ACI EUROPE
AIRPORTS COUNCIL INTERNATIONAL

A PRACTITIONER'S GUIDE TO

SAFE & COMPLIANT AI SOLUTIONS IN AIRPORT OPERATIONS

By Airport Intelligence & Jetpack.AI

June 2026

By Airport Intelligence & Jetpack.AI

airport intelligence

JETPACK.AI

Contents

Executive Summary

This guidebook provides a comprehensive framework for airports to adopt artificial intelligence (AI) in a safe, compliant, and value-driven manner, with a particular focus on operational and airside applications. As AI technologies rapidly mature and become embedded in critical airport processes, airports must move beyond experimentation and implement structured approaches that balance innovation with safety, regulatory compliance, and organisational readiness.

This guidebook is intended for airport professionals responsible for planning, implementing, or supervising AI-enabled operational systems, with a particular focus on airside operations. It is relevant to (higher) management seeking to understand regulatory requirements and key decision points; operations teams integrating AI into daily processes such as stand allocation and turnaround; safety and compliance officers ensuring adherence to regulatory and governance standards; and procurement and IT teams evaluating and contracting AI solutions. While the emphasis is on airside operations, the principles are broadly applicable to other airport domains where data quality, accountability, and compliance are critical.

AI is increasingly enabling airports to improve efficiency, resilience, and decision-making through applications such as predictive maintenance, resource optimisation, and real-time situational awareness. While these capabilities offer significant benefits, they also introduce new risks, including system complexity, evolving human–machine interaction, and reduced ability to rely on historical safety data. As a result, proactive preparation for AI adoption is essential.

A central theme of the guide is alignment with existing regulatory and safety frameworks. Although no dedicated AI regulation for airports currently exists, a strong foundation is provided by the EU regulatory framework, including the EU AI Act, Regulation (EU) 2018/1139 (Basic Regulation), and Implementing Regulation (EU) No 139/2014, complemented by EASA Acceptable Means of Compliance (AMC) and Guidance Material (GM), ICAO Annex 19, and the ACI Safety Management Framework. The EU AI Act is particularly significant, introducing a risk-based classification of AI systems and requirements for high-risk applications, including risk management, transparency, human oversight, and traceability. Airports must integrate these obligations into existing safety management systems and operational processes, ensuring AI systems remain continuously monitored and auditable.

Beyond compliance, AI adoption must be justified through a clear business case. The guide highlights both qualitative benefits (such as improved safety, better decision-making, and enhanced passenger experience) and quantitative gains (including reduced maintenance costs, improved operational efficiency, and increased throughput). A structured methodology is proposed to identify, prioritise, and evaluate AI use cases, combining operational needs, data readiness, risk analysis, and financial impact.

The successful implementation of AI solutions follows a defined lifecycle consisting of ideation, proof of concept, production deployment, and ongoing maintenance. At each stage, airports must evaluate solutions across multiple dimensions, including business value, feasibility, data quality, technology maturity, security, safety, compliance, and workforce impact. These dimensions are interdependent and require clear decision criteria to determine whether projects should progress or be reconsidered.

Risk management is a critical component throughout this lifecycle. Common challenges include poor data quality, lack of stakeholder alignment, cybersecurity vulnerabilities, over-reliance on automated systems, and evolving regulatory requirements. In safety-critical environments, such as airside operations, particular attention must be paid to maintaining human oversight, ensuring explainability of AI outputs, and designing robust fallback mechanisms.

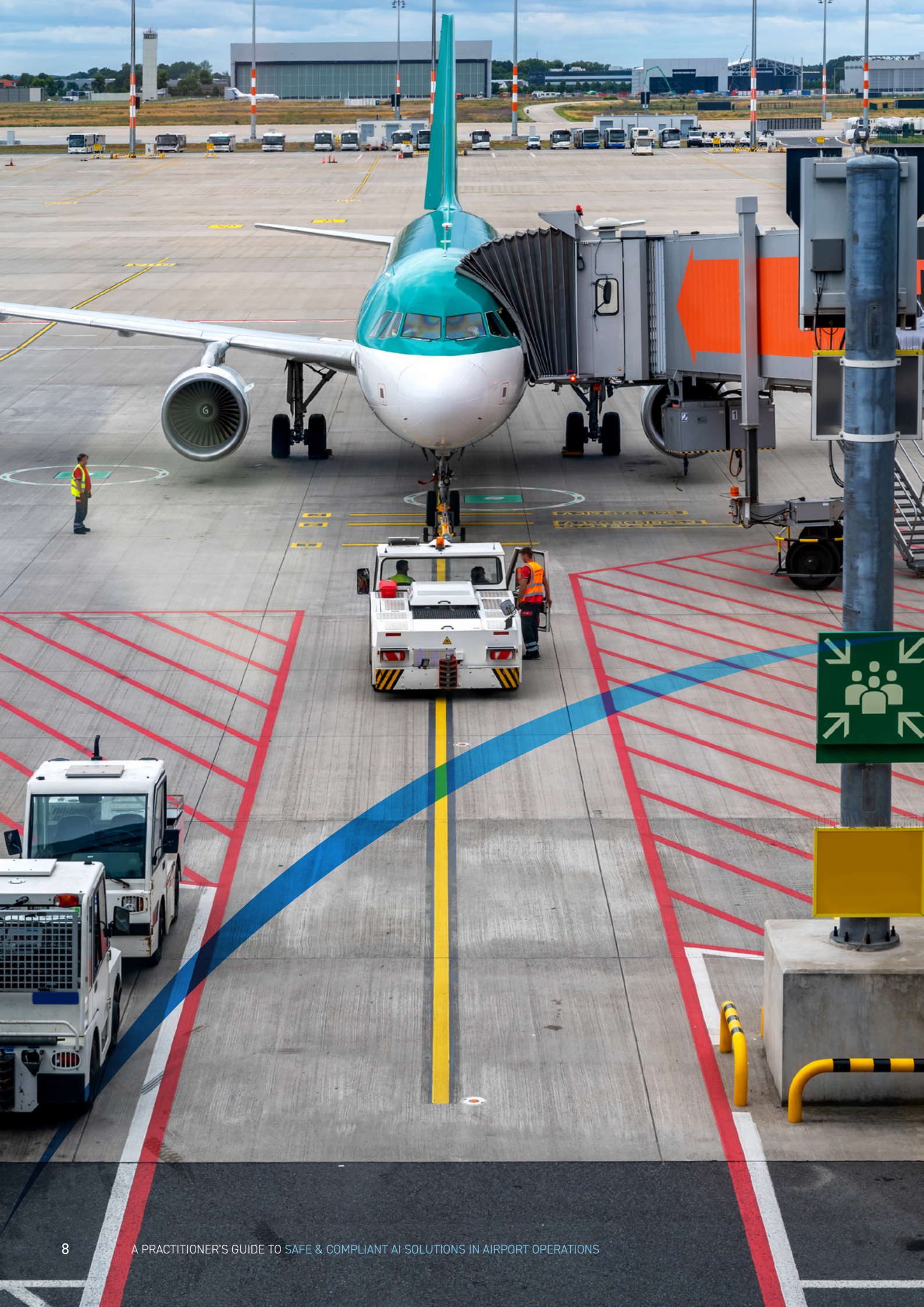
Data governance emerges as a foundational enabler of AI success. Airports must establish clear data ownership, enforce quality standards, and implement continuous monitoring processes. Since AI systems increasingly generate new data that feeds other systems, governance frameworks must also address the risks of feedback loops and data drift. Strong data practices are essential not only for performance but also for regulatory compliance and trust.

The guide further addresses practical implementation decisions, such as whether to build, buy, or adopt hybrid AI solutions, and whether to rely on single or multiple vendors. These decisions should consider total cost of ownership, internal capabilities, vendor dependence, and long-term flexibility. In complex airport ecosystems involving multiple stakeholders, governance must ensure interoperability, data sovereignty, and consistent quality standards across all participants.

Real-world use cases illustrate how these principles are applied in practice. Examples include computer vision-based turnaround monitoring, AI-driven document classification, and staffing optimisation tools. These cases demonstrate that while the specific risks and requirements vary, a consistent focus on safety, compliance, and operational integration is essential across all AI applications.

Finally, the guide emphasises the importance of organisational readiness and governance. Airports should establish dedicated AI governance structures, clearly defined roles and responsibilities, and integration with existing safety and compliance functions. Workforce engagement, training, and change management are critical to building trust and ensuring successful adoption. AI should be positioned as an enabler of human decision-making, rather than a replacement, to foster acceptance and effective collaboration.

In conclusion, the adoption of AI in airport operations represents a significant opportunity to enhance efficiency and safety, but it requires a disciplined, system-wide approach. By aligning with regulatory frameworks, investing in data and governance, and embedding AI within existing operational and safety processes, airports can unlock the benefits of AI while maintaining the highest standards of safety, compliance, and operational excellence.



1 Introduction

In the early 2020s, artificial intelligence (AI) moved rapidly from a largely academic and specialist domain into mainstream adoption. While the foundations of AI date back to the mid-1950s, it is only in recent years (driven by significant advances in computing power, data availability, and algorithmic innovation) that AI has reached the maturity required for large-scale, practical deployment.

Today, AI is transforming industries worldwide, and the aviation sector is no exception. Within airport operations, AI is increasingly enabling new levels of efficiency, resilience, and insight. From predictive maintenance and resource optimisation to enhanced situational awareness on the airside, AI offers powerful tools to manage the complexity and dynamism of modern airport environments. When implemented effectively, these technologies can support better decision-making, improve operational performance, and strengthen safety outcomes.

This guidebook, commissioned in 2026 by the Technical, Operations & Safety Committee of the Airports Council International Europe (ACI EUROPE), has been developed to support airports in adopting AI solutions in a safe, responsible, and compliant manner. It is intended for safety, operations, and compliance practitioners, providing practical guidance on data validation, risk management, and maintaining the integrity and reliability of AI systems.

Given its origin within the Technical, Operations & Safety Committee, the guide focuses primarily on operational and airside applications, where AI can deliver tangible benefits while adhering to aviation safety requirements and regulatory frameworks. To support this objective, the guidebook includes:

- **An overview of relevant regulatory frameworks** (including ICAO, EASA, and the EU AI Act) and ACI World guidance on compliance
- **A summary of the key benefits** of AI for airport operations, safety, and efficiency
- **Step-by-step guidance** across the critical phases of an AI project, with a focus on safety and compliance at each stage
- **Practical use cases** demonstrating how to apply the guidance in real-world operational contexts
- **An overview of existing AI solutions**, both implemented and under development at various European airports.

While the primary scope of this guidebook is focused on operational and airside applications, many of the principles and considerations presented are broadly applicable to the wider use of AI across airport environments. These broader applications, however, encompass a diverse range of topics that warrant dedicated treatment and are therefore beyond the scope of this document.

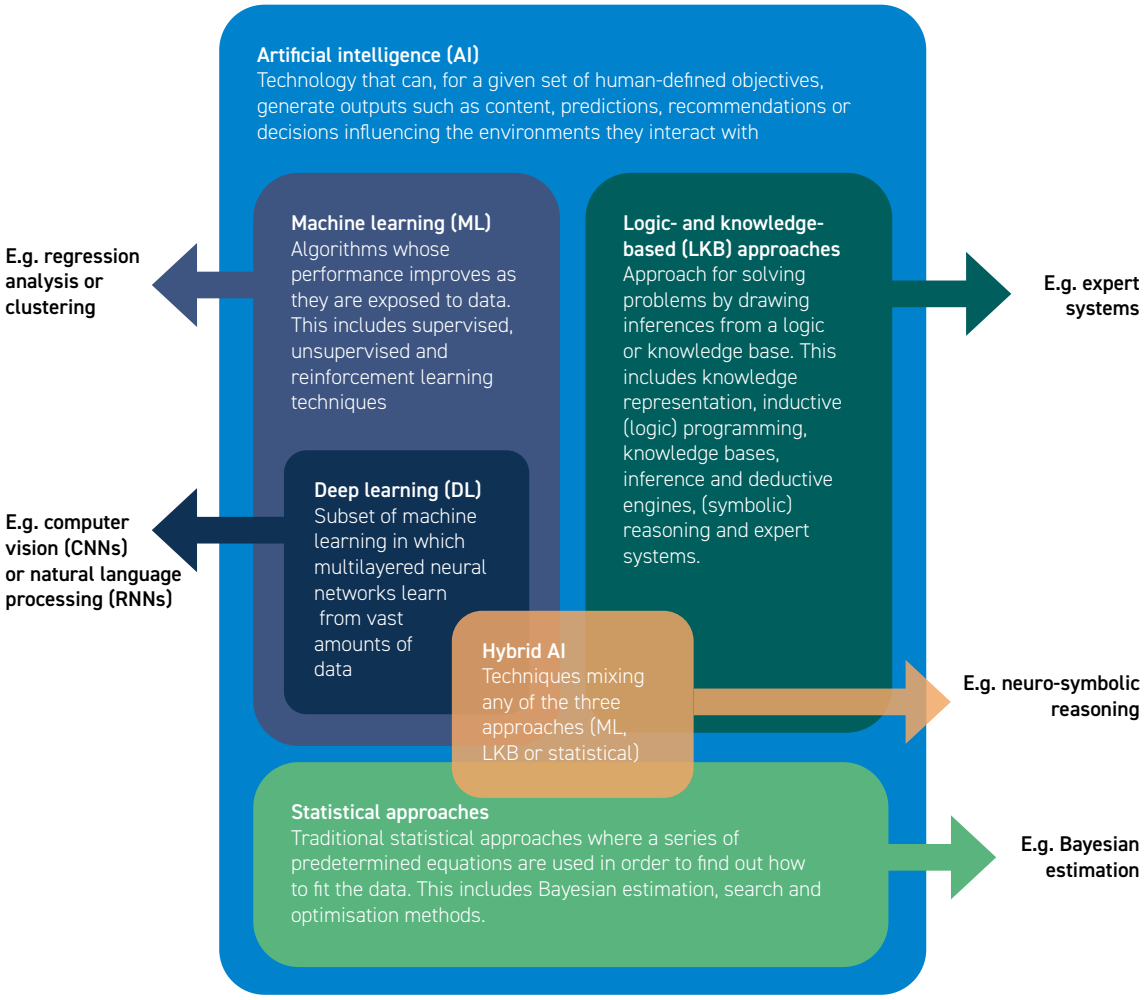
1.1 What is AI?

Artificial intelligence is a field of computer science that enables machines to perform tasks that would normally require human intelligence. This includes tasks such as:

- Recognising patterns in data (e.g., image recognition, anomaly detection)
- Making predictions based on historical data (e.g., predictive maintenance)
- Supporting decision-making through automated recommendations or optimisation
- Learning and adapting over time (e.g., machine learning models improving from experience)

AI is not a single technology but a set of methods and tools, including machine learning (ML), deep learning (DL), natural language processing (NLP), computer vision, and hybrid approaches combining rules-based logic with learning algorithms.

In aviation, AI is increasingly embedded in both operational systems and decision-support tools. Understanding AI's capabilities and limitations is critical for safe and compliant deployment.



Source: EASA AI Roadmap 2.0 (2023)

1.2 Why Preparing for AI is Critical

Airports must proactively prepare for AI adoption due to the fast pace of technological change and the evolving operational, regulatory, and societal environment. Key drivers include:

- **Rapid technology evolution:** AI capabilities advance faster than traditional operational or regulatory adaptation cycles
- **Changing nature of accidents:** New AI-enabled systems can introduce novel hazards that are not fully captured by historical data and ways of working
- **Reduced ability to learn from experience:** Increased speed of deployment and system complexity reduces the time available to detect and mitigate errors
- **Complexity and system coupling:** Integration of AI with multiple interdependent systems increases the likelihood of unintended interactions
- **Evolving human-AI relationships:** Humans increasingly interact with automation in decision-critical roles, requiring oversight and trust frameworks
- **Changing regulatory & public expectations**: European and international authorities, as well as passengers, expect transparency, accountability, and ethical use of AI

1.3 Scope and Audience

This guidebook is intended for airport professionals responsible for planning, implementing, or supervising AI-enabled operational systems, with particular focus on airside operations.

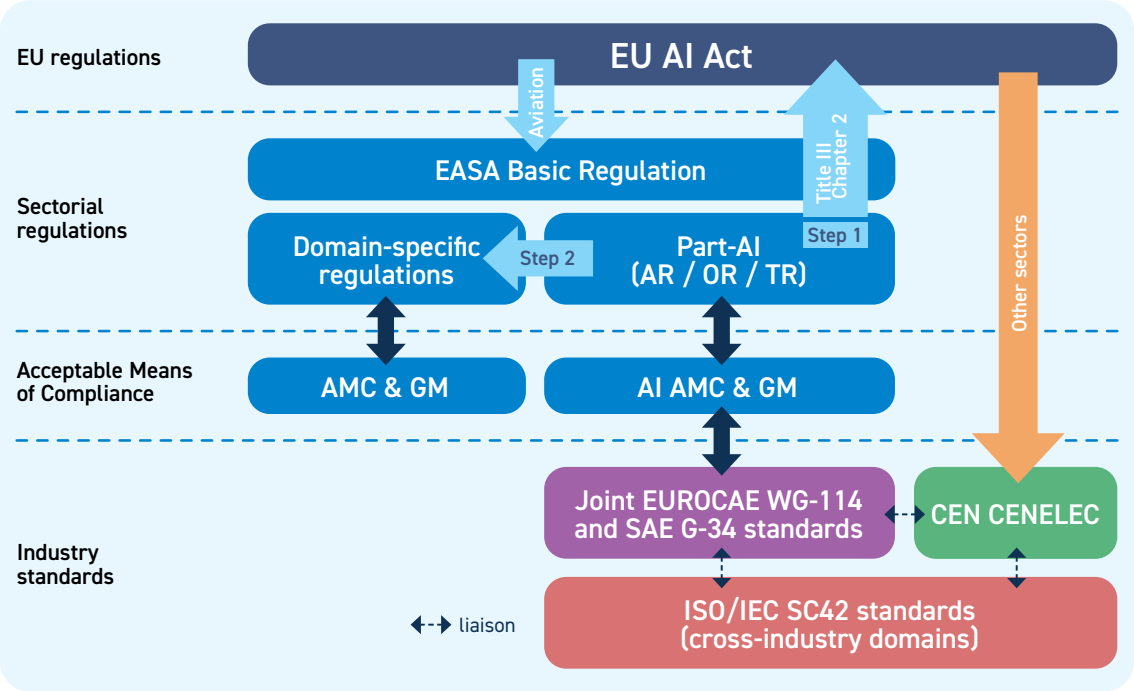
It is relevant to:

- **(Higher) management,** understanding the existing regulations and most important questions to address during an AI project
- **Operations teams**, integrating AI into daily processes such as stand allocation, aircraft turnaround, or resource optimisation
- **Safety and compliance officers**, ensuring that AI systems align with regulatory, data, and governance requirements
- **Procurement and IT teams**, evaluating AI solutions from suppliers and ensuring contractual, ethical, and compliance obligations are met

While the emphasis is on airside operations, the guidance can also be applied to other areas of the airport where data quality, accountability, and regulatory compliance are critical.

2 Alignment with existing Frameworks & Regulations

Implementing AI-based (particularly airside) solutions requires compliance with the key international and European regulations and frameworks. This section provides an overview of what should already be in place and how these frameworks guide safe and compliant AI adoption. The regulatory structure has been visualized by EASA in the following way:



Source: EASA AI Roadmap 2.0 (2023)

2.1 Overview of Aviation Compliance and Safety Regulations

While no AI-specific regulations for airports yet exist, several international and regional frameworks provide guidance:

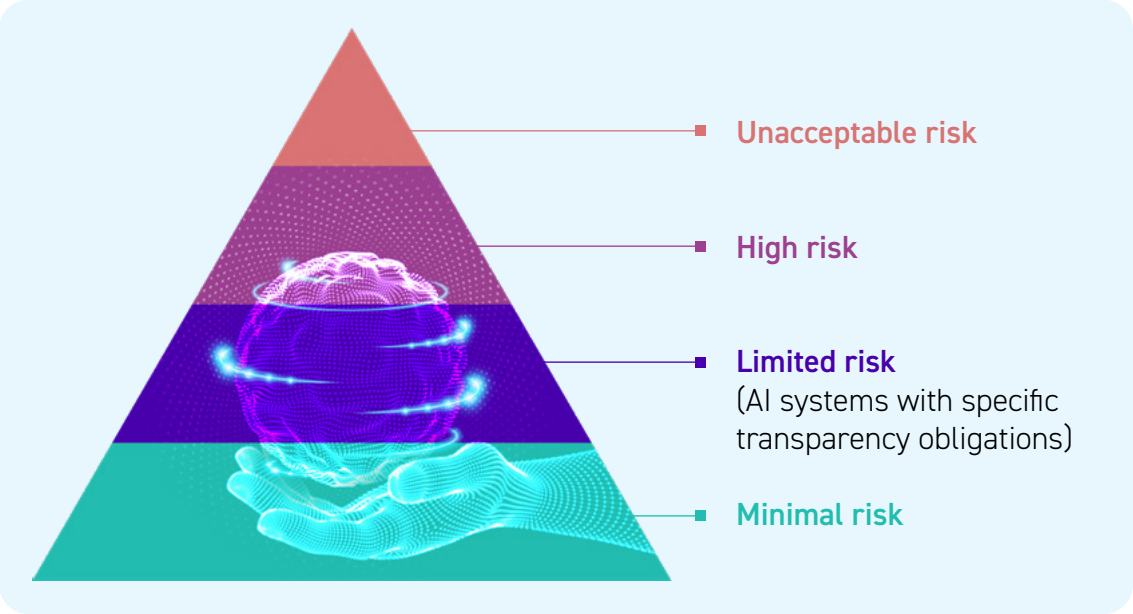
1. EU AI Act
2. EASA guidance
3. ICAO regulations
4. ACI World safety management framework

The sections below shortly outline what has been defined under these legislations to ensure the guidebook can be positioned correctly under the existing guidance.

2.1.1 EU AI Act

This act introduces a risk-based approach to classifying and regulating AI systems and is considered to be the most prominent and relevant regulation. The act bans certain practices and imposes strict obligations for high-risk AI systems.

The AI Act defines 4 levels of risk for AI systems:



European Commission. (n.d.). Regulatory framework on artificial intelligence. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

The model presents 4 categories of risks, which result in different acceptance levels.

- **Unacceptable risk:** AI systems that pose unacceptable risks are prohibited and may not be placed on the market or used.

- **High risk:** These systems can pose serious threats to safety or fundamental rights. Strict obligations must be met, including :
  - > Adequate risk assessment and mitigation systems
  - > Logging of activity to ensure traceability of results, appropriate human oversight measures
  - > Detailed documentation providing all information necessary on the system and its purpose for authorities to assess its compliance
  - > etc.

- **Limited risk:** This refers to the risks associated with a need for transparency around the use of AI. The AI Act introduced specific disclosure obligations to ensure that humans are informed when necessary to preserve trust (e.g. labelling of AI content)

- **Minimal or no risk:** The AI Act does not introduce rules for AI that is deemed minimal or no risk. The vast majority of AI systems currently used in the EU fall into this category (e.g. spam-filters)

Next to this, other obligations and enforcements include:

- **Transparency:** Many AI systems (including some non-high-risk ones) will require disclosure when users interact with AI, and stricter transparency for systems processing biometric or personal data

- **General-Purpose AI (GPAI) models:** Providers have additional obligations to produce technical documentation and to provide transparency info to downstream integrators

- **Market surveillance & enforcement:** National authorities and an EU-level AI Office will monitor compliance

- **Data Protection Laws (e.g., GDPR):** AI solutions handling passenger or operational data must ensure privacy and security

In this perspective, overall data governance frameworks are essential to avoid regulatory breaches and maintain trust.

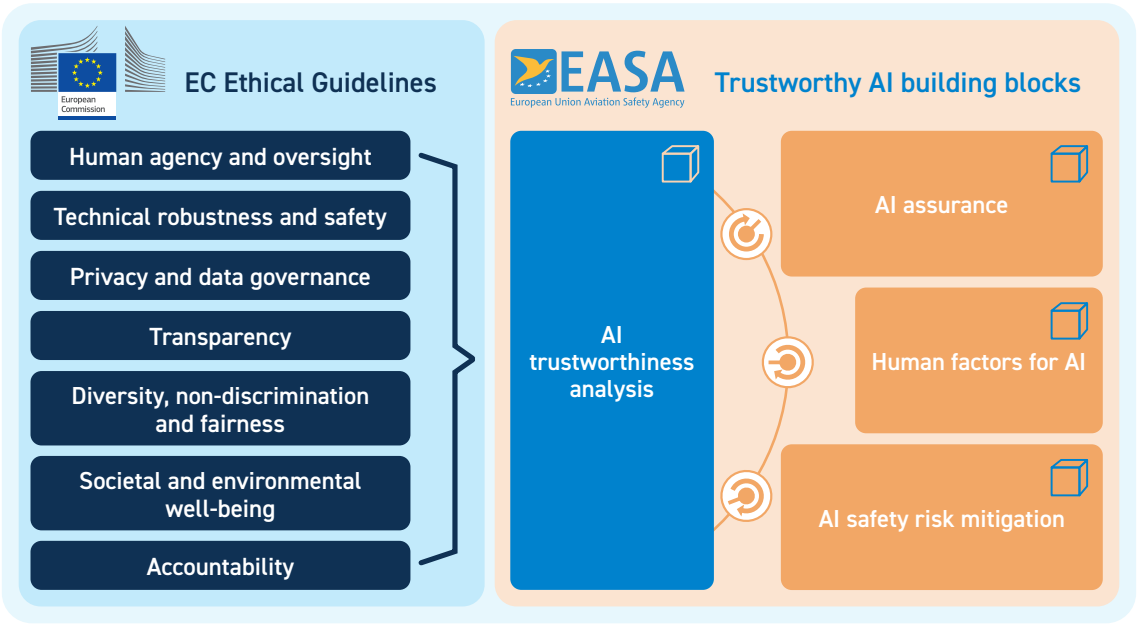
In particular, the AI Act clearly distinguishes between the obligations of providers (those developing or placing AI systems on the market) and deployers (those using AI systems under their authority), especially for high-risk AI systems. Providers are subject to a comprehensive set of obligations, including the establishment of risk management systems (Article 9), data and data governance requirements (Article 10), technical documentation (Article 11), record-keeping (Article 12), transparency and provision of information to deployers (Article 13), human oversight measures (Article 14), accuracy, robustness and cybersecurity requirements (Article 15), and conformity assessment procedures prior to market placement (Articles 43–49). The general obligations of providers are further set out in Article 16. Deployers, by contrast, are required to use AI systems in accordance with the provider's instructions, ensure appropriate human oversight, monitor system operation, retain logs where applicable, and report serious incidents, as specified in Article 26. While this review does not examine these provisions in detail, a stronger operational mapping of such role-specific obligations would help organisations translate the AI Act's legal requirements into concrete governance and compliance measures.

2.1.2 EASA

EASA identifies critical challenges and solutions for integrating AI into aviation safely, as outlined in its *Artificial Intelligence Roadmap 2.0* (EASA, 2023). The summary is included in the visual below.

Adapting Assurance Frameworks	Traditional assurance methods need updating to cover AI-specific aspects like performance metrics, data quality, and model architecture verification.
Knowledge and Data Management	Maintaining traceability between high-level requirements and training datasets is challenging. Ensuring data completeness, correctness, and clear definition of the operational design domain (ODD) is critical for safety.
Predictability and Explainability	AI outputs can be unpredictable due to model complexity. Improved methods for explainable AI are necessary for transparency and trust
Human-AI Teaming	Guidance is required for shared decision-making between humans and increasingly autonomous AI systems.
Stability and Robustness	AI models may behave inconsistently with small input variations. Formal verification methods are needed to ensure robustness and prevent unintended behavior.
Bias and Variance	Data and algorithms can introduce bias, affecting fairness and safety. Continuous monitoring and mitigation of bias across the AI lifecycle are essential.
Embedding AI Models	Challenges include preserving model integrity when transferring to aircraft hardware and qualifying new processors (e.g., AI accelerators).
Adaptive Learning	Real-time or self-updating AI models conflict with current certification rules. New regulatory frameworks are required before deployment in safety-critical systems.

To support this, EASA developed a trustworthiness framework. EASA defines four core building blocks for trustworthy AI, presented in the visual below.



High-level, the building blocks discuss the following:

1. **AI Trustworthiness Analysis:** Evaluates AI applications through safety, security, and ethics-based assessments

2. **AI Assurance:** Covers learning assurance and explainability to ensure AI reliability and traceability. This includes data recording and continuous monitoring for safety and incident analysis

3. **Human Factors for AI:** Integrates human factors into AI design, supporting operational explainability and Human-AI Teaming for effective collaboration

4. **AI Safety Risk Mitigation:** Addresses residual safety risks from AI "black boxes." Uses fail-safe designs, redundancy, and operational safeguards to manage uncertainty

Reference: European Union Aviation Safety Agency (EASA). (2023). Artificial Intelligence Roadmap 2.0. Cologne: EASA.

2.1.3 ICAO Regulations

Existing ICAO regulations can also be applied to the development and deployment of AI solutions.

Annex 19 – Safety Management: Establishes principles for managing operational risks, including hazard identification, safety risk management, safety assurance, and safety promotion. From Annex 19, key takeaway for AI is that AI-enabled processes must be integrated into existing hazard identification and risk management systems. Airports should monitor AI performance, assess risks, and ensure that AI applications comply with safety standards.

Content overview:

- **Safety Policy and Objectives:** Establishing clear safety goals aligned with organizational priorities
- **Safety Risk Management:** Implementing processes to identify and mitigate safety risks
- **Safety Assurance:** Regularly evaluating safety performance and implementing corrective actions
- **Safety Promotion:** Engaging staff and stakeholders in safety initiatives to promote a proactive safety culture

This framework is designed to help airports integrate safety management practices into their operations effectively. For more information, consult the ACI Safety Management Handbook: ACI SMS Handbook.

Reference: ICAO Annex 19 PDF

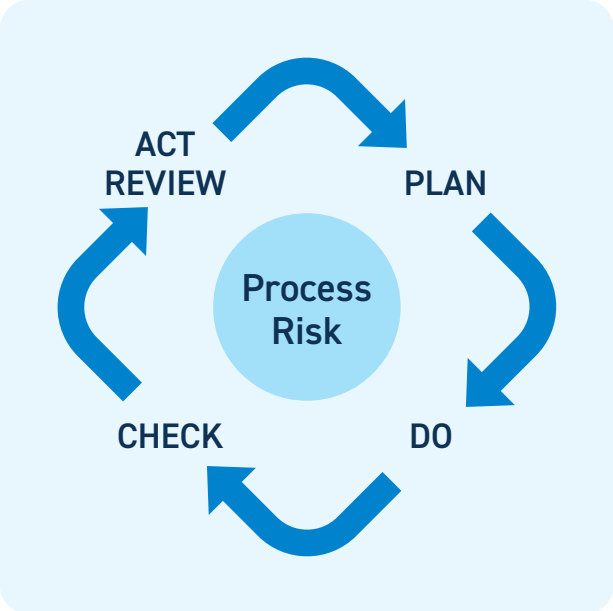
2.1.4 ACI World Safety Management Framework

The ACI World Safety Management Framework is closely aligned with ICAO Annex 19 and complements its principles by providing practical, airport-focused guidance. While the content is similar to ICAO Annex 19, the ACI World framework extends it by detailing how airports can implement safety management at the operational level and offers additional guidance on organizational responsibilities, monitoring, and continuous improvement.

In this framework, the key takeaway for AI is that AI adoption should follow the ACI framework to ensure operational integration is safe, effective, and compliant. **This means embedding AI within airport workflows, defining clear ownership of AI systems, and monitoring outputs to prevent risks from inaccurate predictions, biased data, or operational errors.** ACI guidance ensures that AI enhances operational safety rather than introducing uncontrolled risks.

Key elements:

- **Operational Focus:** Provides detailed recommendations on integrating safety management into daily airport operations, including airside activities, ground handling, and support services
- **Roles and Accountability:** Clarifies responsibilities for different airport teams (operations, airside management, technical services) to ensure governance of safety and AI-enabled processes
- **Continuous Improvement Guidance:** Offers practical methodologies for monitoring and evaluating safety performance, applying lessons learned, and implementing corrective actions
- **Integration with Innovation**: Emphasizes risk management for adopting new technologies, including AI, and encourages structured pilot testing, verification, and validation of systems before full deployment



Reference: ACI SMS Handbook

2.2 What does this mean for airports?

Below table gives a concise overview of regulatory requirements (derived from the EU AI Act, GDPR, ICAO/ACI principles and EASA guidance) and practical actions airports must take when implementing, procuring, or developing AI systems.

Requirement	What to Do
Risk classification	Classify each AI system as prohibited / high-risk / limited / minimal per AI Act. Do not deploy prohibited systems. Record applicability dates and Annex III mapping; register high-risk systems in the EU database.
Technical documentation & conformity	Obtain or produce technical documentation, test reports, and conformity evidence for high-risk systems. Maintain up-to-date model cards and third-party assessment records.
Risk management & safety case	Integrate AI into the airport Safety Management System: update hazard logs, perform safety assessments, implement mitigation controls, and define monitoring plans.
Data governance & GDPR compliance	Ensure lawful data processing, data minimisation, DPIAs, secure storage, and retention rules. For vendors, verify GDPR compliance and proper data agreements.
Human oversight & operational procedures	Define human-in-the-loop / human-on-the-loop controls, clear escalation paths, and accountability procedures. Ensure operational staff can intervene and override AI outputs.
Transparency & end-user information	Inform staff and passengers when AI is used (e.g., chatbots, analytics, biometric systems). For generative AI or GPAI, provide training-data summaries and user notices as required.
Testing & validation	Run pilots, acceptance tests, bias/performance evaluations. Use national AI sandboxes where available and document results as part of conformity evidence.
Monitoring & post-market surveillance	Implement continuous monitoring for drift, incidents, and performance. Prepare workflows for reporting incidents to national authorities and the EU AI Office. Maintain an evidence pack for audits.
Procurement & contractual clauses	Include AI Act compliance, audit rights, liability clauses, remediation timelines, and penalties for non-compliance in all contracts.
Market conformity & certification	For high-risk systems, ensure conformity assessments are completed before full deployment. Retain proof of certification and other evidence.
Special rules for biometric/visual systems	Avoid prohibited facial recognition uses. Obtain regulatory approvals for lawful exceptions and implement strict safeguards. Embed privacy-by-design principles.
GPAI / large model obligations	Require transparency documents from providers, assess model provenance and risks, and maintain traceability for downstream use.
Penalties & remediation planning	Maintain a remediation plan, including rollback procedures and update workflows in case of non-compliance or enforcement action.
Compliance timeline & transitional measures	Check applicability of rules and deadlines for each system. Gate pilots, deployment, and conformity activities according to the AI Act's staged timelines (prohibition active Feb 2025, high-risk full compliance within 36 months).

3 Opportunities and benefits translated into a business case

Artificial Intelligence is increasingly applied across airport operations, enabling smarter decision-making, predictive insights, and operational efficiencies. From airside safety monitoring to resource allocation and predictive maintenance, AI offers both qualitative and quantitative benefits. This section presents the main benefits of AI, outlines frameworks for identifying and evaluating AI use cases, and provides guidance on building a business case.

3.1 Qualitative Benefits

AI can provide several non-monetary benefits that enhance operational quality and strategic decision-making:

Enhanced Safety	Improved Passenger Experience	Proactive Decision-Making	Sustainability & Environmental Benefits
AI enables real-time detection of hazards, such as runway incursions or equipment anomalies, complementing human oversight.	Streamlined operations: faster check-in, boarding, and baggage handling, etc. enhance satisfaction.	Decision-support systems integrate weather, traffic, and operational data to anticipate issues and guide resource allocation.	AI supports energy optimization, emission reduction, and environmental monitoring.
Operational resilience	**Computer Vision for Safety**	**Decision Support Tools**	**Other**
AI allows airports to respond dynamically to disruptions, reducing dependency on reactive measures.	Automated FOD detection, intrusion detection, and apron monitoring improve airside safety while reducing manual inspection effort.	AI systems consolidate multiple data sources for situational awareness, enabling more informed and timely operational decisions	The final chapter outlining use cases, as well as the future, will present numerous other benefits

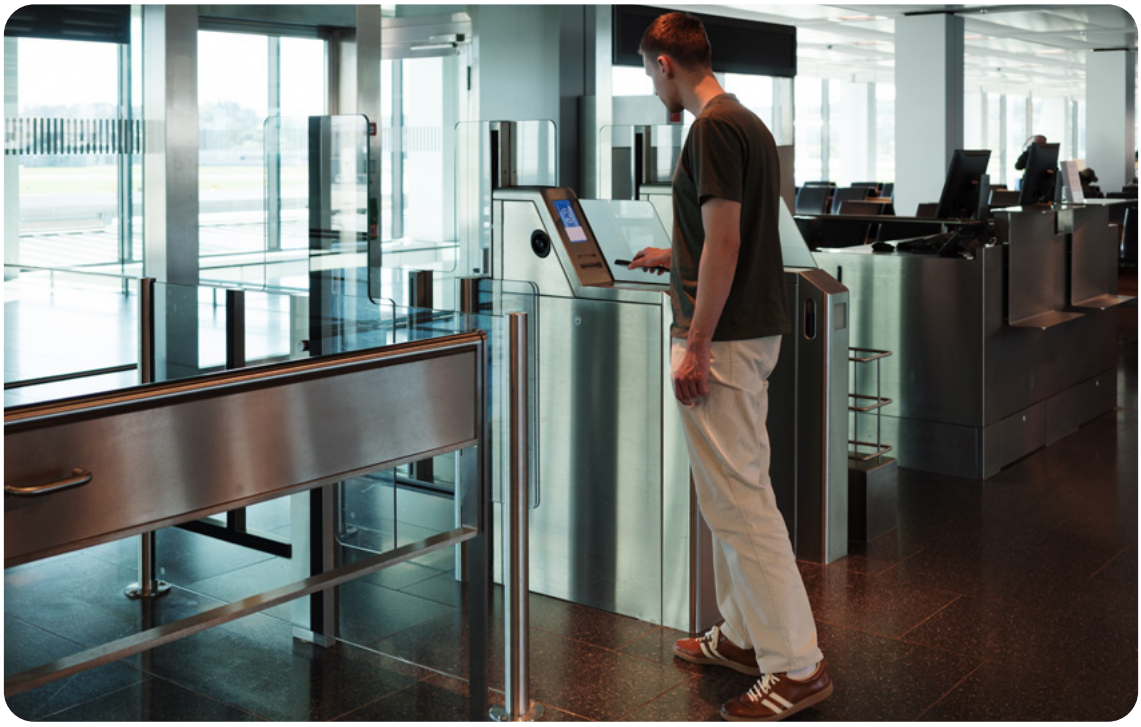
3.2 Quantitative Benefits

Moreover, these technologies can provide measurable improvements across airport operations. These benefits can be quantified in reduced costs, increased throughput, and more reliable operations. The following benefits have been quantified:

Benefit Area	Description	Impact / Metric
Predictive Maintenance	Forecast equipment failures before they occur	10–30% reduction in maintenance costs and downtime
Reduced downtime	Reduced unscheduled aircraft downtime	25% downtime reduction, ~$50M annual savings
Industry-wide Maintenance	Improved equipment effectiveness and reduced downtime	15–25% ↑ effectiveness; 20–50% ↓ unplanned downtime; 25% ↓ maintenance costs
Operational Efficiency	Optimized allocation of gates, stands, and staff	10–15% increase in throughput
Flight Punctuality & Delay Forecasting	AI-driven forecasting of weather, congestion, and disruptions	Saved 160,000 minutes of delays - rerouting program: 243,000 minutes saved
Energy Management	Optimized energy consumption in terminal and airside operations	5–10% reduction in energy costs

In summary, these quantified results clearly illustrate the value of AI deployment, providing strong evidence for investment in these technologies. As adoption grows, further studies are expected to produce even more precise, data-driven metrics of AI's impact on airport efficiency and performance.

The authors are not responsible for the achievement of these exact numbers. The numbers stem from industry research building on estimations as airports are complex ecosystems where a multitude of other factors are evolving at the same time.



3.3 Template for Identifying AI Use Cases

Given the wide range of potential benefits from AI, it can be challenging for airports to prioritize initiatives effectively. It is recommended to start with smaller projects that offer clear, tangible benefits, allowing teams to gain experience and demonstrate value before scaling up. A structured approach can help identify and assess AI opportunities systematically, enabling prioritization based on domain impact, operational difficulty, and expected improvement in key performance indicators (KPIs). This ensures that efforts are focused on areas where AI can deliver the greatest value.

Steps to identify AI use cases:

1. Identify the problem or opportunity by clearly stating what needs to be solved and why it is relevant. Identify the potential AI solution

2. Assess potential safety, compliance, and efficiency benefits by evaluating how the AI solution could improve operational performance, reduce errors, support regulatory compliance, enhance decision-making, and increase productivity.

3. Identify key risks and mitigation strategies by analysing potential legal, ethical, operational, security, and reliability risks, and defining appropriate controls, oversight measures, and safeguards.

4. Determine data sources and quality requirements by identifying required internal and external data sources, assessing data availability and suitability, and defining standards for accuracy, completeness, and governance.

After this, building a robust business case is critical for stakeholder buy-in. A comprehensive business case should include both quantitative and qualitative benefits, risk assessment, and operational impact.

Steps to prepare a business case:

1. Define objectives and scope of the AI project

2. Quantify expected cost savings, efficiency gains, and performance improvements

3. Assess qualitative benefits (safety, passenger experience, sustainability)

4. Investigate readiness for solution (data availability and quality). Evaluate how easily the solution can be developed and implemented

5. Identify risks, mitigation strategies, and regulatory considerations

6. Estimate investment, operational costs, and required resources

7. Define a monitoring and evaluation plan

Combining both steps leads to the following template per AI use case:

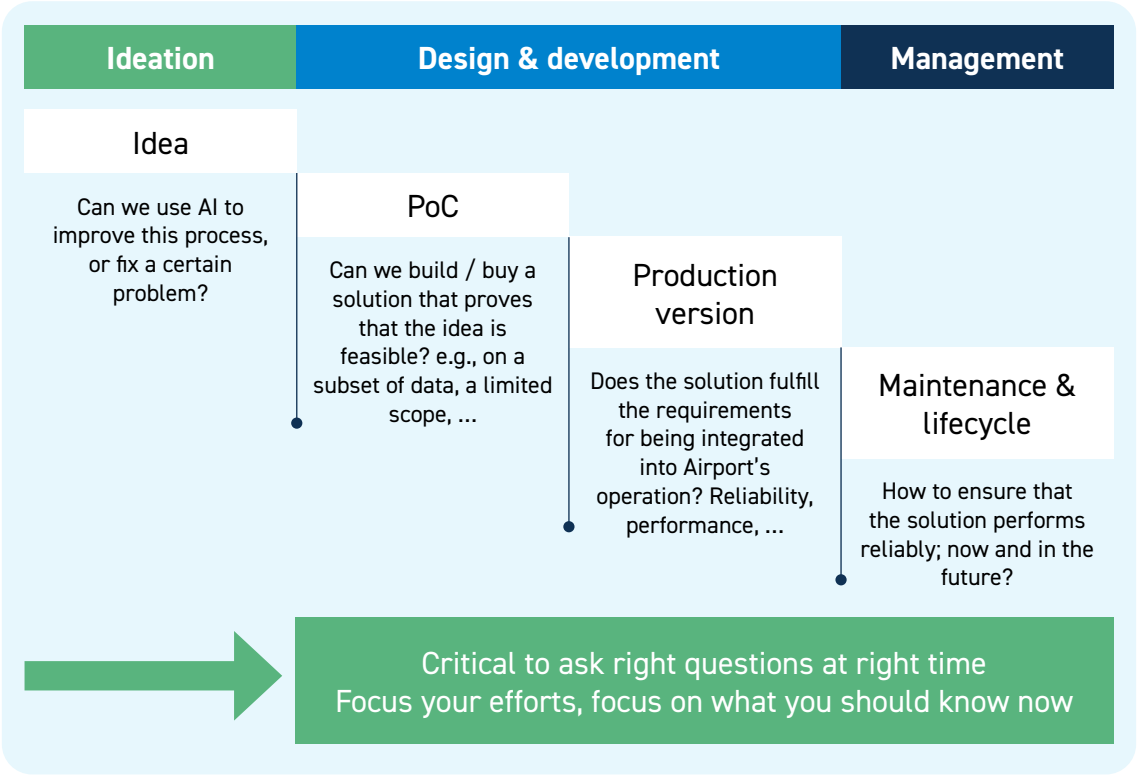
Category	Details
Problem	Operational challenge addressed
AI Solution	Predictive / Computer Vision / Optimization / Decision Support
Safety or Compliance Benefit	How the solution improves safety or regulatory compliance
Key Risks	Potential operational, safety, or data-related risks
Data Source / readiness	Primary data inputs and quality requirements
Investment Cost	Capital expenditure, technology costs, implementation fees
Operational Cost	Maintenance, staff training, support
Quantitative Benefits	Cost savings, efficiency improvements, delay reduction
Qualitative Benefits	Safety, compliance, passenger satisfaction, sustainability
Key Risks	Technical, operational, compliance risks
Net Present Value / ROI	Placeholder for financial assessment
Implementation Timeline	Planned start and end dates

4 AI solution implementation in the airport environment

AI solutions follow a defined implementation lifecycle that is common across most software products. The following sections address the critical questions and attention points that must be resolved at each phase of this cycle.

4.1 The relevant project phases of an AI solution

Below figure illustrates the different and typical project phases for the implementation of an AI solution.



Ideation

The ideation phase centres around identifying opportunities where AI could add value. This could be by optimizing an existing process, solving a persistent problem, or enabling entirely new capabilities. At this stage, the focus is on generating and evaluating ideas. The involvement of technical staff / tech translators is encouraged to already have a rough alignment with the current state-of-the-art of AI, which moves fast certainly in the field of LLMs due to the strong competition between foundational model providers. During this phase, the initial formulation of the business case also begins to take shape by capturing expected value, scope, and high-level feasibility ahead of the structured business case developed later. Additionally, candidate ideas should be screened against early regulatory, compliance, and data protection checkpoints.

Proof of Concept (PoC)

The POC phase tests whether a proposed AI solution is technically viable. Working with a subset of data or a limited operational scope, the objective is to demonstrate that the core concept functions as intended before committing to full-scale development. Beyond technical validation, the PoC should also assess operational readiness to confirm the solution is not only technically viable but also organisationally feasible. This should include human adoption, procedural integration, change management, and an initial risk assessment

Production Version

This phase addresses the transition from prototype to operational deployment. The central question is whether the solution meets the reliability, performance, and integration requirements necessary for incorporation into live airport operations.

Maintenance

Once deployed, attention shifts to long-term sustainability. This phase focuses on ensuring continued performance, including continuous monitoring of data quality and model behaviour, managing updates and model drift, and planning for eventual replacement or decommissioning.

4.2 Relevant core dimension for evaluating an AI solution

To give clearer guidance on the implementation evaluation of an AI project, the AI solution is evaluated on different dimension that each cover a different aspect of the AI solution. These different dimensions are presented in the illustration below.

Category
Business Value
Feasibility
Data
Technology
Security - IT
Safety - Ops
Compliance
Workforce & Organisation

Business Value

This dimension assesses whether the proposed AI solution addresses a genuine operational need and delivers measurable benefits, as referred to above in the business case. Considerations include the clarity of the problem being solved, the expected return on investment, alignment with strategic priorities. A clearly articulated business case ensures that the AI solution really delivers value and does not just sound fancy on paper (avoid AI washing).

Feasibility

Feasibility examines whether the AI solution can realistically be developed, deployed, and sustained within the airport's operational context. This includes evaluating technical complexity, resource availability, timeline constraints, and organisational readiness.

Data

AI systems are fundamentally dependent on data quality, availability, and governance. This dimension addresses whether the necessary data exists, whether it can be accessed and integrated, and whether it meets the quality standards required for reliable model performance.

Technology

This dimension focuses on the technical approach and components required to deliver the AI solution. Key considerations include the type and maturity of the technology, the choice between off-the-shelf and custom-built solutions, and compatibility with existing systems. Performance requirements—accuracy, speed, reliability—must be defined, along with explainability needs where the solution supports human decision-making.

Security – IT

IT security assesses the cybersecurity implications of the AI solution. This includes evaluating vulnerabilities, access controls, data protection measures, and compliance with the organisation's IT security policies. Given the critical nature of airport infrastructure, robust protection against cyber threats is essential.

Safety - Ops

Operational safety addresses the physical and procedural safety implications of deploying AI within the airside environment. This includes assessing how the solution interacts with safety-critical processes, whether it introduces new risks to operations, and how it aligns with existing safety protocols.

Compliance

Compliance ensures that the AI solution adheres to all applicable aviation regulations, data protection laws, and internal governance standards. This dimension covers regulatory approval requirements, audit and documentation obligations, and alignment with frameworks such as the EU AI Act where applicable.

Workforce & Organisation

This dimension addresses the human impact of AI deployment. Considerations include effects on existing roles, potential workforce displacement or augmentation, and requirements for reskilling. Change management, stakeholder acceptance, and clear accountability structures are also evaluated. Transparency regarding AI's role is essential for maintaining trust and ensuring smooth adoption.

4.3 Key considerations per key project phase

Below illustration now translates how the relevant dimensions against which AI initiatives should be evaluated can be applied at each lifecycle phase.

Category	Idea	Analysis / PoC	Production	Maintenance & Lifecycle
Business Value	Identify expected benefits, costs, and scope.	Estimate development costs, market comparison, validate assumptions.	Track actual vs projected benefits and efficiency metrics.	Assess ongoing business value and ROI.
Feasibility	Define technical/ organizational approach; risk assessment.	Define success criteria. Check market solutions, internal capabilities.		
Data	Identify stakeholders, availability, and collection needs.	Evaluate quality, reliability, edge cases.	Ensure data quality and availability.	Implement governance, monitor drift, plan fallback.
Technology	Determine required technology, maturity, off-the-shelf vs custom.	Define performance requirements and final tech stack.	Performance monitoring	Control performance, handle model updates and retraining.
Security - IT	Identify critical constraints (e.g., cybersecurity, biometrics).	Engage security stakeholders, assess risks.	Manage dependencies and third-party integrations.	Monitor ongoing security.
Safety - Ops	Assess operational safety implications.	Confirm solution meets safety/security requirements.	Plan safe rollout, replacement, or upgrades.	Monitor operational compliance.
Compliance	Identify applicable frameworks and limitations.	Check approvals and regulatory alignment.	Ensure compliance in production (AI Act, GDPR, local laws).	Track evolving regulations and maintain compliance.
Workforce & Organisation	Assess impact on existing roles. Identify change management and training needs.	Involve end users. Gather feedback on usability and integration in existing workflows.	Deliver training on system use and appropriate reliance	Monitor adoption patterns. Support role evolution and workforce transitions.

For each dimension, organisations should establish clear continuation criteria, i.e., conditions that must be met to proceed to the next phase, as well as stop criteria that trigger project reassessment or termination. Not all dimensions carry equal weight at every phase, guidance on prioritisation is provided where relevant.

Note that while presented separately, these dimensions are inherently interdependent: compliance requirements constrain technology choices, data availability determines feasibility, and workforce considerations shape the achievable business value.

Business Value

During ideation, the expected benefits of the AI solution must be clearly articulated and estimated. It must be defined whether the objective is to optimise operations, reduce costs or risks, or increase revenues and capabilities. Companies should further aim to put the expected business value in relation with the estimated costs. The anticipated costs need to be considered for the full lifecycle, including initial investment, ongoing operational expenditure, and workforce-related costs such as training and change management. Market research should inform realistic pricing expectations. For external solutions, vendor pricing models should be scrutinised for long-term implications, including dependency risks and exit costs.

The PoC phase serves as a critical validation point: business stakeholders must assess whether initial assumptions regarding benefits and costs hold when confronted with real-world conditions. Stop criteria at this stage include fundamental misalignment between projected and observed value, or discovery of costs that invalidate the business case.

Upon deployment, production tracking compares actual versus projected benefits and establishes cost-per-unit metrics (per flight, passenger, bag processed, ...). Sustained operations require periodic reassessment of generated business value, ensuring the solution continues to justify its investment as conditions evolve.

Feasibility

Initial feasibility assessment addresses both technical and organisational dimensions. The key technical question is whether the technical solutions can fulfill the business requirements. This also critically depends on the type of change: replication of an existing solution, application of proven technology to a new context, or a genuinely novel development. All these different types of processes carry different risks. Feasibility is also tightly coupled with data availability: a sound approach becomes infeasible if required data cannot be obtained or legally used.

Organisational feasibility examines whether the envisioned solution is operation critical or rather represents an enhancement, with the former requiring more rigorous change management. Stakeholder alignment must be evaluated early: are all required parties engaged, and are their objectives compatible? Misaligned incentives between operational, IT, and business stakeholders represent a common source of project failure. For external solutions, feasibility assessment should include evaluation of vendor stability, contractual flexibility, and exit strategies.

The PoC requires clearly defined success criteria established prior to development. Stop criteria include inability to secure necessary stakeholder commitment, discovery of insurmountable barriers, or confirmation that required capabilities exceed organisational capacity.

Data

Data considerations begin with stakeholder identification: who owns, maintains, and governs the relevant data assets? Early assessment determines whether required data exists, is actively used, and can be obtained within reasonable timelines. Data availability directly constrains feasibility; the most elegant solution delivers no value if it cannot access the data it requires. Historical data should be evaluated for coverage of unusual situations, e.g., major weather events, strikes, system outages, as those need special attention when used as training data.

During the PoC, minimum data requirements for achieving reliable results must be validated. If data does not comply with these minimum requirements this presents a **stop criteria** for the project.

Any production deployment of an AI solution demands robust data governance ensuring data availability and data quality. Long-term operations must monitor for data drift (gradual changes that degrade performance) and establish fallback procedures for situations when data sources become unavailable. The absence of viable fallback mechanisms for critical applications should be treated as a blocking issue.

Technology

The starting point is understanding what type of technology the problem requires and how mature that technology is. Can established approaches deliver, or are novel components central to the solution? This assessment informs one of the most consequential early decisions: off-the-shelf procurement versus in-house development. The choice shapes cost, customisation potential, and long-term sustainability. It should also be informed by compliance considerations—solutions offering architectural transparency may simplify regulatory obligations.

During ideation, performance requirements must be defined in measurable terms. What accuracy, speed, or reliability thresholds must the solution meet? Where it supports human decision-making, explainability requirements should be specified. These requirements determine which technologies are worth testing in the PoC.

The PoC validates whether the selected technology is fit for purpose. Clear success criteria must be established beforehand: what benchmarks must be met to proceed, and at what point should the organisation conclude that the technology cannot deliver? Dependent on the project type this metrics might evolve during the PoC phase based on new insights and stakeholder feedback.

In production, performance is monitored against these benchmarks, with defined thresholds triggering intervention. Human oversight mechanisms should be integrated where required, with clear escalation paths when systems produce unexpected outputs.

Sustained operations must address performance degradation over time. Maintenance and update strategies—including retraining frequency where applicable—should be defined upfront. For vendor solutions, contractual provisions should cover updates, compatibility, and data portability to mitigate lock-in risks.

Security – IT

Critical IT security constraints must be identified during ideation, particularly for use cases involving sensitive data. Biometric identification, for example, requires cybersecurity considerations integrated from initial design. Security requirements may fundamentally also constrain technology choices and data handling approaches; these should be surfaced early through engagement with security stakeholders. Stop criteria include identification of security risks that cannot be adequately mitigated or that conflict with organisational policies.

Production deployment must address management of external dependencies, including third-party provider security standards and access controls. For cloud-based or vendor-hosted solutions, security responsibilities must be clearly indicated.

Integration with existing security management systems ensures AI solutions do not create blind spots. Ongoing operations require continuous security monitoring and incident response procedures. In particular, autonomous systems enabled by AI need to be monitored with utmost care.

Safety – Ops

Operational safety implications vary substantially by use case. Solutions operating in safety-critical contexts, e.g., foreign object detection on runways, carry fundamentally different risk profiles than administrative AI tools. This distinction must be established during ideation, as it determines the rigour of subsequent validation and the level of human oversight necessary.

For safety-critical applications, risk assessment must be carried out meticulously, failure scenarios and their consequences must be considered, and mitigation strategies put in place. The interaction between AI outputs and human decision-making must be designed to avoid both over-reliance on automated recommendations and unnecessary friction that undermines adoption. **Stop criteria** include inability to demonstrate acceptable safety margins or failure to secure endorsement from relevant safety functions.

Production planning addresses safe rollout strategies. Introducing a new system requires different approaches than replacing an existing one, with the latter demanding careful transition management. Parallel operation periods, phased rollouts, and defined rollback procedures provide risk mitigation during deployment. Changes to production systems should follow defined protocols with appropriate approval gates.

Compliance

Applicable compliance frameworks must be identified at the onset. These include legal requirements (GDPR, the EU AI Act, local aviation regulations) as well as standards such as ISO 42001 for AI management systems. Compliance requirements interact with multiple other dimensions: they may constrain technology choices, mandate specific approaches to human oversight, and require particular data handling practices.

The EU AI Act introduces risk-based classification with corresponding obligations. Solutions deployed in airport operational contexts may fall into higher risk categories, triggering requirements for conformity assessment, human oversight, transparency,

and documentation. These obligations should be understood during ideation, as they influence architecture decisions and resource planning. **Stop criteria** include confirmation that the proposed approach cannot satisfy mandatory requirements or that the cost of compliance invalidates the business case.

Production deployment must demonstrate ongoing compliance through audit trails and monitoring. Explainability requirements, where applicable, must be operationalised: how will affected individuals or oversight bodies receive meaningful information about AI-driven decisions?

Long-term operations require tracking evolving regulatory requirements, particularly given the phased implementation of the AI Act. Compliance should be treated as a continuous operational requirement. Responsibilities for regulatory monitoring should be assigned, and processes established for assessing implications of regulatory changes.

Workforce & Organisation

This dimension addresses the human and organisational implications of AI deployment. During ideation, the potential impact on existing roles must be assessed: will the solution replace, augment, or reshape human tasks? Transparency with affected employees regarding AI's intended role is essential for maintaining trust. Workforce implications directly affect achievable business value—resistance, skill gaps, or unclear accountability can undermine even successful deployments. Change management requirements should be identified, including communication strategies, training needs, and revised role definitions. Stop criteria include inability to secure workforce cooperation or identification of impacts that conflict with organisational values or labour obligations.

The PoC phase offers an opportunity to involve end users, gathering feedback on usability and practical integration with existing workflows. Resistance patterns identified during PoC should be addressed before production deployment.

Production deployment requires clear accountability structures: who is responsible when AI-supported decisions produce adverse outcomes? The boundary between human and machine responsibility must be explicitly defined, particularly for decisions with significant operational or safety implications. Training should address not only system operation but also appropriate reliance—helping users understand when to trust AI outputs and when to apply additional scrutiny.

Sustained operations require ongoing attention to workforce dynamics. As users gain experience, interaction patterns may shift; monitoring should detect both over-reliance and under-utilisation. Role evolution should be managed deliberately, with affected employees supported through transitions.

4.4 Key risks and attention points

Successful AI implementation requires awareness of the risks that can derail initiatives at each phase. The following summarises the most critical risk factors across the evaluation dimensions introduced earlier.

Business Value

A common failure pattern is technology-first thinking; pursuing AI capabilities without a clear business anchor. When initiatives start as technology experiments rather than responses to defined operational needs, they risk becoming solutions in search of problems. Many projects remain stuck in pilot phases, demonstrating promising results in controlled conditions but never transitioning to production deployment. Measurement challenges compound this issue: traditional ROI frameworks often fail to capture AI's value, leading to premature abandonment or continued investment without evidence of return.

Feasibility

AI projects carry inherent uncertainty about whether a solution can deliver at all for a given use case, a characteristic that distinguishes them from conventional IT implementations. Stakeholder alignment presents particular challenges when multiple parties with differing objectives, authority levels, and risk tolerances must coordinate. Cross-functional misalignment between technical teams and business units frequently undermines otherwise sound initiatives.

Data

Poor data quality remains the primary technical cause of AI project failure. Models trained on incomplete, biased, or unrepresentative data will underperform in production regardless of algorithmic sophistication. Edge case coverage deserves particular attention in airport contexts: models that have not encountered major disruptions (severe weather, strikes, system outages) and common operational irregularities (e.g. public holidays, seasonal traffic patterns or staffing variations) during training may fail unpredictably when such events occur.

Technology

A critical distinction exists between static models trained offline and adaptive models that continue learning during operation, each require different oversight approaches. Non-deterministic behaviour, where systems may not reproduce identical outputs for identical inputs, challenges traditional verification methods.

Security – IT

Airports represent high-value targets for malicious actors, and AI systems introduce new attack vectors. Supply chain vulnerabilities are particularly acute: airports depend on numerous third-party suppliers, and a compromise in shared systems can cascade across interconnected networks. Legacy infrastructure, often lacking modern security features and no longer receiving vendor support, expands the attack surface when integrated with AI capabilities.

Safety – Ops

Over-reliance on automation represents a significant operational risk. When operators trust AI outputs without appropriate scrutiny, or when system design impedes timely human override, minor anomalies can escalate into serious incidents. Skill degradation may occur when personnel disengage from tasks handled by AI, reducing their capacity to intervene effectively when required. The design of human-AI interaction must balance efficiency gains against the need for maintained situational awareness and intervention capability.

Compliance

AI systems operating as safety components in airport contexts will likely be classified as high-risk under the EU AI Act, triggering substantial obligations including conformity assessment, technical documentation, quality management systems, and human oversight requirements. These obligations apply throughout the system lifecycle, not merely at deployment. The regulatory landscape continues to evolve, requiring ongoing monitoring and adaptation.

Workforce & Organisation

Employee resistance to AI adoption is widespread, driven primarily by concerns about job displacement and distrust of AI decision-making. Change initiatives frequently fail due to insufficient attention to these human factors. However, research increasingly suggests that leadership, not workforce readiness, constitutes the primary barrier to successful adoption. Clear communication, meaningful involvement in pilot programmes, and robust training addressing both system operation and appropriate reliance are essential for building acceptance and competence.

5 Practical guidance on AI in an airport context

This chapter aims to address the most relevant practical issues that come up when building AI applications.

5.1 How to govern data source and ensure high quality of data?

When building AI applications, usually data is the underlying fuel that powers the engine. Hence the first step for building an AI project is to install data governance and ensure data quality.

5.1.1 Data governance

Data governance establishes the policies, procedures, and accountabilities that ensure data is managed as a strategic asset. For AI applications in airport environments, this is particularly critical given the operational sensitivity and regulatory scrutiny involved.

Ownership & Accountability

- Who is responsible for each data source? Every dataset (feeding an AI system) at a company should have a clearly designated data owner with authority to make decisions about access, quality standards, and usage permissions.
- How are responsibilities and standards documented and communicated across departments?
- What escalation paths exist when data issues arise?

Governance Framework

- What solution does the organisation use to govern its data sources? This might include data catalogues, metadata management platforms, or integrated data governance tools.
- Are data definitions standardised across the organisation? Inconsistent definitions (e.g., what constitutes a "delayed flight") can undermine AI model accuracy.
- How is data lineage tracked? Understanding where data originates and how it transforms is essential for debugging AI outputs and demonstrating regulatory compliance.
- How is integration of 3rd party data into the airport data ecosystem governed? What SLAs and policies are in place?

Monitoring & Oversight

- What monitoring is in place to detect unauthorised access, data breaches, or policy violations?
- How frequently are governance policies reviewed and updated?
- Are there automated alerts for governance exceptions?

5.1.2 Data quality

Data quality is an important pillar of data governance and directly determines AI system performance. Models trained on incomplete, biased, or erroneous data will produce unreliable outputs regardless of algorithmic sophistication.

Dimension	Definition	Airport Example
Completeness	All required data fields are populated	Passenger flow sensors reporting continuously without gaps
Accuracy	Data correctly represents the real-world entity	Flight times matching actual gate arrivals within tolerance
Consistency	Data values align across different systems	Same flight showing identical status in AODB and passenger displays
Timeliness	Data is available when needed	Real-time baggage tracking updates within acceptable latency
Validity	Data conforms to defined formats and ranges	Temperature readings within physically plausible bounds

Quality Control Mechanisms

Data quality must be actively controlled through clear metrics and thresholds covering completeness, accuracy, consistency, timeliness, and validity. Also note that these metrics are to be set for each project and data source individually as trade-offs might be required (e.g., accuracy vs. timeliness).

Validation rules should be applied at data ingestion points to catch issues early. When quality problems occur, there must be established processes for identifying, logging, and remediating them. Ongoing monitoring ensures sustained visibility, with clearly assigned responsibility for quality oversight.

Key Takeaways

1. **Data governance precedes technology:** No AI tool can compensate for unclear data ownership or inconsistent policies.

2. **Quality is measurable:** Define specific, quantifiable metrics for each quality dimension relevant to your AI use cases.

3. **Accountability matters:** Every data source needs an owner empowered to maintain standards and resolve issues.

4. **Monitor continuously:** Point-in-time quality checks are insufficient; AI applications require ongoing data surveillance, ideally supported by automated (AI-based) data quality monitoring to detect anomalies, drift, gaps and inconsistencies early.

5. **Plan for AI-generated data:** As AI systems produce outputs that enter your data ecosystem, extend governance and quality controls accordingly.

5.2 How to ensure data quality when data is created by AI systems?

AI applications introduce a unique challenge: model outputs may themselves become inputs to other systems or future training data. This creates potential feedback loops where errors compound over time.

Safeguards to implement:

- Separate quality controls for human-generated vs. AI-generated data
- Clear labelling of AI-derived data in downstream systems
- Periodic revalidation of models against fresh, independently verified data

5.3 How to decide between building, buying, or hybrid approaches?

The decision on how to source AI technology is one of the most consequential choices in any implementation. It involves three interconnected considerations: the nature of the technology (off-the-shelf vs. custom), who delivers it (internal vs. external), and how these can be combined.

Technology Type

	Off-the-Shelf	Custom
PRO	Pre-built solutions designed for common use cases	Purpose-built solutions tailored to specific requirements
	Faster deployment, proven track record	Full control over features and evolution
CON	Limited customization, vendor roadmap dependency	Longer development, unproven until tested
	Lower initial investment, licensing cost that might increase	Higher upfront investment, variable development costs

Delivery Model

Internal Development	External Purchase/Contract
Requires in-house AI/ML expertise and dev software	Leverages vendor or contractor capabilities
Full control over priorities and timelines	Dependent on external delivery schedules
Institutional knowledge retained	Knowledge may reside with third party
Ongoing staffing and skills investment	Contractual relationship management

Hybrid Combinations

In practice, most successful implementations combine elements. It is to be noted though that inherently any modern software / AI project is built using external packages, and the difference between an "internal development" and a hybrid model is often just the licensing of the 3rd party software packages.

- Vendor solution + Internal integration:
  - > Buy the AI component, build the airport-specific integration layer
  - > A good example for this is a "classical LLM project" where the AI part is accessed via an API and internally there is an application developed around that external functionality

- Off-the-shelf + Internal customization:
  - > Purchase a foundation, fine-tune with your data

- Custom + External development:
  - > Contract specialists to build bespoke solutions

- Platform + Internal applications:
  - > Use cloud AI services as infrastructure, build applications internally

5.3.1 Some guidance on choosing an approach

Favour Off-the-Shelf / External Purchase when:

- The use case is common across industries (document processing, general object detection, standard analytics)
- Speed to deployment is critical
- Internal AI/ML expertise is limited or cannot be sustained long-term
- Budget constraints preclude significant development investment
- The vendor has proven airport or aviation industry experience
- Risk transfer through contractual arrangements is desirable

Favour Custom / Internal Development when:

- Operational requirements are highly specific to your airport's context
- No existing solutions adequately address the identified need
- Long-term control over the technology roadmap is essential
- Regulatory requirements demand full control over the technology stack
- Integration with legacy systems requires deep institutional knowledge

Favour Hybrid Approaches when:

- Core AI functionality exists off-the-shelf but integration is complex
- You want to build internal capability progressively while delivering value now
- The use case requires combining multiple AI technologies from different sources

5.3.2 Critical Considerations

Total Cost of Ownership. The initial purchase or development cost is often the smaller component. Consider:

Phase	Off-the-Shelf	Custom
Initial	License fees, implementation	Development, infrastructure
Ongoing	Subscription (might change), upgrade fees	Maintenance, retraining, staffing
Hidden	Customization limits, integration complexity	Skill retention, technical debt

Do note that underestimating AI maintenance resources is a common failure mode. Self-developed solutions require ongoing investment in model monitoring, retraining, and adaptation. These costs are often included in vendor contracts but might be overlooked in internal projections.

Vendor Lock-in and Exit Strategy. Regardless of approach, plan for change:

- Ensure data portability from day one
- Avoid proprietary formats that create irreversible dependencies
- Document APIs and integration points thoroughly
- Include exit provisions in vendor contracts
- Retain enough internal knowledge to transition if needed

Capability Building. Consider not just the immediate need but the strategic trajectory:

- Does this decision build or erode internal (AI) capabilities?
- Are you creating sustainable expertise or permanent dependency?
- How does this choice position you for future AI initiatives?

5.3.3 Decision checklist

Before committing to an approach, answer these questions:

Strategic Fit

- Does this approach align with our organisation's AI strategy?
- Have we assessed the long-term implications, not just immediate needs?

Capability Assessment

- Do we have (or can we build) the internal expertise required?
- Can we sustain that expertise over the solution lifecycle?

Risk Evaluation

- What are the risks of each approach for this specific use case?
- How does vendor/development risk compare to operational risk of delay?

Financial Analysis

- Have we calculated true total cost of ownership for each option?
- Are maintenance and evolution costs included in internal development estimates?

Flexibility:

- Does this approach allow us to change course if needed?
- What are the switching costs if this choice proves wrong?

5.3.4 Key take-aways

1. **It's rarely binary:** Most successful implementations combine off-the-shelf components with custom elements and blend internal expertise with external support.

2. **Match approach to use case:** Different AI applications within the same airport may warrant different sourcing strategies.

3. **Plan for the lifecycle, not just deployment:** The initial build/buy decision shapes years of operational reality.

4. **Honestly assess capabilities:** Overestimating internal capacity is as risky as underestimating vendor limitations.

5. **Preserve optionality:** Whatever approach you choose, structure it to allow future flexibility.

5.4 Single vs. multi-vendor approach?

When building a stack of AI solutions within an airport one of the questions that arises often on a strategic level is whether there is a decision to be made for one single or multiple vendors when purchasing solutions. Should there be a preferred vendor?

Below some general considerations can be found to take into account when defining such a strategy.

Single-Vendor Advantages:

- Simplified integration and reduced interoperability challenges
- Single point of accountability for system performance
- Potentially stronger negotiating position through consolidated purchasing
- Streamlined vendor management and contract administration

Multi-Vendor Advantages:

- Multiple expert companies that cater for a specific use case
- Rapidly changing vendor landscape
- Reduced dependency and lock-in risk
- Greater resilience, single vendor failure does not compromise entire AI ecosystem
- Competitive pressure improves negotiation position
- AI projects that are built on top of foundational LLMs functionality can oftentimes be decoupled from a specific vendor that provides the LLM. This presents at a moment a future-proof option at low cost.

Recommended Approach: Establish clear integration standards and APIs, then select vendors based on capability within defined interoperability requirements. Critical operational systems may warrant redundancy through multiple vendors, while back-office applications may benefit from consolidation.

Essential Safeguard: Regardless of approach, ensure data portability and avoid proprietary formats that create irreversible vendor dependencies. Contract negotiations should address exit strategies from the outset.

5.5 Multi-stakeholder and multi-user considerations

Airports operate as ecosystems where multiple stakeholders (airlines, ground handlers, border agencies, retailers, and service providers) increasingly deploy AI-enabled solutions. Without deliberate coordination, this fragmented landscape risks duplicated effort, inconsistent data quality, and unclear accountability when systems interact.

The foundational principle

The airport owns the infrastructure and has a strategic interest to retain sovereignty over the data generated within it. This principle can be embedded in commercial agreements: tenders and contracts should stipulate that relevant data generated through stakeholder activities remains accessible to the airport operator under clearly defined terms. Such provisions protect long-term data sovereignty and prevent vendor lock-in.

Key considerations

Deployment governance: Airports should establish clear parameters for AI deployment by third parties, defining which applications may be deployed independently and which require formal approval. Thresholds should reflect both operational risk and integration complexity.

Standards and interoperability: Mandating minimum standards for data quality, formats, security, and interoperability ensures stakeholder solutions can coexist within the broader ecosystem. Note that shared data environments function most effectively when governed by agreed protocols.

Data quality assurance: When stakeholders produce AI-generated data that enters shared systems, airports should require quality gates, provenance marking, and minimum confidence thresholds before acceptance.

Recommended Approach

Define enforceable standards while providing shared services where consolidation delivers value. Proactive governance is preferable to reactive intervention when issues emerge.

5.6 Workforce and social considerations

AI deployment in airports invariably raises workforce concerns. These span from concerns regarding job displacement, changing role requirements, and the pace of technological change. If unaddressed, these worries can significantly impede implementation regardless of technical merit. Union engagement and employee acceptance frequently determine whether AI initiatives progress beyond pilot stage.

AI as enabler

Positioning AI as a tool that augments rather than replaces human capability is essential for building acceptance. In practice, most airport AI applications enhance decision-making, reduce repetitive tasks, or improve safety oversight; they rarely eliminate roles entirely. Communicating this distinction clearly, with concrete examples relevant to affected staff, helps counter narratives of wholesale automation.

Key considerations

Early engagement. Involve workforce representatives from the ideation phase rather than presenting AI as a "fait accompli". Early dialogue builds trust and surfaces practical concerns that improve implementation design.

Transparency on impact. Be explicit about how roles will change. Uncertainty fuels resistance; clarity enables constructive adaptation.

Reskilling pathways. Demonstrate commitment to workforce transition through training programmes that equip employees to work alongside AI systems or move into new roles created by the technology.

Recommended approach

Leverage existing change management processes rather than creating parallel structures. Most airports have established frameworks for managing operational change that already incorporate human factors, risk assessment, and stakeholder engagement. AI initiatives should integrate with these processes, positioning workforce considerations as standard practice rather than exceptional accommodation.


Prijava na let
Check-in
B 15-22
Odhodi
Departures

6 Safety and compliance for AI projects in practice

This section applies the safety and compliance dimensions of the phased-matrix framework on three real-world use cases.

6.1 Example 1: Turnaround analysis

Leverage cameras monitoring turnaround operations to automatically detect the precise start and finish times of key activities (e.g., refuelling, loading, offloading, etc.). This real-time detection enables early identification of deviations from scheduled operations, ensuring the smooth orchestration of all turnaround-related services.

Category	Idea	Analysis / PoC	Production	Maintenance & Lifecycle
Security - IT	Identify critical constraints (e.g., cybersecurity, biometrics).	Engage security stakeholders, assess risks.	Manage dependencies and third-party integrations.	Monitor ongoing security.
Safety - Ops	Assess operational safety implications.	Confirm solution meets safety/security requirements.	Plan safe rollout, replacement, or upgrades.	Monitor operational compliance.
Compliance	Identify applicable frameworks and limitations.	Check approvals and regulatory alignment.	Ensure compliance in production (AI Act, GDPR, local laws).	Track evolving regulations and maintain compliance.

6.1.1 Ideation phase

Given the substantial costs associated with a Proof of Concept (PoC) for camera based turnaround analytics (e.g. deployment of cameras, networking, IT infrastructure and integration), it is recommended to address security and compliance questions before these investments are made. For this type of use case, the risk profile means that many security and compliance considerations that might be treated lightly or postponed in other projects must be frontloaded into the ideation stage and revisited at PoC approval.

IT security

- **Hardware architecture:** What is the optimal approach for establishing a secure hardware and data environment? Should the focus be on a CCTV type of approach, connected devices, or a combination? Furthermore, how can security be guaranteed throughout the deployment of software and AI model updates?

- **Deployment and Infrastructure:** What is the best strategy for deploying IT services and resources (local vs. cloud)?

Operational safety & security

- **System Reliance and Human Oversight:** What is the required level of dependence on the automatic detection system? What are the consequences of incorrect information, and what role does "Human-in-the-Loop" play in validation and decision-making?

- **Contingency Planning and Risk Management:** What level of reliance is established on the system, and how is the risk of potential downtime or even third party phase out managed?

- **Security and Override Mechanism:** How can the system be reliably deactivated or overridden for high-security scenarios (e.g., special cargo or passengers)?

Regulatory and data compliance

- **Scope Definition:** Define the data strategy, addressing:
  - > What data is captured?
  - > What data is stored, and for what purpose (e.g., Audits, historical performance tracking)?
  - > What are the minimum essential data dimensions required to support this use case?

- **GDPR Compliance:** Ensure adherence to General Data Protection Regulation (GDPR) requirements:
  - > Managing Personally Identifiable Information (PII) for both workers and passengers.
  - > Establishing data retention policies for all PII data.

- **AI Act:** Compliance with the high-risk classification, requiring adherence to all associated standards.

- **Labour Laws:** Address legal implications related to employee surveillance.

6.1.2 Analysis/ PoC

IT security

- **Secure-by-design PoC environment**
  - > Can we apply/test the same basic controls as for production (hardening, patching, MFA, logging), so that these characteristics can be tested as integral parts of the PoC?

- **Early security validation**
  - > During the PoC, run targeted security checks (config reviews, basic vulnerability scans, log reviews) to validate that the chosen architecture and controls are robust enough before scaling.

Operational safety & security

- **Camera placement and operational fit**
  - > Does the actual placement and field of view of the cameras support the intended operational use cases (e.g. visibility of all critical turnaround activities, minimal blind spots, no interference with existing procedures)?
  - > Are there any practical side effects for ramp crews (e.g. glare, obstructions, "dead angles") that require adjustment of camera locations or mounting?

- **Integration into day-to-day operations**
  - > Based on observed performance during the PoC (accuracy, latency, robustness), for which concrete tasks can the tool safely support or replace existing procedures (e.g. activity timestamping, SLA monitoring, incident review)?
  - > What changes to standard operating procedures (SOPs), roles and responsibilities are needed so that the tool is used consistently, without creating confusion or parallel processes?

- **Impact on safety outcomes**
  - > What is the observed impact of the system on safe airport operations during the PoC: do we see more timely detection and reporting of safety relevant events (e.g. incursions, unsafe vehicle movements, equipment misuse) on monitored aprons?
  - > Compared to a suitable control group (stands without the system, or pre PoC baseline), do we observe a change in the frequency, detection rate, or severity of safety relevant events?

Compliance

- **Stakeholder information and involvement**
  - > Have all critical stakeholders been identified and informed about the PoC (e.g. airlines, ground handlers, unions/works councils, Data Protection Officer, security and safety teams, regulator if applicable)?

- **Consent, legal basis, and transparency**
  - > For workers and passengers, what is the appropriate legal basis for processing (e.g. legitimate interest, legal obligation, contract), and in which cases is explicit consent required rather than simple information?
  - > Are notices and communications in place so that people in the monitored areas understand that the PoC is running, what is being recorded, and for what purposes?

6.1.3 Release to production

Security – IT

- **Architecture and deployment**
  - > Define and document the target architecture for turnaround analytics (camera layer, edge devices, backend, storage), including segregation from other airport systems and integrations with third-parties

- **Access control and infrastructure hardening**
  - > Harden and centrally manage all cameras, edge boxes and servers (patching, configuration baselines, secure provisioning and decommissioning).
  - > Ensure logging and monitoring for abnormal access (e.g. unusual clip exports, repeated viewing of a specific stand).

- **Data lifecycle and resilience**
  - > Implement technical retention and deletion rules for raw video, incident clips and derived turnaround events, with evidence of deletion, moving from PoC to quality audit-oriented retention.

Safety – Operations

- **Operational integration and reliance**
  - > Clearly define where the system is advisory versus where operations rely on it (e.g. SLA monitoring, gate assignment, incident review).
  - > Update SOPs, roles and training so ramp crews, airlines and APOC understand how to use the analytics and where human in the loop is mandatory.

- **Safety and incident handling**
  - > Monitor whether the system leads to earlier detection and better handling of safety relevant events on monitored aprons versus baseline/control stands.
  - > Define and rehearse procedures for system outages or degraded performance (manual fallbacks, communication to stakeholders, reversion to baseline processes).

- **Overrides and special situations**
  - > Provide controlled override or “restricted mode” options for high security or exceptional operations (VIP flights, police/military, special cargo).
  - > Log and periodically review all overrides to ensure they are justified and do not undermine overall safety or data integrity.

Compliance

- **Regulatory and contractual alignment**
  - > Maintain an up to date DPIA covering the actual production footprint (stands, partners, vendors, processing regions) and ensure mitigations are implemented.
  - > Align the system with aviation and local safety regulations, airport security programmes, and contractual commitments to airlines and handlers.

- **Privacy, GDPR, and AI Act**
  - > Precisely define what data is captured and stored (video, metadata, events) and why, applying data minimisation and purpose limitation.
  - > Enforce GDPR controls for workers and passengers (legal basis, information notices, retention, deletion, handling of access/erasure requests).
  - > Treat the system as a likely **high risk AI** use case: document risk management, human oversight, logging, quality management and post market monitoring.

- **Labour law and stakeholder governance**
  - > Ensure compliance with labour laws and collective agreements on employee monitoring; consult and maintain dialogue with works councils/unions where applicable.
  - > Clearly limit and document which uses are allowed (safety, operational performance) and which are prohibited (covert disciplinary tracking, individual productivity scoring).
  - > Keep key stakeholders (airport operator, airlines, handlers, DPO, safety and security teams) informed about scope changes and review outcomes.

6.1.4 Operations

In this last stage, a process needs to be supporting the risk categories, typically with questions to be reviewed on a regular basis. For example:

Security – IT: Continuous monitoring

- Are all cameras, edge devices, networks, and backends continuously monitored for vulnerabilities, misconfigurations, and suspicious activity?

- Do we have defined security KPIs and thresholds (e.g. patch latency, failed logins, unusual exports) that trigger investigation?

- Are access, admin and model change logs retained long enough and regularly reviewed by a designated team?

- Is there a clear process to incorporate findings from incidents, audits and pen tests into improved hardening and monitoring?

- Are third party components (camera firmware, VMS, cloud services, AI libraries) tracked for security advisories and promptly updated?

Safety – Ops: Continuous monitoring of operational compliance

- Are operations regularly checked to confirm that the system is used according to approved SOPs (how alerts are handled, when human review is required)?
- Has the level of reliance on the system been reviewed recently (no drift from "decision support" to "automatic decision" where not allowed)?
- Are we monitoring whether safety relevant behaviours and events on monitored aprons are detected, escalated and resolved as designed?
- Do we run periodic reviews with operations, safety and ground handling teams to validate that the system supports safe operations and does not introduce new risks?
- Are override and "restricted mode" features reviewed to ensure they are used only when justified and do not undermine overall safety?

Compliance: Tracking new regulations & maintaining obligations

- Is there a named owner responsible for tracking regulatory and contractual changes relevant to the system (GDPR, AI Act, aviation/security rules, labour law)?
- Are DPIAs, records of processing, policies and contracts reviewed on a regular schedule and whenever scope, technology or vendors change?
- Can we demonstrate ongoing compliance with key obligations (retention and deletion, data subject rights, AI Act high risk requirements, worker information/consultation)?
- Is there a defined workflow to turn new or changed obligations into concrete technical and procedural updates, with evidence of implementation?
- Are key stakeholders (airport operator, airlines, handlers, DPO, safety, security, worker reps) periodically informed about review outcomes and changes affecting them?

6.2 Example 2: Asset management document classification

Brussels Airport's Asset Management department maintains roughly 1 million technical documents across many domains (technical specifications, fire-safety plans, maintenance procedures, BIM information, ...). Organically developed storage spaces and absence of unified, evolutive classification made retrieval difficult and blocked an upcoming migration to a common data platform. An LLM-powered solution was developed, using zero-shot classification pipeline (no training data) and achieving 86–98% accuracy. Unlike the previous use case, the dominant risks cluster around broad data access and personal data, so the framework is applied with that emphasis.

6.2.1 Ideation phase

The defining question at ideation is data access: an application that classifies across the full documentation estate inherently needs broad read access, which is a significant security and governance concern that must be framed before any build.

Security – IT

- **Access scope:** Who needs access to which documents and metadata, and how is access granted without over-provisioning?
- **"Massive data access" red flag:** How do we justify and contain an application that reads across many source systems, including potential data transfer between them?
- **Secure data access:** Establish the requirements for secure, auditable data access for the application.
- **Need-to-know access:** Plan to inherit the organisation's existing access rights rather than create new, broad access, so users only ever see what they are already entitled to.

Operational safety & security

- **Replacing human work with AI:** Assess the risks of automating classification, in particular accountability for misclassification and gradual skill deterioration of staff.

Regulatory and data compliance

- **GDPR**: Confirm applicability up front, since documents may contain PII.

6.2.2 Analysis / PoC

Security – IT

- Treat *secure data access for the application* as an explicit, testable PoC deliverable rather than a later concern.

- Minimise the tech stack and avoid scattering the AI application across multiple vendors, limiting attack surface and integration complexity.

Operational safety & security

- Secure validation of the automated classification by business stakeholders; strong stakeholder commitment is needed to trust and act on the output.

- Define and test the behaviour when classification confidence is low (default safely, route to human review, or hold the document)

Compliance

- Ensure the LLM deployments used in the PoC are compliant (approved models, compliant hosting/region, appropriate data-handling terms).

6.2.3 Release to production

Security – IT

- Roll out securely to all eligible domains across the company.

- Integrate with Enterprise IT (identity and access management, logging, monitoring, support).

Safety – Operations

- Define and run a structured change process so affected teams adapt workflows, roles and responsibilities as classification becomes automated.

Compliance

- Maintain compliance as the system scales from PoC into production use.

- **Clear ownership of the classification scheme:** distinguish ownership of the business rules (categories, naming conventions) from the technical engine, and define how rule changes are proposed, approved, versioned and communicated.

- **Traceability of decisions:** record what the AI proposed, how confident it was, and the final human-validated value, so every classification can be explained and audited.

6.2.4 Operations

Security – IT: Continuous monitoring

- Monitor the underlying foundation models, which have short lifecycles; validate updates before adopting them (regression checks), re-validate classification accuracy, and keep data within the agreed region and governance boundaries.

Safety – Ops: Continuous monitoring

- Track classification performance over time and spot misalignment or drift early.

Compliance: Tracking new regulations & maintaining obligations

- Remain compliant as scope extends to new domains, monitoring evolving **GDPR** and **AI Act** obligations.

- When the classification scheme changes, decide how already-classified documents are reprocessed so the corpus does not drift into inconsistency.

6.3 Example 3: Border & security staffing (Demand–Capacity Balancing)

The airport operations team for border & security ensures the smooth processing of passengers, in cooperation with operational service partners. The deployed solution forecasts passengers per location, simulates queues and waiting times based on capacity scenarios, and recommends staffing levels to achieve SLAs, while also letting users play out what-if scenarios for both post-operations analysis and forward planning. This case is a **decision-support** tool for staffing rather than a safety-critical control system; its main sensitivities are passenger personal data, dependence on external data and partners, and the operational costs of understaffing or overstaffing security and border controls.

6.3.1 Ideation phase

Security – IT

- **Data security & PII:** Passenger volumes and forecasts rely on personal data; identify what is processed and how it must be protected.

- **Data access & processing:** Define which data is needed, where it originates, and how it is processed and stored.

- **Hardware & infrastructure:** Determine the compute and hosting requirements for forecasting and simulation early on.

Operational safety & security

- **Operational criticality:** Is the application operation-critical, and what are the risks and costs of errors (e.g. understaffing causing long queues and missed connections, or overstaffing driving avoidable cost)?

- **Decision support, not automation:** Frame the tool as advice that informs human planning; the teams and operational service partners running the checkpoints stay in control of the final staffing decision.

Regulatory and data compliance

- **GDPR:** Confirm applicability up front, since passenger data is personal data.

6.3.2 Analysis / PoC

Security – IT

- Assess **external dependencies** and third-party integrations (data providers and software), and the risks they introduce to availability and security.

Operational safety & security

- Run a **risk analysis** that quantifies the main risks and defines mitigation strategies (data availability, outages, degraded forecasts, ...).

Compliance

- Confirm the **authorisation and clearance levels** of the involved operational service partners for the data and the decisions the tool supports.

6.3.3 Release to production

Safety – Operations

- Define the **change-management** approach — whether the tool replaces or augments existing staffing decisions — and establish clear product ownership.

- Clarify the **accountability boundary:** the tool advises, while the operational service partners commit and deploy the staff and remain responsible for the final decision; make this split explicit so reliance never drifts into unattributed automated decision-making.

Compliance

- Govern **information sharing with partners:** define what forecasts and recommendations are shared, with whom, how often, and under what confidentiality terms, so operational service partners get what they need without over-sharing.

6.3.4 Operations

Security – IT

- Maintain the system with **secure builds** (library updates, patches) and ongoing IT maintenance.

Safety – Ops

- Monitor forecast and simulation performance, recognising that recommendations are only as reliable as the upstream forecasts and modelled passenger behaviour; watch for drift as patterns shift and re-validate that simulated queues still match reality.

- Use the what-if capability to anticipate disruptions (e.g. strikes, major schedule changes, demand surges) and prepare contingency staffing ahead of time.

Compliance

- Track changes in compliance obligations and other applicable standards over time, including regulatory or operational changes that alter how checkpoints process passengers, and update the model and its assumptions so it stays aligned with reality.

7 Supporting governance model

The introduction of AI into airport operations requires a clear governance structure with defined roles and responsibilities. This section describes the minimum governance set-up required to ensure safe, compliant, and value-driven AI adoption.

Depending on the airport's digital maturity, scale of AI usage, and strategic ambition, this structure can be extended towards a dedicated AI governance or AI-oriented department, particularly where there is a clear intention to develop, operate, and manage AI solutions in-house.

AI governance does not need to be built entirely from scratch. In many cases, it can be anchored in existing governance, safety, compliance, and IT structures, with targeted extensions to address AI-specific risks such as algorithmic decision-making, data dependency, and regulatory requirements under the EU AI Act.

7.1 Basic roles & responsibilities

At a minimum, AI governance should introduce the following components:

- **AI Core Team** (which may evolve into a formal AI Lead function)
- **AI risk management system**, aligned with existing enterprise and safety risk frameworks
- **AI assessment tools**, such as AI questionnaires and checklists, to support classification, procurement, and compliance decisions

These components ensure that AI use cases are identified, assessed, monitored, and governed consistently across the organization.

In addition to governing individual AI use cases, airports should maintain oversight of their overall AI portfolio. This includes maintaining an inventory of AI systems, monitoring aggregated operational, safety, cybersecurity, privacy, and compliance risks, identifying systemic dependencies on AI technologies and suppliers, and ensuring that AI adoption remains aligned with organisational objectives and risk appetite. Periodic reporting to senior management should provide visibility on AI deployments, risk trends, incidents, regulatory developments, and emerging governance needs.

The following roles represent the baseline governance structure needed to safely and compliantly deploy AI at an airport. These roles can typically be embedded within existing departments, under existing roles.

- **AI Governance Lead / AI Core Team**
  - > Responsible for overall AI coordination and governance, without necessarily owning AI systems directly.
  - > Maintain an company-wide inventory of AI systems and use cases
  - > Monitor aggregated AI risks and dependencies across the organisation
  - > Report AI portfolio status, incidents, and emerging risks to senior management
  - > Ensure AI initiatives remain aligned with organisational strategy and risk appetite

- **Compliance & Legal**
  Ensures alignment with regulatory requirements, in particular the EU AI Act.

- **Privacy & Ethics**
  Extends existing data protection and ethical oversight to AI-specific risks.

- **Technical Ownership & Security**
  Ensures that AI systems are technically robust, secure, and fit within the airport's IT architecture.

- **Data Governance**
  Ensures that data used by AI systems is governed, traceable, and suitable for operational and regulatory needs.

7.2 Extended roles for mature AI adoption

As AI becomes more embedded in safety-critical and operational processes, airports should consider extending governance with dedicated AI-focused roles, particularly where high-risk AI systems are involved.

Traditional safety functions should extend their scope to include:

- Algorithmic and data risks
- Model drift and performance degradation
- Transparency and explainability of AI-driven decisions

This function may take the form of a **dedicated AI oversight team** or an extension of an existing safety assurance or SMS function. Key monitoring areas include:

- AI performance and accuracy over time
- Bias, unintended consequences, and edge cases
- Data integrity and availability
- Human-in-the-loop effectiveness
- Incident reporting and corrective actions related to AI outputs

This ensures AI becomes part of the airport's safety culture, rather than a stand-alone technology initiative.

Extended Specialist Roles (Optional, Based on Maturity)

For airports with advanced AI usage, the following roles may be added:

- **AI Safety & Assurance Lead**
  > Accountable for AI-related safety, monitoring, compliance reporting, and integration with SMS.

- **Data Steward / Data Quality Officer**
  > Responsible for data quality, lineage, and fitness-for-purpose across AI use cases.

- **Model Operations Engineer**
  > Deploys and monitors AI models in operational environments, manages drift, retraining triggers, and performance dashboards.

- **AI Change Champion**
  > Supports operational teams, promotes adoption, gathers user feedback, and tracks organizational impact.

- **Regulatory Monitoring Role (within Safety or Compliance)**
  > Monitors evolving AI regulations and standards and ensures timely internal updates.

This section can be summarized in the following table:

Role	Accountability	Key responsibilities
AI Governance Lead / AI Core Team	AI Core Team (evolves into AI Lead)	• Define AI strategy and maintain oversight of AI use cases • Proactively identify value-adding AI opportunities • Establish and coordinate AI governance processes (policies, risk management, documentation) • Drive cross-functional collaboration between business, IT, safety, and data • Build organizational AI capabilities and awareness
Compliance & Legal	DPO / Legal Function	• Monitor compliance with the EU AI Act • Classify AI systems (high-risk, limited-risk, minimal-risk) • Determine the airport's role and obligations under the EU AI Act • Translate legal requirements into AI questionnaires, contractual clauses, and compliance checklists • Act as primary contact for supervisory authorities and coordinate regulatory interactions
Privacy & Ethics	Data Protection Officer (DPO)	• Ensure compliance with GDPR when AI systems process personal data • Advise on Data Protection Impact Assessments (DPIAs) for AI systems • Provide guidance on ethical risks (bias, discrimination, transparency) • Serve as contact point for individuals and authorities on AI-related privacy concerns • Support AI technical documentation and compliance declarations
Technical Ownership & Security	ICT	• Assess AI vendors and technical solutions • Ensure accuracy, robustness, resilience, and cybersecurity of AI systems • Maintain AI-related technical infrastructure and enterprise architecture • Implement technical controls within the AI risk management system
Data Governance	Data & Analytics	• Define and enforce data governance and quality standards • Maintain AI inventory, record-keeping, and logs • Support post-market monitoring requirements • Align AI inventory with business demand • Define buy-vs-build policies, decision matrices, and standard contractual clauses
Extended AI governance roles (for mature AI adoption)		
AI Safety & Assurance Oversight	Safety Function / AI Safety & Assurance Lead	• Extend existing safety governance to include AI-specific risks • Define AI safety policies and interfaces with the Safety Management System (SMS) • Monitor AI hazards (model drift, bias, unintended consequences, data integrity) • Maintain AI performance dashboards, logs, and audit trails • Coordinate incident management, reporting, and corrective actions
Model Operations Engineer	ICT / Data & Analytics	• Deploy AI models into operational environments • Monitor performance, accuracy, and drift • Define retraining triggers and version control • Support reliable and auditable AI operations
Data Steward / Data Quality Officer	Data & Analytics	• Ensure AI training and operational data is accurate, timely, and fit-for-purpose • Monitor data lineage and quality controls • Support compliance and auditability of AI data pipelines
AI Change Champion	Business / Operations	• Promote AI adoption within operational teams • Support change management and user acceptance • Collect feedback and track operational impact of AI solutions
Regulatory Monitoring Role	Safety or Compliance	• Monitor evolving AI regulations, standards, and guidance • Translate regulatory updates into internal policies and processes • Coordinate regulatory readiness across governance functions

7.3 Organizational model

Selecting an organisational model for AI is a key governance decision, as it determines where expertise sits, how decisions are made, and how risks are controlled. The chosen model directly impacts consistency, compliance, speed of innovation, and the ability to scale AI safely in a regulated airport environment. The model should align with regulatory pressure, data maturity, and organisational structure.

Dimension	Centralised	Centre of Excellence	Decentralised
Core concept	Single central body oversees all AI initiatives	Centralised standards and expertise combined with distributed innovation	AI capabilities embedded within business teams
Decision-making	Centralised	Shared between CoE and business teams	Distributed across teams
Ownership of AI initiatives	Central AI team	Business teams own use cases, CoE governs standards	Business teams
Organisational fit	Hierarchical or matrix structures	Organisations undergoing transformations across multiple domains	Flat organizational structures
Benefits	Strong control, consistency, and compliance; clear accountability	Balances control and innovation; facilitates collaboration, and standardisation	High flexibility and autonomy; strong local ownership
Drawbacks	Inflexible; risk of bottlenecks and slower response	More complex to manage and coordinate	Risk of inconsistencies, duplicated effort, and reduced oversight
Best suited for	Heavily regulated environments; strict data protection and privacy needs	Organisations seeking large-scale AI adoption across multiple domains	Low regulatory intensity; mature, autonomous teams with easy access to data

7.4 Changing the organisation

Integrating AI into airport operations requires updates to roles, processes, and governance. Key organisational changes include:

- Reconfiguring process flows to embed AI outputs, alerts, and decision support into operational loops.
- Updating change management protocols to clarify responsibilities, engage staff, and phase transitions to minimise disruption.
- Revising operational manuals (AOM, SMS, SOPs) to reflect new AI tools, interfaces, and organisational structures.
- Establishing procedures for monitoring AI system performance, triggering human review, and maintaining audit trails of AI inputs, outputs, and overrides.
- Implementing data governance and quality assurance procedures specific to AI inputs and feedback loops.
- Defining procedures for AI model retraining, version control, and deployment from pilot to full operational use.

These updates ensure transparency, traceability, and safe integration of AI into the airport's operational ecosystem.

7.5 Organisational Training

Effective training ensures that all stakeholders can safely and confidently operate AI-enabled systems. Training should include:

- Basic training for all staff: AI awareness, capabilities, limitations, risks (e.g., bias, data drift), and safe interaction with AI-enabled workflows.
- Data quality fundamentals: importance of high-quality data and the impact of poor data on AI outcomes.
- Role-specific training for extended roles (AI Safety Lead, Data Steward, Model Operations Engineer) covering technical, procedural, and regulatory responsibilities.
- Continuous learning and refresher sessions to address system updates, new modules, evolving risks, and feedback loops.

A structured training program builds operational readiness and fosters a culture of safe, responsible innovation. Recommended start: annual core sessions with additional updates aligned to system changes and organisational needs.

ANNEX 1
Case Studies across Europe

A summary of use cases (airside oriented) at airports across Europe. The following use cases have been provided by airports through a survey:

Category	Airport Code	Type of Solution	Status
Airside	BER	Digital Turnaround – Apron AI	Implemented
Airside	LJU	AI Apron Management Tool	Tested
Airside	WAW	Turnaround Monitoring	Potential
Airside	AMS	Deep Turnaround	Implemented
Airside	AVN	Autonomous Vehicles	Implemented / Testing
Airside	AVN	Turnaround ML	Testing / Pilot
Airside	AVN	Gate Allocation	Proof of Concept
Airside	AVN	Runway Chemical Support	Proof of Concept
Airside	ARN	FOD & Wildlife Detection	Implemented
Airside	MUC	Camera Turnaround Monitoring	Implemented
Airside	MUC	AIMS (Flight Status)	Project Phase
Airside/Ops	CPH	Better Airport AI	Implemented
Airside/Safety	WAW	Chemical Rescue Support	Potential
Commercial	AVN	AI Route Development	Proof of Concept
Landside	LJU	Autonomous Announcement System	Concept
Landside	WAW	Biometric Solutions	Potential
Landside	WAW	Queue & Taxi Management	Potential
Landside	AVN	Queue Length Prediction	In Operations
Landside	MUC	Pax Flow Analytics	Project Phase
Landside	MUC	Luggage Delivery Prediction	Project Phase
Landside/Service	WAW	Chatbot AI	Potential
Landside/Service	AVN	AVIguide Assistant	Proof of Concept
Landside/Service	MUC	Website ChatBot	Implemented
Operational Support	LJU	Resource Allocation Tool	Under Development
Operational Support	AVN	LLM for Training/Info	Testing
Operational Support	AVN	AI Team Internal Lab	Internal
Security	WAW	Security Screening & Counter-UAV	Potential
Security	AVN	Camera Security Systems	In Operations

On the next pages, a deep dive is presented into the airside solutions.

Berlin Brandenburg Airport (BER)

Digital Turnaround (Apron AI)

Description

AI-driven turnaround monitoring solution that creates transparency across airport stakeholders, airlines, and air traffic control. It monitors turnaround milestones in real time and alerts stakeholders when delays are detected.

Improvements in KPI's

- ✓ Reduced delay minutes, particularly those attributable to ground handlers.
- ✓ Resolved issues related to late baggage delivery.
- ✓ Improved accuracy of predicted turnaround milestones by more than 30%.
- ✓ Improved coordination and operational stability.

Lessons learned

- ✓ Increased transparency and visibility improve accountability and operational performance.
- ✓ Earlier and more reliable predictions support better planning across stakeholders.

Ljubljana / Fraport Slovenija (LJU)

AI Apron Management & Resource Allocation

Description

Testing AI-based apron management tools and implementing AI-supported resource allocation for staff and ground support equipment (GSE).

Improvements in KPI's

Not specified

Lessons learned

- ✓ AI solutions must be evaluated on a case-by-case basis.
- ✓ No solution is fully tailor-made; adaptation and calibration require significant effort.
- ✓ Data quality is critical ("garbage in – garbage out").
- ✓ Good input data can enable meaningful savings and stronger business cases.
- ✓ AI can provide valuable employee support and improve task management in a complex regulatory environment

Warsaw Chopin Airport (WAW)

Potential Future AI Applications

Description

The airport is not currently using AI in operational areas but has identified multiple potential use cases, including biometric passenger processing, queue management, turnaround monitoring, security screening, chatbot support, chemical rescue support, and drone detection.

Improvements in KPI's

Not specified (conceptual/future applications only).

Lessons learned

Not specified.

Copenhagen Airport (CPH)

Optimization – Better Airport

Description

AI-enabled airport operations platform using machine learning for passenger and baggage forecasting, AI-driven turnaround monitoring inputs, and optimization models for stand, gate, and workforce allocation.

Improvements in KPI's

Not specified

Lessons learned

Not specified.

Amsterdam Airport Schiphol (AMS)

Deep Turnaround

Description

AI-powered turnaround monitoring system combining computer vision, neural networks, and prediction algorithms. It monitors more than 70 turnaround processes and integrates with airport operational systems and partners.

Improvements in KPI's

- ✓ Sustainable on-time performance (OTP) improvement of 4 percentage points in 2024.
- ✓ Improved operational predictability.
- ✓ Improved collaboration across the airport ecosystem.

Lessons learned

- ✓ AI itself is only the starting point; benefits are realized through successful deployment and operational integration.
- ✓ Strong ecosystem collaboration is important to realizing value.

Munich Airport (MUC)

AI-Driven Operational Efficiency and Passenger Experience

Description

Munich Airport is deploying AI across multiple operational and passenger-facing processes. The use cases include camera-based turnaround monitoring, passenger flow monitoring, baggage delivery time prediction, automation of flight status updates, and an AI chatbot for passenger support. The overall objective is to improve operational efficiency, increase predictability, reduce manual workload, and enhance the passenger experience.

Improvements in KPI's

Use Case	KPI Improvements
Camera-based turnaround monitoring	Not specified.
Passenger flow monitoring	No quantified KPI improvements provided. Intended to improve operational efficiency, safety, and passenger experience through real-time monitoring and predictive planning.
Baggage delivery time prediction	Not specified.
Flight status automation (AIMS)	Intended reduction in manual workload through automation of flight status updates. No quantified results provided.
AI chatbot	Reduced workload for call center staff. No quantified results provided.

Lessons learned

Munich Airport's AI initiatives demonstrate a broad application of AI across operational efficiency and passenger service processes, but no specific implementation lessons or learnings were documented.

Oslo Airport (OSL) - Avinor

AI in Airport Operations

Description

Avinor is applying and testing AI across a broad range of airport operations. Current operational use cases include passenger queue prediction, security camera vision, and autonomous vehicles for snow clearing and airside inspections. In parallel, Avinor is developing and piloting AI solutions for turnaround optimization, staff training and information retrieval, gate allocation, route development, personalized passenger assistance, and runway condition prediction. These initiatives are driven by both internal AI teams and technology partners.

Oslo Airport (OSL) - Avinor

AI in Airport Operations

Improvements in KPI's

Use Case	KPI Improvements
Queue prediction	Not specified.
Security camera vision	Not specified.
Autonomous snow clearing & airside inspection	Not specified.
AI turnaround optimization	No quantified KPI improvements provided. Intended to improve safety and operational efficiency.
LLM for training & information retrieval	Not specified.
AI gate & stand allocation	Proof of concept indicated potential to increase capacity, improve robustness, and reduce costs. No quantified results provided.
AI route development	Not specified.
AVIguide passenger assistant	Not specified.
Runway chemical-use decision support	Intended reduction in chemical consumption through improved decision support. No quantified results provided.

Lessons learned

Use Case	KPI Improvements
Queue prediction	Not specified.
Security camera vision	Not specified.
Autonomous snow clearing & airside inspection	Not specified.
AI turnaround optimization	The project evolved from a safety-focused initiative toward performance optimization. Testing at Trondheim provides experience for larger-scale deployment at Oslo Airport.
LLM for training & information retrieval	The solution remains experimental and is not yet intended for operational use.
AI gate & stand allocation	The proof of concept demonstrated feasibility and value creation potential. Learnings will be incorporated into future resource management systems.
AI route development	The proof of concept demonstrated that AI can support route development analysis; operational deployment is planned.
AVIguide passenger assistant	Not specified.
Runway chemical-use decision support	Combining runway, weather, friction, and historical data can support predictive runway condition assessment. Proof of concept completed successfully.

ACI EUROPE is the European region of Airports Council International (ACI), the only worldwide professional association of airport operators. ACI EUROPE represents over 500 airports in 55 countries. Our members facilitate over 90% of commercial air traffic in Europe. Airports and air connectivity support 14 million jobs, generating €851 billion in European economic activity (5% of GDP). In response to the Climate Emergency, in June 2019 our members committed to achieving Net Zero carbon emissions for operations under their control by 2050, without offsetting.

airport intelligence

Airport Intelligence's goal is simple: using the wealth of knowledge and operational excellence of our expert team, we support airports in achieving their full operational potential. We offer consulting services with a proven set of methodologies, triggering efficient, pro-active and data-driven operations through process optimisation and implementation of TAM, APOC, AOP & A-CDM. Our in-house built AOP solution suite is available for our clients to enable TAM in the most efficient and user-friendly way. We complement our offering with targeted expertise in the development and implementation of Safety Management Systems, Business Continuity Planning & Emergency Management. To ensure the embedding of new ways of working, our experts also offer tailor-made trainings.

JETPACK.AI

Jetpack brings the power of data science and Artificial Intelligence to airports through a suite of products designed to improve decision-making, operational performance and resilience. By combining advanced analytics with deep airport domain expertise, we help airports transform data into actionable insights across forecasting, simulation, optimisation and AI-driven operations. Our solutions enable airports to accurately predict demand and resource requirements, test operational scenarios before implementation, optimise the allocation of people and assets, and deploy intelligent AI tools that support faster, more informed decisions. Built specifically for the airport environment, Jetpack's products empower teams to increase efficiency, enhance passenger experience and unlock measurable value from their data.

EVERY FLIGHT BEGINS AT THE AIRPORT.

WWW.ACI-EUROPE.ORG

@ACI_EUROPE

Produced by ACI EUROPE in cooperation with Airport Intelligence and Jetpack.AI

Printed on recycled paper