. Strategic Implications for Customs Security and Market Positioning

BAG-INTEL operates in a security-sensitive domain where regulatory approval is a key determinant of market entry success. Customs authorities operate under strict compliance frameworks, and any new AI-driven security technology must meet legal, ethical, and operational requirements. Engaging with policymakers, regulatory agencies, and international organizations from the early stages is necessary to align with security and AI governance laws. The project must address growing concerns over AI ethics, bias, and data privacy, ensuring transparency and explainability in decision-making processes.

In terms of competition, the customs security market is dominated by established players such as Smiths Detection, Leidos, and Rapiscan, which provide advanced baggage scanning technologies. While these companies focus primarily on detection, BAG-INTEL offers a unique combination of AI-driven baggage reidentification, real-time decision support, and digital twin technology. Positioning

[29] European Commission. (2023). Customs risk assessment and AI-driven border security initiatives. Retrieved from https://ec.europa.eu.

[30] World Customs Organization. (2022). SAFE Framework of Standards to Secure and Facilitate Global Trade. Retrieved from https://www.wcoomd.org.

[31] IATA. (2022). Smart border technologies for aviation security. Retrieved from https://www.iata.org.

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

the project as a complementary rather than a competing solution will be critical for securing partnerships with customs authorities and aviation security operators.

Another strategic implication lies in financial sustainability. AI-based customs security systems require significant technological, training, and operational integration investments. Customs authorities operate on fixed budgets, making it difficult to justify high initial costs for new security solutions. Demonstrating long-term cost savings through automation, improved contraband detection rates, and enhanced operational efficiency will be essential for convincing decision-makers to adopt BAG-INTEL's solutions.

2. Recommendations for Market Entry and Expansion

BAG-INTEL must strengthen partnerships with customs authorities, airport security agencies, and logistics operators to ensure successful market entry. Establishing pilot implementations in key international airports will provide real-world validation of the system's efficiency. These pilot programs should be designed to measure performance metrics such as detection accuracy, manual inspection reduction, and passenger processing efficiency. By showcasing early success, BAG-INTEL can build credibility and support from policymakers and funding agencies.

Interoperability with existing security infrastructure is crucial for adoption. Customs agencies are unlikely to replace their entire screening systems; therefore, BAG-INTEL should be designed for modular deployment, allowing for seamless integration with existing X-ray, CT scanning, and risk assessment technologies. A phased implementation approach will help reduce adoption barriers while allowing customs authorities to experience the benefits of AI-powered decision support without significant operational disruptions.

Another critical recommendation is to develop AI ethics and governance frameworks. Customs security relies on public trust, and any AI-driven decision-making system must be transparent, fair, and explainable. BAG-INTEL should proactively engage with regulatory bodies to establish best AI explainability, bias mitigation, and data privacy practices. Creating an AI advisory board that includes industry experts, customs officers, and policymakers can help ensure alignment with evolving legal and ethical standards.

Financial sustainability is a key factor in securing market penetration. Obtaining funding through Horizon Europe, the Digital Europe Programme, and national security grants will help lower costs for early adopters. Exploring partnerships with private sector logistics and security firms could also open new revenue streams, ensuring long-term sustainability beyond government contracts. Developing a cost-sharing model or offering subscription-based pricing for AI-driven customs security services could make the solution more financially viable for lower-budget customs agencies.

3. Long-Term Vision and Sustainability

To ensure long-term success, BAG-INTEL must integrate into global smart border strategies. Alignment with initiatives such as the EU's Digital Customs Roadmap, IATA's Smart Borders program, and the WCO's SAFE Framework will position the project as a leading AI solution for border security. Expanding beyond airports to land and maritime border operations will further increase its applicability and market reach.

Continuous innovation will be necessary to maintain competitiveness. BAG-INTEL must invest in ongoing AI model improvements, ensuring its detection algorithms adapt to emerging smuggling tactics and new security threats. The integration of cybersecurity measures will also be critical, as customs AI systems will need to remain resilient against potential cyberattacks and data breaches.

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

The long-term vision for BAG-INTEL should include establishing itself as a global hub for AI-driven customs security solutions. Partnering with universities, research institutions, and AI think tanks will contribute to ongoing development and knowledge-sharing. Providing training programs and AI certifications for customs professionals will further reinforce the project's role as an industry leader.

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

5 SOCIOECONOMIC ANALYSIS

The BAG-INTEL project is expected to generate significant socio-economic benefits by enhancing customs operations' efficiency, security, and sustainability through AI-driven solutions and digital twin technologies. Understanding these innovations' broader economic, social, and regulatory implications is essential for ensuring their successful adoption, scalability, and long-term impact.

This section provides a comprehensive socioeconomic analysis, evaluating the project's influence on customs operations, economic efficiency, workforce adaptation, regulatory compliance, and societal acceptance. The study incorporates PESTLE and SWOT assessments to identify key political, economic, social, technological, legal, and environmental factors affecting the project's implementation and sustainability.

By assessing market drivers, potential barriers, and long-term benefits, this analysis helps shape BAG-INTEL's exploitation strategy. It ensures that the project not only delivers cutting-edge security innovations but also contributes to economic growth, regulatory modernization, and enhanced public safety in the evolving border control landscape.

5.1 PROJECT PESTLE ANALYSIS

PESTLE analysis is a widely used strategic tool that examines external factors influencing an organization, initiative, or project. It evaluates Political, Economic, Social, Technological, Legal, and Environmental elements, offering a structured approach to identifying opportunities and risks in the macro-environment. By understanding these external influences, businesses and projects can adapt their strategies, align with trends, and mitigate potential challenges, ensuring more informed decision-making and strategic planning.

When applied to projects, PESTLE analysis focuses on assessing the external factors directly impacting the project's lifecycle, goals, and outcomes. It provides insights into potential risks, opportunities, and regulatory or societal considerations that could affect implementation or success. This helps project teams ensure compliance, anticipate challenges, and maximize the project's long-term impact and value, particularly in dynamic or multi-stakeholder environments.

The following is a PESTLE analysis of the project, evaluating the external factors influencing its progress and success.

5.1.1 Political Factors

1. **Policy Support**: BAG-INTEL aligns with the European Union's priorities to secure borders and reduce contraband activities. The project benefits from Horizon Europe funding under the Secure Society goals.

2. **Regulatory Frameworks**: Adherence to EU regulations, including GDPR, NIS directives, and customs laws, ensures compliance with data privacy, security, and trade practices.

3. **Customs Modernization Drive**: Political will to enhance customs operations and align with the EU's Schengen Zone security measures supports the project's objectives.

4. **Risk of Bureaucratic Delays**: Potential delays in policy implementation or resistance to adopting new technologies among member states could pose barriers to rapid deployment.

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

5.1.2 Economic Factors

1. **Cost Efficiency**: BAG-INTEL aims to reduce operational costs by 20% through AI-driven detection and reidentification, minimizing the need for human resources.

2. **Economic Impact of Contraband**: The project could disrupt the illegal trade economy, potentially saving the EU millions in lost customs revenues.

3. **Investment in Technology**: Airports and customs agencies must allocate resources to adopt BAG-INTEL solutions. Financing schemes will be critical to ensure affordability.

4. **ROI and Scalability**: Return on investment is anticipated through increased contraband detection and enhanced passenger throughput, making it appealing for broader market adoption.

5.1.3 Social Factors

1. **Improved Traveler Experience**: Reduced delays and focused customs checks will enhance passenger satisfaction.

2. **Safety and Security**: The project contributes to societal safety by intercepting harmful contrabands, such as drugs and weapons, before entering the market.

3. **Resistance to Change**: Customs officers and airport stakeholders may exhibit resistance due to unfamiliarity with AI-based systems and concerns over job displacement.

5.1.4 Technological Factors

1. **Advanced AI and Digital Twins**: BAG-INTEL leverages cutting-edge AI for contraband detection and luggage reidentification and uses digital twins for operational simulation.

2. **Interoperability and Scalability**: The multi-cloud IoT-edge architecture ensures flexibility and compliance across airport setups.

3. **Need for Continuous Innovation**: Competing technologies in AI-driven customs systems could necessitate ongoing updates to maintain relevance and effectiveness.

5.1.5 Legal Factors

1. **Data Protection Compliance**: Strict adherence to GDPR and other EU privacy laws ensures the lawful processing of passenger and customs data.

2. **Intellectual Property Management**: Effective handling of IPR for BAG-INTEL's technological outputs underpins the exploitation strategy.

3. **Liability and Accountability**: Contracts and agreements among consortium partners ensure clear responsibility in case of breaches or underperformance.

5.1.6 Environmental Factors

1. **Sustainability Goals**: By reducing unnecessary customs interventions and delays, the project aligns with broader sustainability goals, such as reducing emissions from airport congestion.

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

2. **Digital Infrastructure**: Using digital twins and cloud solutions minimizes the need for physical infrastructure expansion.

3. **Environmental Risks**: Hardware-intensive solutions, such as advanced scanners, might pose environmental challenges related to disposal or energy usage.

The PESTLE analysis reveals the diverse external factors that influence the project, providing valuable insights into opportunities and challenges across political, economic, social, technological, legal, and environmental dimensions. Politically, the project benefits from alignment with EU priorities on border security and customs modernization, while economically, its potential to reduce operational costs and disrupt illegal trade creates significant value. Socially, the project's focus on improving safety and passenger experience enhances its societal relevance, while technologically, its advanced AI and digital twin solutions position it at the forefront of innovation.

Legal compliance and environmental sustainability are critical for ensuring long-term viability and scalability. Addressing privacy regulations, intellectual property management, and ecological challenges will be key to maintaining the project's impact and acceptance. The analysis highlights the need for proactive risk management, stakeholder engagement, and continuous technological adaptation to fully realize the project's objectives and maximize its contribution to efficient and secure customs operations.

5.2 PROJECT SWOT ANALYSIS

A SWOT analysis is a strategic tool to evaluate a project's Strengths, Weaknesses, Opportunities, and Threats. It provides a structured approach to understanding both internal and external factors that can impact the project's success. Strengths and weaknesses are internal characteristics, such as the project's resources, capabilities, and execution strategies, while opportunities and threats are external influences, including market conditions, regulatory changes, and stakeholder dynamics.

A SWOT analysis is critical for projects like BAG-INTEL, which involve innovative technologies, multi-stakeholder collaboration, and alignment with strategic objectives. It allows project teams to capitalize on internal strengths, address weaknesses, leverage opportunities, and mitigate external threats. By integrating these insights, the project team can build a robust strategy for implementation and sustainability, ensuring that the project achieves its desired impact efficiently and effectively. Below is an extensive analysis of the BAG-INTEL project through the lens of SWOT.

5.2.1 Strengths

1. **Innovative Technology**: The project leverages of cutting-edge AI tools, such as luggage reidentification systems and digital twins, to enhance customs operations and contraband detection.

2. **Strong Consortium**: It benefits from a diverse and experienced consortium of partners, including academic institutions, research centers, and industry leaders, ensuring technical and operational expertise.

3. **Alignment with EU Priorities**: The project's objectives align with the European Union's focus on enhancing security, improving border management, reducing illegal activities, ensuring political and financial support.

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

4. **Cost Efficiency**: The project aims to significantly lower customs authorities' operational costs by reducing their reliance on human resources and introducing automation.

5. **Scalability**: The modular architecture and multi-cloud IoT-edge solutions allow for easy adaptation across different airport sizes and regions.

5.2.2 Weaknesses

1. **Data Dependency**: AI-driven systems require large volumes of high-quality data for training and optimization, which may not always be readily available.

2. **Complex Implementation**: Integrating new systems into existing airport infrastructure and customs processes can be challenging and time-consuming.

3. **Limited Awareness and Adoption**: Resistance to change among end-users, including customs officials and airport operators, may slow down the adoption of the project's solutions.

4. **High Initial Costs**: Despite its long-term cost-saving potential, the upfront investment required for hardware, training, and deployment may deter some stakeholders.

5. **Regulatory Complexity**: Compliance with data privacy laws, security standards, and customs regulations across multiple countries adds complexity to implementation.

5.2.3 Opportunities

1. **Global Expansion Potential**: The project's solutions can be deployed in airports worldwide, offering scalability beyond the EU and addressing universal challenges in customs operations.

2. **Technological Advancements**: Continued developments in AI, machine learning, and cloud computing provide opportunities to enhance the project's capabilities over time.

3. **Increased Security Awareness**: Rising concerns over border security and illegal trade create a favorable environment for adopting advanced customs control technologies.

4. **Collaboration with Stakeholders**: Partnerships with international customs organizations, airport operators, and regulatory bodies can increase support and ensure smoother implementation.

5. **Standardization Leadership**: The project can potentially set new benchmarks and standards for AI-driven customs operations, influencing future regulations and industry practices.

5.2.4 Threats

1. **Technological Competition**: The rapid evolution of AI and detection technologies could lead to competing solutions that may outpace the project's offerings.

2. **Economic Constraints**: Budget limitations among customs authorities and airports, especially in developing regions, could hinder widespread adoption.

3. **Cybersecurity Risks**: The project relies heavily on cloud-based systems and data sharing, which exposes it to potential cybersecurity threats and data breaches.

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

4. **Political Instability**: Changes in political priorities or government instability in partner countries could impact funding and project support.

5. **Market Resistance**: Stakeholders may hesitate to invest in unproven technologies or favor alternative solutions with a longer track record.

The SWOT analysis provides a comprehensive overview of the internal and external factors influencing the project's success. The project's key strengths lie in its innovative technology, strong consortium, alignment with EU priorities, and potential for scalability and cost efficiency. These strengths position the project to address pressing challenges in customs operations effectively while driving operational improvements and enhanced security.

However, the analysis also highlights critical weaknesses, such as data dependency, complex implementation processes, and potential resistance to change among stakeholders. To overcome these challenges, the project must leverage opportunities like global expansion, technological advancements, and partnerships with international stakeholders. At the same time, it must proactively address external threats, including competition from emerging technologies, economic constraints, and cybersecurity risks. The analysis underscores the importance of strategic planning, collaboration, and adaptability in ensuring the project's long-term success and sustainability.

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

6 STAKEHOLDER IDENTIFICATION AND ANALYSIS

The success of BAG-INTEL relies on the active involvement of a diverse range of stakeholders, each playing a crucial role in the development, deployment, and adoption of the project's AI-powered customs control solutions. Identifying and understanding these stakeholders is essential to ensure effective engagement, dissemination, and exploitation of the project's results.

This section provides a structured approach to stakeholder analysis. It defines the key groups that interact with BAG-INTEL, assesses their influence and impact on the project, and outlines strategies for collaboration. The study categorizes stakeholders into regulatory authorities, end-users, industry and technology providers, research institutions, policy organizations, and civil society. By mapping their interests and levels of engagement, the project ensures that its technological innovations are aligned with real-world needs, regulatory requirements, and market expectations.

A well-defined stakeholder engagement strategy enhances project adoption, sustainability, and long-term impact, ensuring that BAG-INTEL's innovations contribute to efficient, secure, and AI-enhanced customs operations across Europe and beyond.

6.1 TYPES OF STAKEHOLDER CHARACTERIZATION

In the project context, stakeholders encompass a broad spectrum of entities, from regulatory authorities to technology providers and end-users, each playing a crucial role in the project's lifecycle. Stakeholder characterization is necessary to ensure effective engagement, dissemination, and exploitation of project results.

The identified stakeholders in BAG-INTEL can be classified into the following categories:

1. **Regulatory and Governmental Authorities**
    - European Commission (EC) and the European Research Executive Agency (REA).
    - National Customs and Border Control Authorities.
    - Law enforcement agencies (e.g., national police forces, border security units).
    - Aviation security regulators (e.g., European Civil Aviation Conference - ECAC).
2. **End-Users and Operational Stakeholders**
    - Customs control officers and border police responsible for baggage inspection.
    - Airport authorities and operators (e.g., FRAPORT Greece, other international airport operators).
    - Airlines and freight carriers involved in passenger baggage transport.
    - Passengers and travelers indirectly impacted by BAG-INTEL's solutions.
3. **Industry and Technology Providers**
    - AI and machine learning solution developers.

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

- Cybersecurity firms ensuring the protection of sensitive customs data.
- Baggage scanning and detection system manufacturers (e.g., Smiths Detection Germany GmbH).
- Digital Twin developers and software vendors.
- System integrators providing technical interoperability.

4. **Academic and Research Institutions**
   - Universities and research centers involved in AI, machine learning, and risk assessment.
   - Technical partners contributing to digital twin modeling and predictive analytics.
   - Institutions focusing on ethical considerations and data protection.
5. **Policy and Standards Organizations**
   - World Customs Organization (WCO).
   - European Union Aviation Safety Agency (EASA).
   - International Air Transport Association (IATA).
   - Standardization bodies (e.g., ISO, CEN, EOS SSD Working Group).
6. **Civil Society and the General Public**
   - NGOs focused on data privacy, ethical AI, and human rights.
   - Travelers and consumer protection groups advocating for passenger rights.
   - The broader public, which benefits from improved security and reduced contraband trafficking.

Each stakeholder category has a distinct interest, ranging from regulatory compliance to operational efficiency and commercial exploitation.

6.2 STAKEHOLDER ANALYSIS

Stakeholder analysis involves assessing the impact, influence, and interest of each stakeholder group to develop engagement strategies that maximize project adoption and sustainability.

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

Table 6-1: BAG-INTEL Stakeholder Analysis

Stakeholder Group	Impact on BAG-INTEL	Influence on Implementation	Engagement Strategy
Regulatory Authorities (EU, National Customs, Border Control, Law Enforcement)	High – Define security and customs regulations governing system deployment	High – Provide policy and legal framework for AI-powered baggage control	Regular policy briefings, compliance assessments, advisory board participation
End-Users (Customs Officers, Airport Authorities, Police, Airlines)	High – Responsible for operational deployment and real-world validation	Medium – Implementation depends on willingness to adopt and invest in technology	Pilot programs, hands-on training, usability workshops, iterative feedback loops
Industry & Tech Providers (AI, Cybersecurity, Baggage Scanners, System Integrators)	Medium – Suppliers of technical solutions and infrastructure	High – Drive innovation, customization, and long-term technological sustainability	Technical workshops, co-development initiatives, partnerships for commercialization
Academia & Research Institutions	Medium – Contribute knowledge on AI, risk assessment, and operational efficiency	Medium – Influence long-term research impact and development of advanced solutions	Research collaborations, publications, conference presentations, AI ethics panels
Policy & Standards Organizations	Medium – Ensure alignment with international security protocols and best practices	High – Define operational and security compliance frameworks	Participation in policy dialogues, contributions to standardization efforts
Civil Society & Public	Low – Indirectly impacted through improved security and efficiency	Medium – Public perception affects acceptance of AI-based customs checks	Public awareness campaigns, privacy and ethics transparency reports

6.2.1 Key Stakeholder Engagement Strategies

To ensure effective engagement and buy-in from key stakeholders, the following targeted strategies will be employed:

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

1. **Customs & Border Control Authorities**
    - Establishment of an End-User Advisory Board (EUAB) for continuous feedback.
    - Dedicated training workshops to familiarize officers with AI-driven customs control.
    - Collaborative pilots at multiple airports to validate real-world effectiveness.
2. **Technology Providers & Industry Partners**
    - Joint exploitation agreements to define business models and licensing strategies.
    - Integration of BAG-INTEL solutions into existing baggage scanning and risk detection platforms.
    - Inclusion in pre-standardization working groups to drive adoption.
3. **Regulators and Policy Bodies**
    - Close collaboration with WCO, ECAC, EASA to ensure compliance with existing frameworks.
    - Regular participation in policy roundtables and regulatory discussions.
    - Contribution to EU-funded security and AI initiatives for cross-sector integration.
4. **Academia & Research**
    - Establishment of research partnerships on AI, Digital Twins, and risk assessment.
    - Open-access scientific publications and presentations at AI and security conferences.
    - Development of training curricula for customs AI applications.
5. **Public & Civil Society**
    - Privacy impact assessments and GDPR-compliant data management policies.
    - Transparent communication on AI ethics and bias mitigation strategies.
    - Engagement through media outreach, press releases, and public webinars.

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

7 EXPLOITATION PLANS

The BAG-INTEL project involves a diverse consortium of partners, each bringing specialized expertise in AI-driven security solutions, digital twin technologies, risk assessment, and customs operations. To ensure the long-term sustainability and impact of the project's results, each partner has developed a tailored Individual Exploitation Plan (IEP) aligned with their strategic objectives, market focus, and technical contributions.

This section outlines the exploitation strategies of key project partners, detailing how they plan to leverage BAG-INTEL's innovations for commercial applications, operational improvements, and further research initiatives. These plans include direct product commercialization, technology licensing, consulting services, institutional adoption, and academic integration. These exploitation plans enhance customs efficiency, security intelligence, and border control operations across Europe and beyond by defining clear pathways to market adoption and stakeholder engagement.

7.1 INDIVIDUAL EXPLOITATION PLANS

7.1.1 STAM

STAM's exploitation plan focuses on leveraging its Multimethod Modeling and Decision Support System (DSS) for Customs to expand its expertise in digital twin technologies and predictive logistics and customs control analytics. STAM aims to integrate these innovations into commercial services for security, airport management, and supply chain optimization. The DSS is a customizable simulation tool that enables airport and customs authorities to optimize resource allocation and security checks through real-time and predictive scenario analysis. The commercialization plan includes direct sales to airports, security agencies, and border control operators, with licensing options for government institutions. STAM also plans to collaborate with AI-driven security technology providers to embed the DSS in broader risk assessment ecosystems.

7.1.2 LEGIND TECHNOLOGIES AS (LTA)

LTA's primary exploitation goal is the commercialization of AI-based security solutions for baggage control, focusing on AI-Vision-Based Reidentification of Luggage (AI4bagReID), Connection-Analysis-Based Risk Assessment (ConnRisk), and the AI-powered Decision Support System (DSS). These solutions enhance customs efficiency by automating luggage tracking, identifying high-risk baggage, and streamlining risk assessment processes. The business strategy includes direct partnerships with customs agencies, airport operators, and AI-based security software providers. LTA also plans to license ConnRisk and AI4bagReID as standalone solutions or integrated components of customs AI infrastructures. The operational framework emphasizes a subscription-based AI-as-a-service model, ensuring continuous updates and optimization through machine learning.

7.1.3 CEA (Commissariat à l'énergie atomique et aux énergies alternatives)

CEA aims to integrate its Advanced Detection Systems into existing X-ray scanning technologies and customs security infrastructures. These innovations rely on AI-powered object recognition and spectral analysis to detect contraband with enhanced accuracy. The primary commercialization strategy involves licensing AI detection algorithms to baggage scanning system manufacturers and security service providers. CEA also explores partnerships with European and global airport security bodies to facilitate pilot deployments and regulatory compliance testing. Additionally, the exploitation strategy

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

includes participation in EU security standardization bodies, positioning CEA's technologies as a core component of future regulatory frameworks for automated customs inspection.

7.1.4 UNIVERSITY OF GRANADA (UGR)

UGR focuses on the Knowledge Graph Database and Intelligent Analysis, a data-driven customs risk assessment and security intelligence methodology. The research exploitation strategy includes integrating this semantic AI technology into next-generation risk analysis platforms and collaborating with industry partners to refine predictive analytics capabilities for border security. The university aims to commercialize its research by offering consulting services and licensing the methodology to software firms specializing in customs, law enforcement, and security intelligence. Additionally, UGR plans to incorporate its findings into academic courses and research projects, ensuring long-term knowledge dissemination.

7.1.5 PSI LOGISTICS

PSI plans to exploit its CCTV AI Detection Integrator, a software system that enhances airport surveillance with AI-powered object detection. The company's exploitation strategy focuses on integrating this software into existing airport security infrastructures, targeting airport operators, customs agencies, and private security firms. The business model is centered on software licensing, with options for on-premise deployment and cloud-based monitoring services. PSI is also exploring the expansion of AI-driven video analytics for broader logistics security applications, including cargo screening and warehouse surveillance.

7.1.6 ICCS (Institute of Communication and Computer Systems)

ICCS's Secure Communication Systems provide encrypted data transmission for customs operations, ensuring GDPR-compliant information sharing among customs authorities, law enforcement agencies, and AI-driven risk assessment platforms. The exploitation plan includes direct collaborations with national and European border security agencies, offering consulting services and software licensing. ICCS also aims to expand its encryption framework beyond customs, targeting secure communications in defense, intelligence, and financial regulatory compliance.

7.1.7 SMITHS DETECTION GERMANY (SDE)

SDE's Advanced Baggage Scanning System integrates AI-enhanced object recognition into high-resolution X-ray scanners. The company plans to upgrade its existing product portfolio by embedding these capabilities into next-generation scanning systems for airports, border checkpoints, and high-security zones. The commercialization model includes direct sales to airport authorities and government agencies and licensing of AI-enhanced scanning software to third-party hardware manufacturers. Additionally, SDE is pursuing strategic partnerships with EU security bodies to establish its AI-driven detection systems as an industry standard for customs security screening.

7.1.8 EXUS SOFTWARE

EXUS aims to commercialize its AI-Based Risk and Decision Support Tool, designed to enhance customs authorities' risk analysis through machine learning and predictive analytics. The exploitation plan involves direct sales and SaaS-based licensing models, targeting customs agencies, security firms, and international trade compliance platforms. EXUS is also exploring joint ventures with AI research institutions and cybersecurity firms to refine its decision support algorithms for broader applications in financial fraud detection and organized crime prevention.

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

7.1.9 INSTITUT NATIONAL DES SCIENCES APPLIQUÉES DE ROUEN (INSA)

INSA's Optimal Probabilistic Bijective Mapping (OPBM) for Luggage Reidentification is a mathematical model for AI-driven bag tracking in customs areas. The institution plans to license this methodology to AI security firms and research institutions working on risk-based border control solutions. INSA also seeks EU and international grants to expand the technology's applications beyond customs, including AI-based image recognition for security surveillance and forensic analysis. Additionally, INSA integrates OPBM into higher education curricula, fostering cross-disciplinary research in AI, risk modeling, and applied mathematics.

7.1.10 CONCEPTIVITY s.à.r.l. (CPT)

CONCEPTIVITY will use the implementation and demonstration elements of the project to develop potential end user client engagement opportunities and furthermore, follow-on projects are possible to continue work efforts with BAG-INTEL consortium partners. The solutions resulting from the project may also represent a clear long term opportunity with an expanded set of stakeholders – including both those inside and outside the project consortium.

7.1.11 HELLENIC POLICE (HPOL)

HPOL's Customs Bag-Risk Management Tool will enhance customs risk assessment and contraband detection in operational environments. The exploitation strategy includes direct implementation within Greek customs and law enforcement agencies, with the potential for expansion through collaborative EU security projects. HPOL also works on interoperability between BAG-INTEL solutions and national security databases, ensuring long-term adoption and regulatory alignment.

7.1.12 HOCHSCHULE FÜR DEN ÖFFENTLICHEN DIENST IN BAYERN (HFOD)

HFOD's Training and Education Modules for Customs will be integrated into national customs training programs and offered to EU customs agencies as educational packages. The exploitation plan focuses on institutional adoption, with HFOD acting as a certification provider for AI-driven customs training. Additionally, HFOD is developing online training platforms to extend the reach of its educational content to customs officers across different jurisdictions.

7.2 JOINT EXPLOITATION PLANS

Beyond individual exploitation efforts, the BAG-INTEL consortium has established Joint Exploitation Plans to ensure project outcomes' collective impact and sustainability. These plans focus on integrating complementary technologies, developing shared business models, engaging in regulatory standardization, and fostering long-term collaborations across industry, academia, and public-sector stakeholders.

7.2.1 Collaborative Technology Integration and Commercialization

Several project partners are aligning their AI-driven solutions, digital twins, and risk assessment models to create integrated security platforms for customs and border control agencies. This includes:

- STAM, LTA, and INSA collaborating on the AI-Vision-Based Reidentification of Luggage (AI4bagReID), integrating LTA's AI processing with STAM's digital twin modeling and INSA's mathematical optimization framework.

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

- SDE, CEA, and PSI working together on the Advanced Baggage Scanning System, combining AI-powered detection algorithms with high-resolution scanning hardware and real-time CCTV analytics.

- UGR, ICCS, and EXUS jointly developing an AI-Based Risk and Decision Support System, integrating knowledge graph databases, encryption protocols, and predictive analytics to enhance customs intelligence.

7.2.2 Standardization and Policy Advocacy

To ensure regulatory alignment and industry adoption, BAG-INTEL partners are working together on pre-standardization activities and policy recommendations:

- LTA, ICCS, and CEA are leading efforts to establish AI security and customs risk assessment benchmarks, which will contribute to EU aviation security and customs regulations.

- STAM and PSI are working with international security bodies, including the European Civil Aviation Conference (ECAC) and the World Customs Organization (WCO), to ensure BAG-INTEL solutions align with global security frameworks.

- HFOD and HPOL contribute to training guidelines for AI-powered customs control, ensuring that BAG-INTEL methodologies become part of official security training programs across Europe.

7.2.3 Joint Market Engagement and Business Models

The consortium is developing shared commercialization strategies to maximize revenue generation and long-term sustainability:

- LTA, SDE, and PSI are exploring a software licensing model where AI-powered detection and risk assessment solutions are licensed to third-party security firms and government agencies.

- STAM and INSA offer customized digital twin simulations for airport security as a consulting and service-based business model.

- EXUS and ICCS focus on AI-powered SaaS platforms for customs risk assessment, targeting international security markets through cloud-based deployments.

7.2.4 Long-Term Collaboration and Research Initiatives

Several partners are continuing post-project research collaborations to enhance BAG-INTEL technologies:

- UGR, INSA, and CEA are forming a research consortium for AI-driven security applications, securing additional funding for advanced customs risk analysis.

- STAM and LTA are developing a next-generation AI-powered customs system that integrates real-time data fusion from multiple security sources.

- HFOD and HPOL are expanding AI training curricula for customs agencies, ensuring the long-term knowledge transfer of BAG-INTEL's findings.

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

8 STANDARDS & STANDARDISATION

Standardisation can provide the base for successful customs detection and control of passenger baggage in multiple areas – the focus has been upon the technologies used, the operational procedures and how issues are addressed.

The intention of this deliverable with respect to standardisation issues is first identifying the key relevant standards used by the different actors including users (customs primarily), equipment manufacturers (e.g. detection equipment), services providers, technology providers, software solutions and other relevant law enforcement.

And thus as an important part of this process, we have developed a very short questionnaire that we have asked a broad set of key stakeholders to complete.

This short questionnaire consisted of the seven questions as follows:

1. **What type of organisation do you represent?**

   Customs

   Law Enforcement

   Government Agency

   Equipment Manufacturer

   Technology Provider (including software)

   Consultant / Consulting

   Services Provider

   Other

2. **In which areas do you believe European / International standards are necessary:**

   Detection / scanning systems images / results

   National data sharing among customs / law enforcement

   International data sharing among customs / law enforcement

   Risk Assessment

   Other areas

3. **Are there any other areas you believe standards are necessary?**

   TEXT Answers possible

4. **Do you know and/or use standards in your daily operational activities?**

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

Yes

No

Unsure

Not applicable

5. **If you are using standards, in which areas are these and which standards are involved?**

   TEXT Answers possible

6. **Do you have any recommendations for issues that need to be addressed by standards?**

   TEXT Answers possible

7. **Is there any area lacking which needs more immediate attention?**

   TEXT Answers possible

The further intention is also to have a more complete understanding of what standards are being used and more importantly, what standardisation aspects are potentially yet to be addressed.

Within the different stakeholders there are standards that are enforced with regulations, standards that are resulting from legislation, standards that are voluntary and often driven by the stakeholders themselves (for example in detection imaging), and areas that will require further work efforts to address.

The Key Standards Development Organisations Identified by the Stakeholder Communities and their relevance:

- NEMA (https://www.nema.org/): Founded in 1926, the National Electrical Manufacturers Association (NEMA) is an ANSI-accredited Standards Developing Organization made up of business leaders, electrical experts, engineers, scientists, and technicians. They have developed the Digital Imaging and Communication in Security (DICOS) standard (Section 8.1 below). NEMA publishes more than 1,000 electrical and medical imaging standards and technical documents based on the latest science and engineering. NEMA standards promote the safety, efficiency, resilience, and sustainability of products and systems used to power the world.[32] ***NEMA is relevant as the key detection systems imaging standard DICOS is maintained by NEMA.***

- ISO (https://www.iso.org): In London, in 1946, 65 delegates from 25 countries met to discuss the future of International Standardization. In 1947, ISO officially came into existence with 67 technical committees (groups of experts focusing on a specific subject). Since then, the ISO brings together 173 countries, publishes about 25726 international standards and has 844 technical committees and subcommittees to take care of standards development. ISO standards support global trade, drive inclusive and equitable economic growth, advance innovation and promote health and safety to achieve a sustainable future. ISO provides a neutral platform where experts the world over come together to develop and agree on

[32] About NEMA, as taken from NEMA web site: https://www.nema.org/standards

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

standards. The building of consensus across multiple levels establishes trust and credibility in our organization, and the International.[33] ***Quite a number of relevant ISO Standards have been identified by the stakeholder communities (see the questionnaire results for a list and description of the multiple different standards involved).***

- IEC (https://www.iec.ch): The IEC is a global, not-for-profit membership organization, whose work underpins quality infrastructure and international trade in electrical and electronic goods. Our work facilitates technical innovation, affordable infrastructure development, efficient and sustainable energy access, smart urbanization and transportation systems, climate change mitigation, and increases the safety of people and the environment. The IEC brings together ~170 countries and provides a global, neutral and independent standardization and conformity assessment platform for 30 000 experts globally. It administers 4 Conformity assessment systems whose members certify that devices, systems, installations, services and people work as required. The IEC publishes around 10 000 IEC International Standards which together with conformity assessment provide the technical framework that allows governments to build national quality infrastructure and companies of all sizes to buy and sell consistently safe and reliable products in most countries of the world. IEC International Standards serve as the basis for risk and quality management and are used in testing and certification to verify that manufacturer promises are kept.[34] ***A number of relevant IEC Standards have been identified by the stakeholder communities (see the questionnaire results for a list and description of the different standards involved).***

8.1 REGULATORS AND REGULATIONS

Especially in the realm of civil aviation, certain regulatory bodies and regulations are key in addressing standards, specifically with respect to detection equipment addressing security issues. By extension, and within the context of the BAG-INTEL project, we are employing the same detection equipment used for security purposes in order to address critical customs control of passenger baggage and as such the standards and regulations and the regulators are relevant for what we doing in the BAG-INTEL project.

8.1.1 European Civil Aviation Conference (ECAC)

ECAC: Founded in 1955 as an intergovernmental organisation, the European Civil Aviation Conference (ECAC) seeks to harmonise civil aviation policies and practices amongst its Member States and, at the same time, promote understanding on policy matters between its Member States and other parts of the world. ECAC brings together the widest grouping of Member States of any European organisation dealing with civil aviation, being currently composed of 44 Member States. ECAC's mission is the promotion of the continued development of a safe, efficient and sustainable European air transport system.[35]

The ECAC Common Evaluation Process (CEP) of security equipment is the laboratory testing programme established by ECAC Member States to assess security equipment against ECAC/EU performance standards and provide a common reference for national administrations to certify/approve the security equipment deployed at airports under their responsibility.

[33] About ISO, as taken from ISO web site: https://www.iso.org/what-we-do.html

[34] About IEC, as taken from the IEC web site: https://www.iec.ch/what-we-do

[35] About ECAC, as taken from ECAC web site: https://www.ecac-ceac.org/about-ecac

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

The aims of the CEP are to:

- evaluate the technical performance of security equipment in an objective and standardised manner across the different participating test centres involved in the process. This includes developing and keeping up to date the applicable Common Testing Methodologies (CTMs); and
- provide ECAC Member States with reliable information on equipment performance against adopted technical standards.

In January 2020, the European Commission acknowledged the CEP as a pre-condition for the approval of civil aviation security equipment in the European Union. As a consequence, the European Commission grants automatic eligibility for the EU approval of security equipment and the "EU Stamp" marking to security equipment confirmed by the CEP as meeting ECAC/EU performance standards.

In addition, those tested configurations found to meet an ECAC/EU performance standard are published in the public part of the ECAC website, for the benefit of the wider international community, i.e. non-ECAC Member States and industry stakeholders (e.g. airport operators).

Non-ECAC States such as Australia, Canada, Israel or the United States, which have their own security equipment testing programmes, recognise the value of the CEP and participate in ECAC technical meetings to exchange information and work towards the harmonisation of performance standards and testing procedures.[36]

ECAC CEP has published a list of equipment of Explosive Detection Systems for Cabin Baggage (EDSCB[37]).

ECAC CEP is relevant because there are standards for testing detection equipment used for security purposes and this is the same equipment that is tasked with addressing customs detection requirements of passenger baggage upon arrival, and thus, these standards are relevant as the equipment has already therefore been tested to these standards.

8.1.2 Explosive Detection System (EDS)

ECAC EDS Standard 3 is a regulatory framework passed by the European Commission to improve aviation security. As new regulations demand that airports step up their security to detect a higher level of threats while lowering operational false alarm rates (FAR), hold baggage screening (HBS) entered a transformative phase with airports everywhere upgrading to ECAC EDS Standard 3 approved explosive detection systems (EDS).

ECAC EDS Standard 3 is the answer to greater operational efficiency, improved resource optimization, and more accurate security decisions.

Understanding that every airport and terminal has its own unique set of needs and constraints, our HBS solutions, offer the flexibility and scalability to meet them all. Certified with the industry's highest ECAC and TSA standards, while accompanied by specialized service teams to provide proactive support, we never leave you alone to transition."

[36] About ECAC/CEP, taken from ECAC web site: https://www.ecac-ceac.org/activities/security/common-evaluation-process-cep-of-security-equipment

[37] List of Explosive Detection Systems for Cabin Baggage (EDSCB) as published 18.10.2023 by ECAC CEP: https://www.ecac-ceac.org/images/activities/security/ECAC-CEP_Explosive_Detection_Systems_for_Cabin_Baggage_20231018.pdf

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

The benefits of ECAC EDS Standard 3 are:

- **Reduced Operational Alarm Rates**: Standard 3 delivers a reduced operational alarm rates of up to 30% as compared to Standard 2
- **Superior Image Quality**: Std 3 systems deliver superior image quality, to ensure faster and more accurate alarm resolution by operators, minimising the need for re-checks
- **Enhanced Explosive Detection**: Significantly improve detection capabilities for explosives with the highest international standards for Hold Baggage screening
- **Higher Throughput Rate**: Faster belt speed with a higher throughput of up to 1,800 bags per hour for a more efficient turnaround time.
- **Upgrade without Disruption**: With over 750 installations worldwide and industry leading programme management, we can install new HBS without disrupting your existing operations[38]

EDS explosive detection systems are also key in the detection of drugs and their precursors, and as such are very relevant for the use cases as identified and tested and demonstrated within the BAG-INTEL project.

8.2 TRANSPORTATION SECURITY ADMINISTRATION (TSA)

8.2.1 Accessible Property Screening System (APSS)

The APSS detection standard is expected to advance checkpoint capability because it requires detection of a broader range of homemade explosives, reduced false alarm rates, automated detection for threats and prohibited items, remote image screening, detection of greatly reduced threat mass, and the potential ability for passengers to leave all accessible items in bags.[39]

[38] About ECAC EDS from Smiths detection web site at https://www.smithsdetection.com/market-sectors/aviation/accelerate-security-with-ecac-eds-standard-3-explosive-detection-systems/

[39] Homeland Security - Advanced Integrated Passenger and Baggage Screening Technologies (2018) https://www.dhs.gov/sites/default/files/publications/TSA%20-%20Advanced%20Integrated%20Passenger%20Screening%20Technologies.pdf and https://www.dhs.gov/sites/default/files/publications/tsa_-_advanced_integrated_passenger_and_baggage_screening_technologies.pdf

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

9 BAG-INTEL STAKEHOLDERS COMMUNITIES SURVEY

In December 2024 and January 2025, a survey was widely circulated to all stakeholders within the Consortium and more broadly to all the stakeholder groups in order to gather feedback from stakeholders as to:

- The areas in which that they believed European / International standards were necessary;
- whether they knew of and/or used standards in their daily operations, and, if possible, which standards were used;
- if there were any areas which needed particular attention.

The survey is attached as Annex I. The Survey was distributed to all members of the Consortium, to contacts on Linked on and on the Bag-Intel web site. The survey was open for 2 months and in total, there were 59 replies.

The overall results are provided in Section 9.1-9.7

9.1 QUESTION 1: WHAT TYPE OF ORGANISATION DO YOU REPRESENT? MULTIPLE SELECTION IS POSSIBLE

The survey identified the following main stakeholders:

- Customs
- Technology suppliers, including software
- Government agencies
- Consulting firms
- Law enforcement agencies
- Service providers

In total, the survey was completed by 59 individuals who represented one or more of the above stakeholders. For example, some organizations were both customs and law enforcement. Customs, Technology providers (including software producers), Government agencies were the main areas which completed the survey. Figure 9-1provides the breakdown of the stakeholders which participated in the Survey.

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

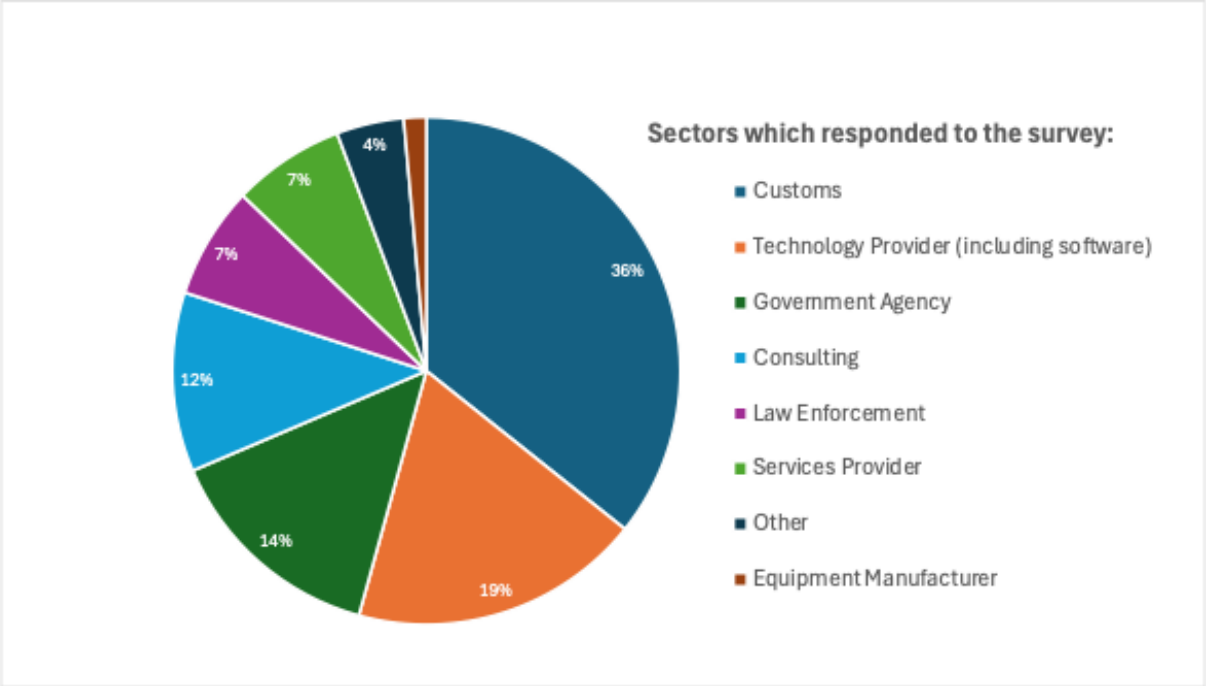

Figure 9-1: Response to Question 1 - Stakeholders which participated in the Survey

9.2 QUESTION 2: IN WHICH AREAS DO YOU BELIEVE EUROPEAN / INTERNATIONAL STANDARDS ARE NECESSARY:

The survey sought to determine which European/International standards are necessary to stakeholders. The grouping given covered the following areas with the possibility to provide select multiple options:

- Detection / scanning systems images / results
- National data sharing among customs / law enforcement
- International data sharing among customs / law enforcement
- Risk assessment
- Other areas

The areas in which it was considered that European / International standards were necessary are given in Figure 9-2.

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

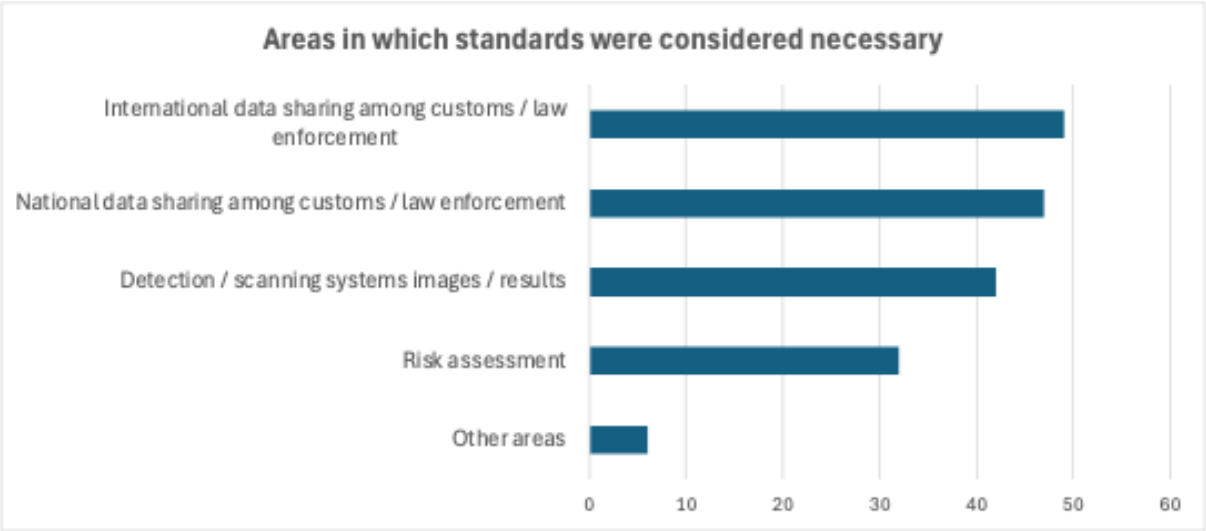

Figure 9-2: Response to Question 2 – Areas in which standards were considered necessary

9.3 QUESTION 3: ARE THERE ANY OTHER AREAS YOU BELIEVE STANDARDS ARE NECESSARY?

In addition, stakeholders identified specific areas in which they considered standards to be necessary. They are listed hereafter:

- Airport infrastructure for ingoing baggage: There need to be space specifications in the baggage pipeline (conveyor belt before the carousel) to ensure sufficient space for scanner/sensor equipment which may be used to detect contraband in the baggage.
- Export control: More EU security standards on export control.
- National data sharing among customs / law enforcement in order to maximize efficiency and utilization of time.
- Customs training.
- Providing harmonized solutions for customs classification of goods.
- Commercial and transport documentation.
- Data standards for Customs post audits. Multiple supervisors and others ask the same data from a company which costs the company a lot of time. The standard is not only for customs but for all supervisors. One standard multiple users. Also, the internal audits can use this standard.
- Standards for recruitment, minimum training requirements, common responsibilities of customs, legal powers, pay to equal or exceed national averages.

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

- Various standards, i.e. anti-smuggling sharing best practices. Reporting etc. Communication with member state countries (easy friendly secure equipment).
- x-ray scanning equipment for customs/law enforcement.
- Help custom and tax admininistrtions to improve cooperation.
- Sharing data customs with other authorities (like market surveillance).
- Formats for decision support algorithms in X-ray image analysis; Software environment for the implemention of decision support algorithms in X-ray image analysis.
- Safe and faster trade.
- Standards are necessary in all areas of law enforcement if we are to deal with international organized crime. Through overseas assistance from national bodies and other organisations such as the UN, OSCE etc countries can achieve uniform standards. The problem of course is dealing with countries with poor human rights, corrupt and venal legal systems, death penalty etc. Assisting repressive regimes in border control is difficult when it is used for political ends.
- Data Privacy and Security: Ensuring compliance with GDPR and other privacy regulations when sharing passenger and baggage data across systems.
- Training and Usability: Establishing best practices for training customs officers and other personnel on tools and interfaces.
- Citizens/travelers data sharing and how these are treated by the authorities.
- Areas involving cybersecurity facets, such as ISO 27001 on data accuracy, confidentiality & availability, ISO27018 surrounding Cloud-based data privacy, ISO22301 on business continuity planning vis-a-vis disruptive actions undertaken by the attacker and so on.
- System Safety, Security, Medical & Health sectors, production, Energy Generation & Distribution, Backing & Stock Market, Risk & Emergency Management, Transportation, Insurance, Communication, Near & Far Space Exploitation, Wast Collection, Recycling & Disposal.
- Artificial intelligence

A broad range of aspects have been indicated, however the answers have a number of key elements noted, namely (but not limited to): Training, Specific Data Sharing, Documentation, Incoming Baggage Screening, Cyber Security, Data Privacy, Software and Technology, etc. Quite a number of these areas are already being addressed and we have provided a summary level in the results and conclusions section of this deliverable.

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

9.4 QUESTION 4: DO YOU KNOW AND/OR USE STANDARDS IN YOUR DAILY OPERATIONAL ACTIVITIES?

The reply on awareness of standards and usage of standards in daily operational activities resulted in a more than half of the participants confirming that they use standards in their daily work.

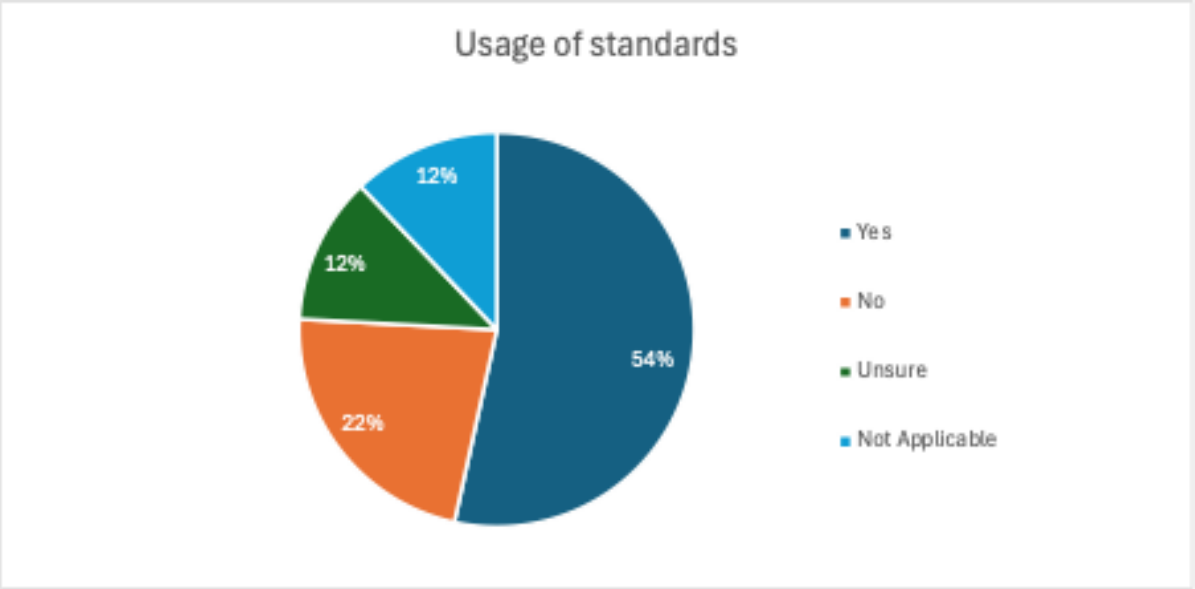

Figure 9-3: Question 4 -Usage of standards in daily operations

9.5 QUESTION 5: IF YOU ARE USING STANDARDS, IN WHICH AREAS ARE THESE AND WHICH STANDARDS ARE INVOLVED?

The following list of standards are those specifically identified by stakeholders in the Survey. The ISO standards are, among other things, employed in the areas of exercise planning and testing, quality requirements for systems, and the interaction involving machines and humans. Namely, the ISO standards corresponding to those are, ISO22398:2013, ISO/IEC TR 25060:2010, ISO 9241-11:2018., including those related to Information security, i.e., ISO 27001 regarding certification of information security management system and ISO 27002 for implement and security measures.

- ISO 5401:2024 – Audit Data Collection – Customs and Indirect Tax Extension
- ISO 21378 - 2019 Audit Data Collection
- ISO-9001-2015 - Standard for Quality Management Systems (QMS)
- ISO-27001 - Information Security Management systems (ISMS)
- ISO-27002 - Information Security, Cybersecurity and Privacy Protection – Information Security Controls

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

- ISO/IEC-27005:2022 - Information Security, Cybersecurity and Privacy Protection – Guidance on Managing Information Security Risks
- ISO-22398:2013 - Societal Security – Guidelines for Exercises
- ISO/IEC TR 25060:2023: Systems and Software Engineering
- ISO 9241-11:2018: Ergonomics of Human-System Interaction
- ISO-45001: Occupational Health and Safety
- Kyoto Convention
- DICOS

These represent the key standards used by the different stakeholder community groups and the following Sections 9.5.1 to 9.5.11 provide a brief description of each of these standards.

9.5.1 ISO 5401:2024 – Audit Data Collection – Customs and Indirect Tax Extension

This document specifies the functional requirements that build on ISO 21378 for audits in the areas of customs duties and indirect taxes [e.g. value-added tax (VAT) and excise duties]. It addresses how tax auditors obtain audit data for these audits, including data element formats and to some extent content requirements.

In practice, this document applies to virtually every step in the whole process in the supply chain and covers both goods, services and works.

It includes domestic transactions, cross-border transactions (import and export) and can cover both third-party and intercompany transactions or even movements of goods within the same company. This document does not describe when an event is taxable nor how to calculate tax or customs duties as this is legislation-specific and the situation can vary from country to country or even within the same country.

This document covers standard exchange of the data related to taxable operations/activities by businesses to perform controls and audits more effectively and efficiently through automated tests. This document focuses on the characteristics related to taxability and the related formalities of the indirect tax and customs duties regulations. It includes the result of a tax calculation, the relevant underlying parameters which can be processed by ERP-systems and/or indirect tax/customs duties systems, and data needed to comply with indirect tax and customs duties legislation and formalities.

This document is not designed to collect audit data from the regulators like tax and/or customs authorities.[40]

9.5.2 ISO 21378 - 2019 Audit Data Collection

This document aims to resolve the common problems that auditors face when requesting data to perform their audit procedures. The information contained within this document will help to improve the accessibility and transparency of audit data, standardize the process of collecting audit data, avoid duplicate efforts and save resources. The worldwide standardization of audit data content and formats

[40] About ISO 5401:2024, as taken from ISO web site: https://www.iso.org/standard/81231.html

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

will enhance the effectiveness and efficiency of government, internal and external audits, and provide benefits to related stakeholders.

This document focuses on major business modules of accounting and ERP systems that are typically used in various organizations. These modules relate to major business processes, including the areas of purchase, sales, inventory, fixed assets and financial reporting, with the aim to identify and specify the data elements and file formats needed for auditing.[41]

9.5.3 ISO-9001-2015 - Standard for Quality Management Systems (QMS)

ISO 9001 is a globally recognized standard for quality management. It helps organizations of all sizes and sectors to improve their performance, meet customer expectations and demonstrate their commitment to quality. Its requirements define how to establish, implement, maintain, and continually improve a quality management system (QMS).

Implementing ISO 9001 means your organization has put in place effective processes and trained staff to deliver flawless products or services time after time.[42]

9.5.4 ISO-27001 - information security management systems (ISMS)

The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.

Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard.[43]

9.5.5 ISO-27002 - Information Security, Cybersecurity and Privacy Protection – Information Security Controls

The ISO 27002 international standard provides guidance for organizations looking to **establish, implement, and improve an Information Security Management System** (ISMS) focused on **cybersecurity**. While ISO/IEC 27001 outlines the requirements for an information security management system **(**ISMS), ISO/IEC 27002 offers best practices and control objectives related to key cybersecurity aspects including **access control, cryptography, human resource security, and incident response**. The standard serves as a **practical blueprint** for organizations aiming to effectively safeguard their information assets against cyber threats. By following ISO/IEC 27002 guidelines, companies can take a proactive approach to cybersecurity risk management and protect critical information from unauthorized access and loss.[44]

9.5.6 ISO/IEC-27005:2022 - Information Security, Cybersecurity and Privacy Protection – Guidance on Managing Information Security Risks

This document provides guidance to assist organizations to:

[41] About ISO 21378:2019, as taken from ISO web site: https://www.iso.org/obp/ui/en/#iso:std:iso:21378:ed-1:v1:en

[42] About ISO 9001-2015, as taken from ISO web site: https://www.iso.org/standard/62085.html

[43] About ISO/IEC 27001, as taken from ISO web site at https://www.iso.org/standard/27001

[44] About ISO 27002, as taken from ISO web site: https://www.iso.org/standard/75652.html

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

— fulfil the requirements of ISO/IEC 27001 concerning actions to address information security risks;

— perform information security risk management activities, specifically information security risk assessment and treatment.[45]

9.5.7 ISO-22398:2013 - Societal Security – Guidelines for Exercises

The ISO 22398:2013 international standard describes the elements of a generic approach to planning, conducting and improving exercise programmes and projects. The purpose of this International Standard is to:

— provide a basis for understanding, developing and implementing an effective exercise programme within an organization;

— provide guidelines for planning and conducting an exercise project;

— enhance the organization's ability to conduct exercises with internal and external involved parties;

— assist the organization with developing and assessing its exercising capability in a consistent and risk-assessed manner that reflects good practice; and,

— enable continual improvement in exercise programmes and projects within an organization.[46]

9.5.8 ISO/IEC TR 25060:2023: Systems and Software Engineering

This document focuses on those information items needed for design, development and evaluation of usable systems, rather than prescribing a specific process."[47]

9.5.9 ISO 9241-11:2018: Ergonomics of Human-System Interaction

This document provides a framework for understanding the concept of usability and applying it to situations where people use interactive systems, and other types of systems (including built environments), and products (including industrial and consumer products) and services (including technical and personal services).[48]

9.5.10 ISO-45001: Occupational Health and Safety

ISO 45001 is an international standard that specifies requirements for an **occupational health and safety (OH&S) management system**. It provides a framework for organizations to manage risks and improve OH&S performance.

The standard establishes criteria for an OH&S policy, objectives, planning, implementation, operation, auditing and review. Key elements include leadership commitment, worker participation, hazard

[45] About ISO 27005, as taken from ISO web site: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:en

[46] About ISO-22398:2013, as taken from ISO web site: https://www.iso.org/obp/ui/#iso:std:iso:22398:ed-1:v1:en

[47] About ISO/IEC TR 25060:2023, as taken from ISO web site: https://www.iso.org/standard/83763.html

[48] About ISO-9241-11:2018, as taken from ISO web site: https://www.iso.org/obp/ui/en/#iso:std:iso:9241:-11:ed-2:v1:en

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

identification and risk assessment, legal and regulatory compliance, emergency planning, incident investigation and continual improvement.

ISO 45001 utilizes the Plan-Do-Check-Act methodology to systematically manage health and safety risks. It applies to organizations of all sizes and can be integrated with other ISO management system standards.[49]

9.5.11 Kyoto Convention

The International Convention on the simplification and harmonization of Customs procedures (as amended), known as the Revised Kyoto Convention is the blueprint for modern and efficient Customs procedures in the 21st century.

The Convention elaborates several key governing principles- chief among these are the principles of:

- transparency and predictability of Customs actions;
- standardization and simplification of the goods declaration and supporting documents;
- simplified procedures for authorized persons;
- maximum use of information technology;
- minimum necessary Customs control to ensure compliance with regulations;
- use of risk management and audit based controls;
- coordinated interventions with other border agencies;
- partnership with the trade.

The revised Kyoto Convention promotes trade facilitation and effective controls through its legal provisions that detail the application of simple yet efficient procedures. The revised Convention also contains new and obligatory rules for its application which all Contracting Parties must accept without reservation.

The revised Kyoto Convention entered into force on February 3, 2006.[50]

In addition, stakeholders mentioned general areas in which they used standards, namely:

- Import, transit and export control;
- Customs Datamodels;
- Customs related standards (SAFE framework, HS Convention, Agreement on Customs Valuation, etc.);

[49] About ISO 45001, as taken from the ISO web site: https://www.iso.org/standard/63787.html

[50] About the Kyoto convention, as taken from the WCO web site: https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/conventions/pf_revised_kyoto_conv.aspx

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

- Risk assessment, post clearance audit, trade facilitation (AEO);
- Reports, international standards;
- Customs declaration processing and (in development) image meta data standards
- X-ray image quality indicators (ASTM and IEC/ ISO standards), information security (ISO), laboratory performance (ISO);
- Customs valuation, HS and Tarif, RoO,
- Border Force not only has Codes of Conduct and standards but has a regular assurance checks;
- Standard operating procedures;
- X-ray detection of explosives + prohibited items, standards issued by ECAC and TSA;
- Detection;
- Aviation security cabin baggage: ECAC EDSCB; ECAC EDS; TAG; TSA APSS
- Data security.

9.6 QUESTION 6: DO YOU HAVE ANY RECOMMENDATIONS FOR ISSUES THAT NEED TO BE ADDRESSED BY STANDARDS?

Stakeholders provided the following recommendations for issues that need to be addressed by standards:

- The conveyor belt before the carousel in the baggage claim area should be shielded from this area and have space for scanner/sensor equipment and possibly also a part of the belt where sniffer dogs can be employed (i.e., a "dog track").
- Data sharing, more time efficient operations.
- Electronic versions Commercial documentation and transport documents need to be standardised at global level.
- The most important aspect of sharing information for risk management is the means by which it is done. There should be a standard for sharing information via Blockchain, using the OMA data model.
- Fraud and smuggling are international. It is essential that national customs authorities can share intelligence on a daily basis, coordinating their responses to risk. Low pay encourages corruption and should be set by national authorities at a level to reduce that risk. Basic training to ensure minimum standards are set.
- Use of AI in risk assessment.
- Standards needs to be explained before they are used.

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

- Clear, unambiguous, based on best practices.
- Standards on information exchange in general are very much needed.
- Recycled commodities, used cars.
- Not within our organisation, when working overseas training with other law enforcement organisations, we make recommendations.
- Image standards.
- Customs risk assessment, data and images sharing.
- Ensuring adequate sharing of detection standards between international partners; ensuring evaluation against standards is technology agnostic; facilitating training with real materials or simulants of the same; end-of-life re-evauation.
- Setting clear guidelines for the quality, consistency, and interpretation of detection and scanning system images and results, ensuring reliable identification of contraband.
- Security by design concerning the platform
- Potential issues seeking to be addressed by standards are, for the most part, relatable to the CIA properties of collected data, namely Confidentiality, Integrity & Availability.

Again, a number of areas have been noted across many different topics including, but not limited to: data sharing, intelligence sharing, equipment standards, risk assessment, training / best practices, technology, and even operational concepts such as the "dog sniffing area".

9.7 QUESTION 7: IS THERE ANY AREA LACKING WHICH NEEDS MORE IMMEDIATE ATTENTION?

The following areas were identified as requiring more immediate attention:

Safe, private and secure application:

- Support for safe, privacy secure application of law enforcement databases (e.g., SIS II);
- Fast exchange between European customs agencies of experienced new drug substances and new smuggling modus operandi;
- Fast exchange of information between customs and law enforcement, since serious smuggling is often connected to organised crime.
- Movement of clothing in small clothing packages purchased through online causes a huge financial loss due to under pricing by sender i.e. not disclosing the correct customs value by sellers this resulting in incorrect taxes collect. An example is shein and temu.
- Even closer and more cooperation between EU National Contact Points
- Border crossing, detection of illicit goods

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

- Ensuring harmonization of classification of goods for customs purposes
- Standardisation of images produced by detection technology
- Minimum IT requirements at border stations.
- Communication with member state countries. There is a need for a secure way of communicating (available system for all memberstate countries) - that´s a kind of standard.
- AI use in customs/law enforcement activities
- Intelligence data
- Scan and detection images
- Customs will need to be able to process all kinds of sensor data. Most of the sensors (e-seal, field analytical tool, X-ray image data, etc) the data processed by the sensors are seldomly open source and/ or strandardized. This makes every step in this field a complex one involving a multitude of commercial entities. Next the documents we need to process (BoL, licenses, etc.) seldomly carry a worldwide standard which multiplies every step (iand investment) in coming to process these documents.
- Recycled economy need immediate attention.
- Issues that need to be addressed by Border Force are predominantly to do with manning levels and poor prioritisation within the organisation. For example minimising queues at ports takes priority over border security. Whilst all law enforcement agencies bemoan lack of manpower, it does impinge on robust border checks both in immigration & customs.
- Customs data sharing
- Risk assessment
- Risk assessment sharing
- Faster turnaround for evaluation of new systems and technologies; how to address ML and AI in detection standards; how to integrate cybersecurity requirements without requiring retesting.
- Pharmaceutical & drugs industry

Many of the answers here focus upon exchange of information, exchange of intelligence, understanding and sharing of modus operandi of the criminal elements and risk assessment. While there are many mechanisms in this area, there are often national and international issues and aspects which prevent total open information / intelligence / criminal operations sharing of this.

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

10 THE DICOS IMAGE STANDARD

One of the issues encountered within the realm of detection technology equipment was the different proprietary image standards that were utilised by each different manufacturer. As such, unless you had the software of the given manufacturer, you could not readily share and interpret images from different equipment, so that the sharing of images even among government agencies, custom and law enforcement in the same country could be quite limited.

The result was an effort driven by the manufacturers and the security industry to both address the imaging standard as well as to look at an "open architecture" approach in order to enable and facilitate the sharing and exchange of images from different manufacturers' equipment to different sets of users of stakeholders in customs, law enforcement and other relevant government agencies.

And thus the DICOS (Digital Imaging and Communication in Security) standard was developed along with the industry "Open Architecture" approach.

This section thus explains the DICOS standard as well as the open architecture efforts within the manufacturers and the security industry and furthermore, we also include a reference to a similar earlier imaging standard used in the medical health care field (DICOM).

10.1 DIGITAL IMAGING AND COMMUNICATION IN SECURITY (DICOS)

In the area of imaging and communications technologies, NEMA developed the Digital Imaging and Communication in Security (DICOS) Standard which provides a "data interchange protocol and interoperable, data interchange protocol and interoperable, extensible file format to facilitate data information interchange (e.g., demographic information, x-ray radiographs, material-specific information, trace detection signatures, and/or threat assessment) for humans, animals, and other objects of inspection for utilization across range applications.

The DICOS Standard is designed to, and offers, the following benefits:

1. Modular: Data entered for one purpose is reusable for other purposes.
2. Standardized: Metadata associated with a security image is standardized so that the transmitting and receiving device both read and understand the metadata associated with a security image.
3. Interoperable: Metadata associated with an image captured and transmitted from one manufacturer's device can be read and understood by a receiving device from another manufacturer.
4. Extensible: Should an implementing entity wish to use additional technologies for security examination purposes in the future, DICOS can be extended to accommodate new technologies
5. Responsive: DICOS permits the exchange of security images (where appropriate) and standard metadata in a timely fashion[51]

[51] About DICOS from NEMA web site https://www.nema.org/membership/nema-councils/imaging-and-communications-council/dicosusa

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

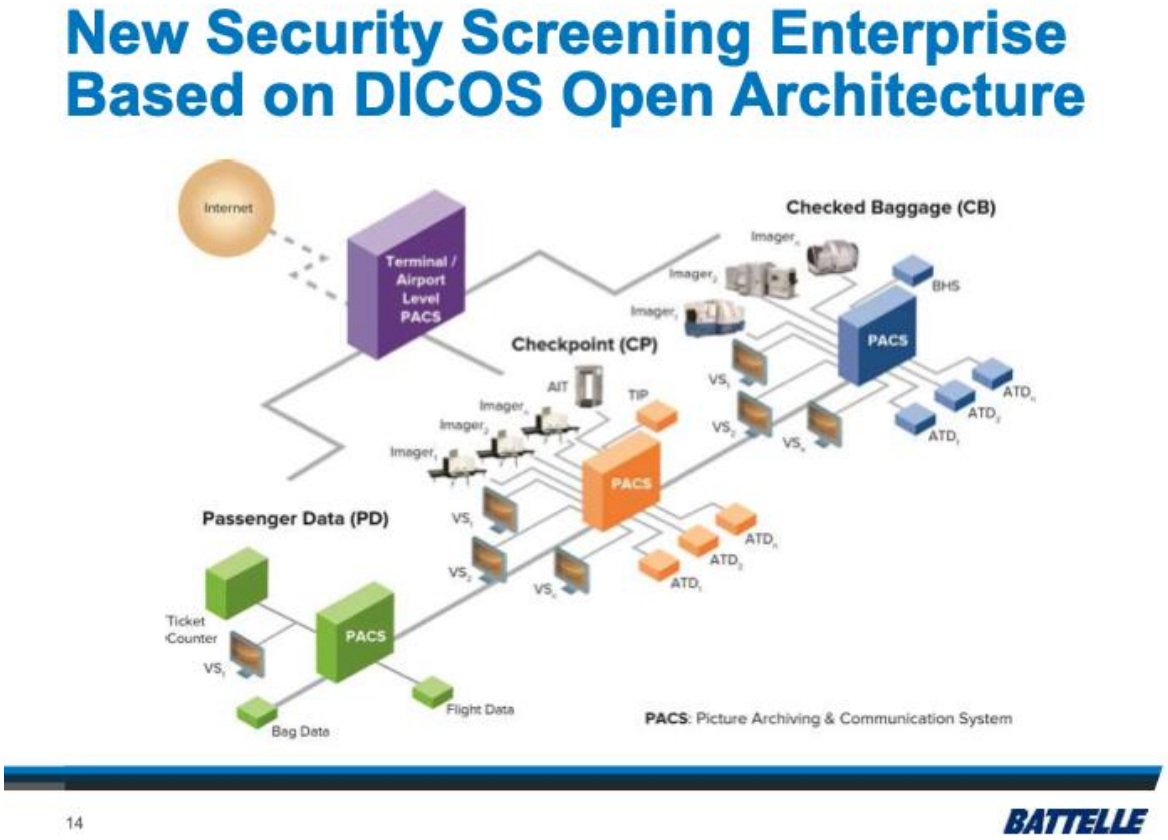

Figure 10-1: New Airport Security Screening Paradigm as illustrated by Battelle[52]

The advantages of DICOS as provided by Battel are given hereafter in the list entitled "DICOS Value Proposition"[53].

[52] Figure of New Airport Screening Paradigm, as taken from Battelle web site: https://www.battelle.org/docs/default-source/infrastructure/brochures/dicos_612.pdf

[53] As taken from Battelle web site: https://www.battelle.org/docs/default-source/infrastructure/brochures/dicos_612.pdf

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

DIGITAL IMAGING AND COMMUNICATIONS IN SECURITY (DICOS)

DICOS Value Proposition

Feature/Capability	Value Proposition
Open architecture, interoperability	Interchangeability of a true plug-and-play environment enables numerous benefits: • Reduced prices (system and software) resulting from greater competition • Accelerated development cycles resulting from more players/resources • Innovation through non-traditional participants (e.g., algorithm developers)
DICOS – open architecture standard	DICOS is derived from DICOM: • Proven based on DICOM's worldwide experience and use over many decades Published and non-proprietary, allowing users to control the standard through a standards development organization (SDO) • Strengthened through industry collaboration and NEMA DICOS standards committee • Adaptable over time as needs arise and new technologies emerge
Networked screening systems	Networking interconnects all generators (screening equipment and security data) and users of security information for multiple benefits: • Images and other metadata can be viewed at any workstation; all system elements, including PACS, are integrated to maximize interchange and use of screening related information resulting in prompt and appropriate system response • Centralized equipment performance data can be analyzed over time to identify systems degradation or potential operational issues
Risk-based security	Risk-based security is greatly enabled/enhanced by DICOS permitting new concepts of operation (CONOPS): • Networking allows remote/dynamic data entry (e.g., hand-held tablets) to improve situational understanding and on-the-spot response • Real time access to all data improves risk analysis capability and responsiveness to changing security environment • Open security architecture allows enhanced security response (e.g., different algorithms linked to different security risks)
Common image and data standard	DICOS record consolidates all relevant passenger security data to improve security enterprise: • Centralizes PAX images (baggage, avatars) and associated metadata; other data (e.g., biometrics) can be added • NEMA IIC 1 v02A standard provides 232 pages of details of this image/data standard • PAX data can be complemented with third party input (e.g., screener response, behavioral officer input, etc.) • Data can be stored and retrieved as required from PACS for analysis, investigations, and response
Operational benefits	• "Performance over time" analysis of equipment optimizes maintenance • Real-time monitoring/analysis of screening process increases efficiency • Real-time monitoring of screeners improves performance • Screening data and metrics collected online improves CONOPS

Every day, the people of Battelle apply science and technology to solving what matters most. At major technology centers and national laboratories around the world, Battelle conducts research and development, designs and manufactures products, and delivers critical services for government and commercial customers. Headquartered in Columbus, Ohio since its founding in 1929, Battelle serves the national security, health and life sciences, and energy and environmental industries. For more information, visit www.battelle.org.

800.201.2011 | solutions@battelle.org | www.battelle.org

BATTELLE
It can be done

ID 612 10/17

Figure 10-2: DICOS Value Proposition as given by Battelle

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

10.2 EOS OPEN ARCHITECTURE STUDY GROUP

On April 23, 2023, the European Organisation for Security (EOS) Open Architecture Study Group released a Standard Application Programming Interface (API) for development of Open Architecture (OA)-based screening solutions. The API was designed to facilitate the exchange of DICOS x-ray images and related data between operational screening devices for image analysis and display of screening results. It supports real -time streaming and is non-proprietary.[54]

The U.S. Transportation Security Administration (TSA) has an active role in the current revision of the DICOS Standard and previously worked with NEMA to publish the previous version. The current revision will include areas like streaming security image data, enhanced threat detection reporting, and new modalities such as air cargo.

The TSA initiative for an imaging standard to meet open architecture and interoperable requirements necessary to meet emerging threats is imperative. DICOS accomplishes this mission by improving security screenings of checked baggage, cargo, and passengers. [55]

10.3 DIGITAL IMAGING AND COMMUNICATIONS IN MEDICINE (DICOM)

DICOM is the international standard for medical images and related information (ISO 12052). And DICOS (section 10) is an adaption of Digital Imaging and Communications in Medicine (DICOM).

It defines the formats for medical images that can be exchanged with the data and quality necessary for clinical use. DICOM is implemented in almost every radiology, cardiology imaging, and radiotherapy device (X-ray, CT, MRI, ultrasound, etc.), and increasingly in devices in other medical domains such as ophthalmology and dentistry.

[54] EOS Press Release from EOS web site: https://www.eos-eu.com/Files/EOS%20PRESS%20RELEASE_API%20FOR%20OA%20RELEASED_26%20April%202023.pdf

[55] Taken from NEMA site : https://www.nema.org/membership/nema-councils/imaging-and-communications-council/dicosusa

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

11 CONCLUSIONS AND ANY RECOMMENDATIONS

The BAG-INTEL project significantly advances AI-driven customs control, integrating cutting-edge machine learning, digital twin modeling, and risk-based decision-support systems to enhance security and operational efficiency. This deliverable, D6.3: Standardisation, Exploitation, and Sustainability Strategy and Plan, outlines the project's approach to ensuring its long-term impact, commercial viability, and integration within customs and security infrastructures.

The preliminary market and competition analysis indicates that the global customs security landscape is evolving towards AI-based automation, driven by increasing trade volumes, regulatory compliance requirements, and the need for enhanced contraband detection technologies. BAG-INTEL's solutions provide a competitive advantage through AI-powered baggage reidentification, dynamic risk assessment, and digital twin technology, offering a scalable and adaptable alternative to traditional security solutions.

Despite its technological strengths, the project faces key market entry challenges, including regulatory compliance, stakeholder resistance, and integration complexities with existing security infrastructures. Addressing these barriers requires a multi-faceted approach, including early engagement with customs authorities, regulatory bodies, and industry stakeholders to facilitate adoption. The project's exploitation strategy ensures that its innovations are positioned for commercial uptake, with specific Key Exploitable Results (KERs) identified for licensing, technology transfer, and direct implementation in airport security operations.

Using PESTLE and SWOT methodologies, BAG-INTEL's socioeconomic impact analysis highlights the project's potential to contribute to border security modernization, reduced operational costs, and improved traveler experience. The project aligns with EU policy frameworks and global security initiatives, reinforcing its relevance within international customs operations. The stakeholder engagement strategy ensures that key actors—including customs agencies, airport operators, and AI technology providers—are actively involved in deploying and refining BAG-INTEL solutions.

The individual and joint exploitation plans developed by project partners provide a roadmap for the commercialization and long-term sustainability of the results. By aligning business models with market needs, leveraging strategic collaborations, and ensuring regulatory compliance, BAG-INTEL is well-positioned to become a leading AI-driven solution for next-generation customs control.

Standardisation is a tool which enables structures and organisations to have similar approaches and to be able to share data and information in compatible formats. Quite a number of the issues represented in the responses from the communities of stakeholders in the survey are actually not truly standards issues as mentioned below.

Furthermore, the reality is that the standardisation process takes a significant amount of time and the timeframe for our BAG-INTEL project is not sufficient to ensure that even the first steps can be accomplished, however, in this deliverable we have noted that a number of efforts are already underway, in some cases driven by the technology providers, at times also driven by the users communities, such that the issues and challenges are already well known and are currently in the process of being addressed.

Adding to the complexity are the issues of both national regulations and trust aspects in customs and law enforcement data sharing, intelligence sharing, criminal modus operandi sharing, and cooperative law enforcement, leading to selective sharing and controlled interactions which are not fully "open" between the different law enforcement agencies operating in different countries, under different rules

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

and regulations and having different concepts of operations and different focal issues in the day to day activities. While these aspects potentially touch upon standards, the limiting factors are related to the regulatory aspects and the “human in the loop” issues.

At the same time, a number of different mechanisms exist for information sharing, law enforcement cooperation, intelligence sharing, and criminal modus operandi understanding as these are managed by law enforcement agency cooperative groupings such as EUROPOL, INTERPOL, the World Customs Organisation and other inter-agency organisations.

And thus, in the end, the vast majority of issues identified in the final questions of the survey are actually not aspects that can fully be addressed with standards, but rather by increased cooperation via structures that already exist.

There is one important conclusion point about standardisation, which is evident from our analysis of existing standards and successful standardisation activities and that is the active involvement of industry providing the solutions working alongside the regulatory bodies and the end users. DICOS is an example of this where the detection technology industry was implicated from “day one” in this standard development and continues to play a very active part in the evolution of the development of the standard. This can be considered one of the best practices benchmarks in the standards development process.

The final conclusion is that there are already many relevant and useful standards available, which are key to the operational success of customs control of passenger baggage, with mechanisms for information and intelligence sharing already in place, having still limitations related to national regulations and controls and trust aspects.

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