Data governance best practices for the AI-ready airport

Received (in revised form): 1st October, 2024

TREVOR STROME

Director, Information Technology, Winnipeg Airports Authority, Canada

Trevor Strome MSc is the Director of Information Technology at Winnipeg Airports Authority, where he leads critical IT functions, including service desk, cyber security and infrastructure and data, analytics and integration. With over 20 years' experience in technology leadership across various public and private sector industries including healthcare and aviation, Trevor has a proven track record of building high-performing data and analytics teams that drive innovation and operational excellence. He is a recognised expert in leveraging data democratisation and advanced analytics to fuel digital business transformation, ensuring that cutting-edge technology solutions align with strategic business objectives. Trevor is the author of the leading textbook *Healthcare Analytics for Quality and Performance Improvement* and has contributed to numerous book chapters and peer-reviewed articles. In addition to his writing, he is a frequent conference presenter, has participated on several airport technology working groups and he teaches several courses on data governance, data strategy and advanced analytics. Trevor's forward-thinking approach consistently empowers organisations to harness the power of technology for measurable, transformative results.

Winnipeg Airports Authority, 249-2000 Wellington Ave, Winnipeg, MB R3H 1C2, Canada
E-mail: tstrome@waa.ca

Abstract

Airports generate vast amounts of data across various systems that are crucial for operational efficiency, safety and enhanced passenger experience. As airports increasingly rely on this data in order to adapt to evolving passenger experience demands, business environments and regulatory requirements, data governance becomes essential for managing, safeguarding and leveraging data effectively. A robust data governance framework provides the structure for ensuring data quality, security and compliance while enabling airports to harness data for artificial intelligence (AI) applications such as predictive maintenance and passenger flow management. By starting with a clear scope, objectives and policies, airports can build a data governance framework that addresses both current needs and future challenges. This paper explores the role of data governance in making airports AI-ready, outlining best practices for implementing a governance programme. It highlights the importance of tools such as data lineage tracking and the need for strong data security measures to comply with regulations such as General Data Protection Regulation (GDPR). The paper also emphasises the need for a culture of accountability, outlining key roles such as data stewards and chief data officers (CDOs) to ensure consistent, robust data management. As AI adoption grows, airports must focus on maintaining data integrity, fostering transparency and ensuring regulatory compliance to unlock the full potential of their data assets while safeguarding privacy and building stakeholder trust.

Keywords

data governance, artificial intelligence, AI, data privacy and security, regulatory compliance

DOI: 10.69554/ZHBT2608

INTRODUCTION

Airports generate and utilise large volumes of data from diverse computer systems and processes essential for ensuring the smooth and efficient movement of aircraft and passengers. Typical airport data ranges from passenger counts and dwell time information to baggage handling statistics, aircraft movements (on-block, off-block, etc.) and cargo volumes. Data is crucial for maintaining operational efficiency, safety and a seamless passenger experience. As airports continue to adapt to evolving regulatory, economic and passenger dynamics, the need for accurate, timely and well-managed data grows ever more important, highlighting the necessity for strong data governance practices to support decisions that increasingly rely on data.

The accelerating adoption of artificial intelligence (AI) in airports offers significant potential to enhance, if not entirely transform, airport operations. AI is 'the simulation of human intelligence processes by machines' and works by 'ingesting large amounts of labeled training data, analyzing that data for correlations and patterns, and using these patterns to make predictions about future states'.[1] AI encompasses the subfields of machine learning (ML) and deep learning (DL) and involves the development of algorithms that 'model the decision-making processes of the human brain, that can "learn" from available data and make increasingly more accurate classifications or predictions over time'.[2] Generative AI (GenAI), which is a form of AI generating a lot of excitement currently, refers to 'deep-learning models that can generate high-quality text, images, and other content based on the data they were trained on'[3] and includes examples such as OpenAI's ChatGPT[4] and Google's Gemini.[5]

By using business intelligence and reporting tools, advanced analytics and AI to leverage their data fully, airports can achieve higher levels of operations excellence, improved situational awareness and predictive maintenance, with the goal of achieving a better overall passenger experience. The reliable use of AI and data-enabled applications, however, heavily depends on the availability, quality and ultimately the governance of the underlying data. Without accurate and reliable data, ensured by strong data governance, the full benefits of AI and other data-driven technologies cannot be realised.

To fully realise the full potential of their data combined with AI, airports must ensure their data governance practices are up to the task of providing the highly reliable data required for these purposes. Effective data governance can help ensure that the large volumes of data generated and used by airports are accurate, secure and well-managed. To that end, this paper explores the role of data governance in preparing airports to be AI-ready and offers practical insights into best practices and key data governance components to help airport management establish a solid data governance framework.

USING DATA AND AI IN AIRPORTS

Airport data is continuously processed from myriad sources including airport systems and external data feeds. The generation, exchange and analysis of this diverse array of data forms the backbone of modern data- (and AI-) driven applications and data-informed decision making required to enable smooth airport operations. For instance, data from baggage handling system data can be used to optimise logistics

and improve overall baggage-handling efficiency. Another example is video analytics, which consumes the feeds from surveillance cameras and helps enhance security by monitoring passenger flow, identifying suspicious behaviour and ensuring compliance with safety regulations. The metadata generated through video analytics can also be used for other purposes, including determining passenger dwell time in locations throughout the terminal during different times of the day.

As mentioned earlier, one promising application of AI in airports is predictive maintenance. Predictive maintenance has 'emerged as a dynamic solution, leveraging data-driven insights and AI algorithms to predict when equipment is likely to fail' and is possible because 'through the analysis of historical and real-time data, AI can identify patterns and anomalies that may indicate potential issues, allowing for timely intervention and maintenance'.[6] This proactive approach to maintenance minimises downtime, reduces maintenance costs and ensures equipment readiness, thereby improving overall reliability and safety.

Another significant application is passenger flow management. Leveraging various predictive analytics techniques, AI-enabled systems can 'forecast peak travel times and suggest optimal staffing levels, ensuring that security and check-in counters are adequately manned to handle the influx of passengers'.[7] This helps optimise staffing levels, reduce congestion and improve queue management at security checkpoints, boarding gates and baggage claim areas. Enhanced passenger flow not only improves the passenger experience but also boosts operational efficiency.

As airports continue to experiment with and deploy systems utilising AI, the creative ways in which this emerging technology is utilised will only continue to expand. With the expansion of airport systems that generate and consume data, the need to ensure high-quality, accurate data is available to these systems (and decision makers) in a timely manner will only continue to increase. This can only be accomplished through effective data governance.

UNDERSTANDING DATA GOVERNANCE IN AIRPORTS

What is data governance?

Data governance is the system an organisation puts into place to 'ensure data is secure, private, accurate, available, and usable' and 'includes the actions people must take, the processes they must follow, and the technology that supports them throughout the data life cycle'.[8] Data governance involves defining who can take what action with what data, under what circumstances, using which methods, and 'aims to ensure data integrity, availability, and security, and provides a structured approach to data management that aligns with the organisation's goals and regulatory requirements'.[9] By establishing clear rules and responsibilities, data governance helps organisations maximise the value of their data while minimising risks related to data breaches, inaccuracies and misuse.

Benefits of data governance

Implementing and maintaining a robust data governance programme can, in general, bring numerous benefits to an airport. Data governance enhances airport data quality, ensuring that data is accurate, consistent and reliable, which

is essential for improving operational efficiency, supporting effective decision making and enabling data-driven strategic planning. Data governance also strengthens data security and privacy by establishing protocols for data access and handling, reducing the risk of data breaches and helping ensure compliance with regulatory requirements. This helps to build trust with stakeholders and ultimately with passengers, who can be confident that their data is handled responsibly. After all, data breaches in the aviation industry[10] only serve to erode stakeholders' and the public's trust in the privacy of their information.

Additionally, data governance helps promote both transparency and accountability within an airport organisation. By clearly defining data ownership and responsibilities for data, data governance helps foster a culture of accountability, where individuals are aware of and embrace their roles in maintaining data quality and security. This clarity helps eliminate the data silos often present with airport systems and enables increased collaboration across departments. This 'big picture' view of an airport's data assets leads to more integrated and effective data management. Ultimately, data governance supports the organisation's overall goals by ensuring that data is leveraged to its fullest potential while safeguarding against risks.

IMPLEMENTING DATA GOVERNANCE IN ORGANISATIONS

Data governance framework

Implementing data governance within an airport organisation involves several key steps. One of the first steps is to identify and establish a data governance framework suitable to your organisation. A well-defined framework ensures that data is handled consistently and responsibly, which is critical for maintaining data integrity, security and compliance. A data governance framework usually:[11]

- Consists of rules, processes and role delegations;
- Covers strategic, tactical and operational roles and responsibilities;
- Ensures data is trusted, well documented and easy to find;
- Helps keep data secure, compliant, private and confidential.

A data governance framework serves to define the scope, objectives and key data governance components such as policies, procedures, roles and responsibilities and technology supports (see Table 1). The data governance framework should align with and support your organisation's strategic goals and regulatory requirements.

Rather than starting from scratch, airports can start with resources such as the Data Governance Institute,[12] Data Management Body of Knowledge (DMBOK)[13] and Control Objectives for Information and Related Technology (COBIT)[14] to guide the development and implementation of an effective data governance framework for your airport.

Scope and objectives

The data governance scope outlines the boundaries and focus areas for managing airport data assets. It defines all types of data collected, processed, stored and used across various departments. For instance, data generated from all corporate and airport operating systems might be identified as in-scope, while data from third-party vendors that is not directly integrated into airport systems could be

Table 1 Key components of data governance framework

Component	*Description*
Scope	Defines the boundaries of the data governance programme, including the types of data covered, the departments involved and the specific data processes addressed.
Objectives	Specifies the goals of the data governance initiative, such as improving data quality for AI applications, ensuring data security and maintaining compliance with regulations. Clearly aligns with the organisation's operational and business development objectives.
Policies and procedures	Provides comprehensive guidelines and step-by-step instructions for governing data activities, including data collection, storage, processing, access, sharing and security practices.
Roles and responsibilities	Identifies and assigns specific roles such as data stewards, data custodians and data owners, detailing their duties in maintaining data quality, security and compliance.
Tools and technologies	Identifies the software and platforms used to support data governance activities, including data cataloguing, data quality assessment and security monitoring.
Metrics and key performance indicators (KPIs)	Defines the key performance indicators and metrics used to measure the success and effectiveness of the data governance initiatives.

considered out-of-scope (once again, depending on the goals and objectives of your data governance programme). Overall, the scope specifies which data domains are covered, the processes involved and the stakeholders responsible for data management.

The data governance programme objectives clarify the goals the organisation aims to achieve through its data governance efforts. These goals generally include improving data quality, ensuring data security, maintaining compliance with regulations and facilitating data-driven decision making. Objectives guide the strategic direction and priorities of the data governance programme, ensuring that they align with the airport's overall mission and goals relating to business development and operational objectives. By defining clear scope and objectives, the data governance programme ensures that all relevant data-related activities fall under a unified governance framework to maintain consistency, control and strategic alignment across the organisation.

Policies and procedures

Implementing data governance within an airport 'promotes the availability, quality, and security of an organisation's data through different policies and standards' and 'these processes determine data owners, data security measures, and intended uses for the data'.[15] Policies and procedures should cover data quality management, data security, data privacy, data life cycle management and other key data governance support aspects. Training and educating employees on data governance policies and their roles in data governance is necessary to ensure adherence and foster a data-centric culture within the organisation.

It is important for an organisation to avoid spending excessive time creating policy documents that merely end up unused and collecting dust. Instead, the focus should be on developing a few

high-impact, practical policies that can be effectively implemented and enforced. Some critical policies that would benefit airport data governance initiatives include:

- *Data quality policy*: Ensures that data is accurate, complete, consistent and timely. High-quality data is crucial for making reliable business decisions, supporting operational efficiency and maintaining the integrity of AI models.
- *Data security and privacy policy*: Protects sensitive information from unauthorised access, breaches and misuse. This policy is vital for complying with legal and regulatory requirements, safeguarding personal data and maintaining trust with stakeholders.
- *Data access and usage policy*: Defines who can access data, under what conditions, and how it can be used. This policy helps prevent data misuse, ensures compliance with ethical standards, and facilitates the responsible sharing of data within and outside the organisation.
- *Data management policy*: This policy ensures that data management practices over the entire data life cycle are consistent and aligned with organisational goals and regulatory requirements, promoting efficient and secure handling of data throughout its life cycle.

By establishing these key policies and procedures, airports can ensure that data is accurate, reliable and available when needed, supporting both day-to-day operations and strategic decision making.

Roles and responsibilities

A key component of a data governance framework is the clear definition of roles and responsibilities based on the needs of the organisation and scope of the data governance programme. Assigning specific roles ensures accountability for various aspects of data management helps prevent data silos, promotes collaboration and ensures that all data-related tasks are properly managed and executed. Common roles and responsibilities in supporting data governance within an organisation[16] are outlined in Table 2.

Table 2 Data governance roles and responsibilities

Role	*Description*
CDO/data governance officer (DGO)	Provides strategic leadership for the data governance programme, including policy development and compliance oversight. Acts as a liaison between departments to promote data governance and a data-driven culture.
Data owner	Accountable for the management and oversight of specific data domains, ensuring data quality, integrity and availability.
Data steward	Executes day-to-day data governance activities, ensuring data classification, quality, documentation and protection.
Data custodian (data administrator)	Ensures the accessibility and reliability of data systems, manages technical infrastructure and implements data security measures.
Data user	Utilises information and insights derived from data to achieve organisational goals while adhering to governance policies, plays a key role in decision making and operational improvements.

Defining roles and responsibilities in data governance is crucial for making an airport more AI-ready. Clear delineation of tasks ensures that data is consistently managed, protected and utilised effectively, which is vital for the accuracy and reliability of AI applications. By establishing accountability, data quality is maintained, data security is reinforced and regulatory compliance is assured, all of which are essential for building trust and preventing legal issues. This structured approach creates a robust foundation for integrating AI technologies and available data to improve airport operations and passenger experiences.

Tools and technology

To enhance the effectiveness and efficiency of data governance, the use of data governance-related tools and technology helps to streamline processes and reduce manual effort. For example, implementing a data catalogue tool helps create a comprehensive inventory of data assets, enabling better data discovery and management. This facilitates the identification of data sources, lineage and usage, which is crucial for maintaining data integrity and compliance.[17] Data quality assessment tools automate the detection and correction of data errors, inconsistencies and redundancies, ensuring that high-quality data is consistently available for decision making and operational processes.[18,19] Data security tools provide robust mechanisms for protecting sensitive information. These tools include encryption, access controls and real-time monitoring, which help safeguard data from unauthorised access and reduce the risk of data breaches.

By automating routine and repetitive tasks such as data validation, monitoring and reporting, data governance tools help free up human resources to focus on more strategic, high-value activities. This not only increases efficiency but also reduces the likelihood of human error, thereby enhancing overall data governance compliance.

Metrics and KPIs

To effectively measure the impact of data governance, airports must establish clear metrics, KPIs and objectives and key results (OKRs). Metrics such as data accuracy, operational efficiency and regulatory compliance provide quantitative assessments of improvements in data quality and adherence to legal standards. KPIs, including the rate of data errors, level of data completeness and number of compliance violations, offer specific targets that gauge the success of data governance initiatives.[20] OKRs further drive performance by setting target goals, such as decreasing data processing time, eliminating data breaches and increasing user satisfaction rates. These measures collectively ensure that data governance efforts are aligned with the airport's strategic objectives, enhancing overall operational efficiency, security and readiness for AI-driven innovation.

REGULATORY COMPLIANCE

A data governance framework can help airports comply with regulatory requirements and industry standards. Such regulations (which vary across regions) impose guidelines on how personal data should be collected, processed and stored. For example, they may mandate that organisations obtain explicit consent from individuals before processing their data and ensure that individuals have the right to access, rectify or delete

their personal data. Non-compliance with such regulations often results in severe penalties, making it imperative for airports to establish comprehensive data governance practices that adhere to these regulations. Examples of such regulations include:

- General Data Protection Regulation (GDPR) (Europe).[21]
- Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada).[22]
- In the US, the California Consumer Privacy Act (CCPA)[23] and a patchwork of other state-level regulations set requirements for data privacy and protection.

In general, these regulations emphasise the importance of data transparency, giving individuals more control over their personal information and imposing significant penalties for data breaches.

The implications of these regulations on AI use in airports are substantial. AI models rely on very large amounts of data to learn and make predictions. Compliance with their applicable data protection laws means that airports must ensure the data used for creating or 'tuning' AI applications is collected and processed lawfully, with proper consent and transparency. These important steps include anonymising personal data to protect individual privacy and implementing robust security measures to prevent data breaches.

One challenge with anonymisation of data is that 'anonymized personal data can easily be de-anonymized by AI' and that 'researchers have found there is minimal anonymity in even coarse data sets', resulting in a high degree of reidentification.[24] 'Privacy by design' is an approach that integrates privacy protections into AI technologies from the very start, ensuring that data privacy is built into systems rather than added later. This proactive strategy can help safeguard individual rights and prevents risks such as biased decision making and unauthorised access to personal data.[25]

A well-structured data governance framework helps navigate these complexities, ensuring that AI applications are both effective and compliant with data protection regulations, ultimately enhancing operational efficiency, security and passenger satisfaction.

DATA MANAGEMENT AND DATA QUALITY

Implementing best practices for managing and accessing data in airports helps ensure the effective use of AI and other data-intensive applications. One fundamental practice is establishing clear data governance policies that define how data should be managed throughout its life cycle, including data collection, storage, processing, sharing and destruction. These policies need to be aligned with regulatory requirements and industry standards as well as airport requirements to ensure compliance and to protect sensitive information.

Data life cycle management

Data life cycle management (DLM) is 'an approach to managing data throughout its life cycle from data entry to data destruction'.[26] The data life cycle includes several key stages: data creation and collection, data storage, data usage, data sharing, data archiving and data destruction (see Table 3). Each stage requires specific practices and controls to ensure data integrity, security and compliance. Properly managing each stage

Table 3 Data management life cycle

Stage	*Description*
Data creation and collection	Data is generated from various sources such as airport operating database systems and security checkpoints.
Data storage	Data is securely stored in databases or data warehouses with protections against unauthorised access.
Data usage	Data is analysed and processed to derive insights and support decision making.
Data sharing	Data is shared across departments and stakeholders with controlled access permissions.
Data archiving	Data is stored long-term for compliance and future reference.
Data destruction	Obsolete or redundant data is securely deleted to prevent unauthorised access or misuse.

of the data life cycle helps maintain high data quality and supports the effective use of AI and other data-driven applications.

In the data creation and collection stage of the life cycle, data is generated from various sources such as the airport operational database (AODB), baggage handling systems (BHS) and security checkpoint scans. Ensuring the accuracy and completeness of data at this stage is crucial. Once collected, data is stored in secure databases or data warehouses, where it must be protected against unauthorised access and breaches. The data usage stage involves analysing, processing and otherwise using data to derive insights, support decision making and trigger action. Data sharing allows different departments, stakeholders and systems to access and use the data while maintaining control over who (or what system) can access and/or modify it. Data archiving involves storing data long-term for compliance and future reference, while data destruction ensures that obsolete or redundant data is securely deleted to prevent unauthorised access or misuse.

Data quality

Data quality is 'the degree to which data meets a company's expectations of accuracy, validity, completeness, and consistency'.[27] Maintaining high data quality and integrity is necessary for creating and effective functioning of AI applications, and for overall airport operations in general. High-quality data is required to develop and/or tune AI models to produce accurate and reliable outputs (such as predictions or recommendations), which are used to assist with decision-making processes. Poor data quality, on the other hand, can lead to incorrect insights, operational inefficiencies and increased risks.

To achieve high data quality, airports must implement a range of strategies and controls including comprehensive data quality standards and metrics. These should cover the basic dimensions of data quality, such as accuracy, completeness, consistency, timeliness and validity.[28,29] Although these data quality dimensions are not universally agreed upon, Table 4 provides definitions for the most commonly used data quality dimensions.

Leveraging technology is helpful for maintaining data quality and integrity. Implementing advanced data management platforms that offer features such as data profiling, data lineage tracking, data cleansing and data enrichment can significantly enhance

Table 4 Data quality dimensions and definitions

Data quality dimension	*Definition*
Data completeness	Measures the proportion of complete data in the dataset, indicating the presence of missing values.
Data accuracy	Assesses the correctness of data by measuring the extent to which the data values match the true values, thereby ensuring that the data describes the real world.
Data consistency	Evaluates the uniformity of data across different data sources or within the same dataset.
Data validity	Measures the proportion of data that adheres to predefined data rules and constraints.
Data freshness/timeliness	Assesses how up-to-date the data is by measuring the time elapsed between data capture and data availability.
Data uniqueness	Measures the proportion of unique records in a dataset, helping to identify and eliminate duplicates.

data quality.[30] These platforms can automate many of the processes involved in maintaining data quality, making it easier to manage large volumes of data efficiently. Regular data quality assessments, real-time monitoring and alerts and periodic data quality audits can help identify and address issues promptly, ensuring that the data remains reliable and fit for use. Additionally, using AI and ML algorithms to continuously monitor and improve data quality can help airports stay ahead of potential issues and ensure data accuracy and robustness. Finally, data stewards help ensure that data governance policies are followed and that any data-related issues are promptly addressed.

Data security and privacy

In the context of AI and airport data governance, robust data security and privacy measures are essential. Airports handle large amounts of potentially sensitive data ranging from private information of passengers, customers and employees to security footage and critical operational details. This type of data is essential for various AI-driven applications; however, its sensitive nature makes it a prime target for cyber-attacks and data breaches, necessitating stringent security and privacy measures to protect it.[31]

Robust data security measures begin with implementing comprehensive access controls. This involves ensuring that only authorised personnel have access to sensitive data and that their access is limited to what is necessary for their roles. Role-based access control (RBAC) and multi-factor authentication (MFA) are essential tools in this regard, helping to prevent unauthorised access to and changing of data, and reducing the risk of breaches and possible data exfiltration.[32,33] RBAC limits access based on user roles within an organisation, while MFA requires multiple forms of verification to confirm user identity. Regular monitoring and frequent auditing of data access and real-time alerting are essential for identifying and mitigating potential security risks before they escalate.

Encryption is another critical component of data security. By encrypting data both at rest and in transit, airports can protect sensitive information from being intercepted or accessed by

malicious actors. Advanced encryption standards such as AES with a 256-bit key (AES-256)[34] can be employed to safeguard data, ensuring that even if it is compromised, it remains unreadable and unusable. Additionally, implementing secure communication protocols such as transport layer security (TLS)[35] for data transmission further enhances data protection, especially when sharing information between different systems and stakeholders.

Data privacy measures are equally important, especially given the stringent regulations governing personal data. Compliance with regulations previously mentioned such as GDPR, PIPEDA and CCPA (depending on jurisdiction) requires airports to implement policies and practices that protect individuals' privacy rights. Such policies and practices may include measures such as obtaining explicit consent for data collection, fostering transparency about data usage, and ensuring that individuals can exercise their rights to access, rectify or delete their personal data.

To address the challenges related to the potential reidentification of anonymised data, researchers are developing privacy-preserving AI techniques including federated learning and homomorphic encryption. These methods allow models to be trained on decentralised or encrypted data without exposing the underlying raw information. In federated learning, the model is trained across multiple systems that retain local data, sharing only model updates rather than the actual data itself. Homomorphic encryption enables computations on encrypted data, allowing AI models to analyse and learn from it while keeping the data secure. These approaches ensure that AI can identify patterns and improve performance while maintaining privacy standards and complying with regulations.[36,37]

In addition to these technical measures, fostering a culture of security awareness within an airport organisation helps maintain data security and information privacy. Regular training and education programmes can help employees understand the importance of data security and privacy, recognise potential threats and follow best practices to protect sensitive information. This proactive approach helps ensure that everyone in the organisation is aligned with the goal of maintaining robust data security and privacy.

Ethical considerations often come into play when managing sensitive data and utilising AI in airport operations. As AI systems become more embedded in the daily functioning of airports, ensuring their responsible use is essential to maintain fairness, transparency and trust. One significant ethical concern, for example, is the potential for bias in AI algorithms, which is 'the occurrence of biased results due to human biases that skew the original training data or AI algorithm'.[38] Bias can stem from training AI models on unrepresentative or skewed data, leading to discriminatory outcomes that unfairly disadvantage certain groups of people. For example, a report from the National Institute of Standards and Technology (NIST) found that certain facial recognition algorithms have higher false positive rates for Asian and African American faces compared to Caucasian faces.[39] This means that travellers from these groups could potentially be more likely to be incorrectly identified or flagged for additional screening, leading to delays and potentially stressful experiences. Addressing bias requires rigorous efforts to ensure that AI algorithms and their training datasets are diverse and

inclusive,[40] reflecting the broad spectrum of passengers and scenarios encountered in airport environments.

Establishing robust 'Responsible AI' guidelines and oversight mechanisms as part of an airport's data governance programme is essential for maintaining ethical standards in AI applications. This could include forming an ethics committee or board to review and guide AI projects, ensuring such projects adhere to the ethical principles of fairness, accountability and transparency. Continuous monitoring and evaluation of AI systems is necessary to ensure they operate as intended and do not evolve in ways that could lead to irresponsible and unethical outcomes. By prioritising ethical considerations, airports can leverage AI technologies responsibly, ensuring that their use enhances operations without compromising the rights and trust of passengers and stakeholders.

Overall, robust data security and privacy measures are crucial to protect the sensitive data managed by airports. These measures ensure regulatory compliance and build trust with passengers, employees and other stakeholders, enhancing the effectiveness of AI applications and airport operations. By prioritising data security and privacy, airports can confidently leverage AI technologies, knowing their data is safeguarded against potential threats and implemented ethically.

FUTURE OUTLOOK

As airports adopt advanced technologies that generate and consume large volumes of data, robust data governance programmes will become increasingly essential. Advancements in AI and ML will enable real-time data analysis, allowing for more proactive and adaptive management of airport resources. This capability will streamline and enhance operations, from passenger flow management to predictive maintenance. Airports must actively maintain their data governance practices to address new threats and challenges, fostering a culture of accountability and continuous improvement. This shift will require ongoing education and training to keep all employees informed about best practices and the importance of data governance.

In conclusion, the future of data governance in AI-ready airports will be dynamic and transformative. Embracing real-time analytics, prioritising data privacy and security and fostering strong governance roles will help airports navigate modern data management complexities. These efforts will keep them at the forefront of technological advancements, enhancing operational efficiency and improving the passenger experience.

References

(1) Craig, L., Laskowski, N. and Tucci, L. 'What is AI? Artificial Intelligence explained', TechTarget, available at https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence (accessed 1st October, 2024).
(2) IBM, 'What is artificial intelligence (AI)?', available at https://www.ibm.com/topics/artificial-intelligence (accessed 1st October, 2024).
(3) IBM, 'What is generative AI?', available at https://research.ibm.com/blog/what-is-generative-AI (accessed 1st October, 2024).
(4) ChatGPT, available at https://chat.openai.com/ (accessed 1st October, 2024).
(5) Gemini, available at https://gemini.google.com/ (accessed 1st October, 2024).
(6) Megasis Network (March 2024), 'AI and Predictive Maintenance: Keeping Machines Healthy', Medium, available at https://megasisnetwork.medium.com/ai-and-predictive-maintenance-keeping-machines-healthy-99ec76731a8c (accessed 1st October, 2024).

(7) Petrie, J. (April, 2024), 'Airports Must Embrace AI for Enhanced Passenger Experience', Aviation Pros, available at https://www.aviationpros.com/airports/article/55000105/airports-must-embrace-ai-for-enhanced-passenger-experience (accessed 1st October, 2024).
(8) Google, 'What is Data Governance', available at https://cloud.google.com/learn/what-is-data-governance (accessed 1st October, 2024).
(9) Stedman, C., 'What is data governance and why does it matter?', available at TechTarget, https://www.techtarget.com/searchdatamanagement/definition/data-governance (accessed 1st October, 2024).
(10) Saraogi, V. (July 2019), 'Five times airports were involved in cyberattacks and data breaches', Airport Technology, available at https://www.airport-technology.com/features/five-times-airports-were-involved-in-cyberattacks-and-data-breaches/?cf-view (accessed 1st October, 2024).
(11) Qlik, 'Data Governance', available at https://www.talend.com/resources/data-governance-framework/ (accessed 1st October, 2024).
(12) Data Governance Institute (DGI), 'DGI Date Governance Framework', available at https://datagovernance.com/the-dgi-data-governance-framework/ (accessed 1st October, 2024).
(13) DAMA International, available at https://dama.org/ (accessed 1st October, 2024).
(14) Patil, P. (April 2024), 'Data Governance Framework: A Comprehensive Guide to COBIT Implementation', Medium, available at https://medium.com/@parth.patil20/data-governance-framework-a-comprehensive-guide-to-cobit-implementation-97e06eca779a (accessed 1st October, 2024).
(15) IBM, 'What is data governance?', available at https://www.ibm.com/topics/data-governance (accessed 1st October, 2024).
(16) Analytics8 (July 2024), 'Defining Data Governance Roles and Responsibilities', available at https://www.analytics8.com/blog/defining-data-governance-roles-and-responsibilities/ (accessed 1st October, 2024).
(17) Lawton, G., '18 top data catalog software tools to consider using in 2024', available at https://www.techtarget.com/searchdatamanagement/feature/16-top-data-catalog-software-tools-to-consider-using (accessed 1st October, 2024).
(18) Casalinuovo, V. and Kiviranta, P., 'What are the best tools and methods for data quality assessment and improvement?', LinkedIn, available at https://www.linkedin.com/advice/0/what-best-tools-methods-data-quality-assessment (accessed 1st October, 2024).
(19) IBM, 'IBM Databand', available at https://www.ibm.com/products/databand (accessed 1st October, 2024).
(20) Foote, K. D. (April 2024), 'Data Governance Metrics: How to Measure Success', Dataversity, available at https://www.dataversity.net/data-governance-metrics-how-to-measure-success/ (accessed 1st October, 2024).
(21) European Union (EU), 'Complete guide to GDPR compliance', available at https://gdpr.eu/ (accessed 1st October, 2024).
(22) Office of the Privacy Commissioner of Canada, 'The Personal Information Protection and Electronic Documents Act (PIPEDA)', available at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/ (accessed 1st October, 2024).
(23) State of California Department of Justice (March 2024), 'California Consumer Privacy Act (CCPA)', available at https://oag.ca.gov/privacy/ccpa (accessed 1st October, 2024).
(24) Booz, Allen, Hamilton, '4 Ways to Preserve Privacy in Artificial Intelligence', available at https://www.boozallen.com/s/solution/four-ways-to-preserve-privacy-in-ai.html (accessed 1st October, 2024).
(25) Pandectes (July 2023), 'Data Privacy and Artificial Intelligence (AI)', available at https://pandectes.io/blog/data-privacy-and-artificial-intelligence-ai/ (accessed 1st October, 2024).
(26) IBM, 'What is a data lifecycle management (DLM)?', available at https://www.ibm.com/topics/data-lifecycle-management (accessed 1st October, 2024).
(27) Suer, M. (September 2023), 'What is Data Quality and Why is is Important?', Alation, available at https://www.alation.com/blog/what-is-data-quality-why-is-it-important/ (accessed 1st October, 2024).
(28) Gwande, S., '6 Dimensions of Data Quality, Examples, and Measurement', iceDQ, available at https://icedq.com/6-data-quality-dimensions (accessed 1st October, 2024).
(29) Collibra (October 20213), 'The 6 data quality dimensions with examples', available at https://www.collibra.com/us/en/blog/the-6-dimensions-of-data-quality
(30) Lawton, G., 'Evaluate and choose from the top 10 date profiling tools', TechTarget, available at https://www.techtarget.com/

searchdatamanagement/tip/Evaluate-and-choose-from-the-top-data-profiling-tools (accessed 1st October, 2024).
(31) Beumer Group, 'Airport Cybersecurity: Safeguarding Against Today's Threats', available at https://www.beumergroup.com/knowledge/airport/cybersecurity-for-airports-safeguarding-against-todays-threats (accessed 1st October, 2024).
(32) Tools4Ever, 'Role-Based Access Control (RBAC)', available at https://www.tools4ever.com/solutions/role-based-access-control/ (accessed 1st October, 2024).
(33) Panyam, S., Bhattacharya, S. and Gujar, P. (March 2024), 'Role-Based Multi-Factor Authentication', DZone, available at https://dzone.com/articles/role-based-multi-factor-authentication (accessed 1st October, 2024).
(34) GeeksforGeeks, 'Advanced Encryption Standard (AES)', available at https://www.geeksforgeeks.org/advanced-encryption-standard-aes/ (accessed 1st October, 2024).
(35) Cloudflare, 'What is TLS (Transport Layer Security)?', available at https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/ (accessed 1st October, 2024).
(36) Thaine, P. (January 2020), 'Perfectly Privacy-Preserving AI', Medium, available at https://towardsdatascience.com/perfectly-privacy-preserving-ai-c14698f322f5 (accessed 1st October, 2024).
(37) Rathnayake, D. (May 2024), 'Ensuring Privacy in the Age of AI: Exploring Solutions for Data Security and Anonymity in AI', Tripwire, available at https://www.tripwire.com/state-of-security/ensuring-privacy-age-ai-exploring-solutions-data-security-and-anonymity-ai (accessed 1st October, 2024).
(38) IBM, 'What is AI bias?', available at https://www.ibm.com/topics/ai-bias (accessed 1st October, 2024).
(39) National Institute of Standards and Technology (NIST) (December 2019), 'NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software', available at https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software (accessed 1st October, 2024).
(40) Manyika, J., Silberg, J. and Presten, B. (October 2019), 'What Do We Do About the Biases in AI?', Harvard Business Review, available at https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai (accessed 1st October, 2024).