Library Management

Navigating through information governance turbulences at an air traffic management company in South Africa

Refiloe Mabaso
Air Traffic and Navigation Services SOC Ltd, Kempton Park, South Africa and Department of Information Science, University of South Africa – Muckleneuk Campus, Pretoria, South Africa, and
Mpho Ngoepe
Department of Library and Information Services, University of South Africa – Muckleneuk Campus, Pretoria, South Africa

Received 18 May 2025
Revised 15 May 2026
Accepted 24 June 2026

Abstract

Purpose – The implementation of information governance ensures that the organisation meets legal compliance, builds institutional memory, and makes decisions based on trusted information. However, in many organisations, facets of information governance exist but are managed by different units without a coordinated effort, resulting in duplication and overlapping roles. The purpose of this study was to explore information governance practices at an air traffic management company in South Africa.

Design/methodology/approach – This qualitative study, anchored in the interpretivist research paradigm, used purposive sampling to select participants from Air Traffic and Navigation Services (ATNS) employees at various levels within the organisation. Qualitative data were collected through interviews and document analysis.

Findings – The main finding was that some information governance facets, such as records management, knowledge management, and business intelligence, are already in place within ATNS but operate in different units. It is recommended that the organisation defines the role(s) with key strategic and operational responsibilities for implementing information governance.

Research limitations/implications – The limitations of this study relate to the overreliance on IT personnel responses, which may have introduced a degree of bias, potentially skewing the findings towards a technology-centric perspective of information governance.

Practical implications – This study adds value to the existing theoretical and conceptual issues that constitute the ongoing discourse on information governance at the organisational and national levels in developing countries.

Originality/value – The study contributes empirically to the limited body of knowledge on information governance within the aviation sector. It proposes an information governance framework that, if implemented, may address organisational fragmentation, ensure that the organisation meets legislative requirements and accountability, and make information assets easily accessible for decision-making.

Keywords Information management, Information governance, Air traffic and navigation service, Information technology, Records management, Knowledge management

Paper type Research article

Introduction and background to the study

Developments in information governance have led to renewed interest in various aspects of records management, information management, knowledge management, freedom of information, e-discovery, and information privacy worldwide (Mullon and Ngoepe, 2019).

Library Management
Emerald Publishing Limited
e-ISSN: 1758-7921
p-ISSN: 0143-5124
DOI 10.1108/LM-05-2025-0070

Globally, there is a consensus that regards information within the possession of organisations as invaluable assets, processes, or knowledge. Smallwood (2014a) defines information governance as a concept of information management based on evidence-based policies with the aim of minimising costs, reducing risk, and towing the regulatory and legal lines. Information needs to be managed effectively and efficiently so that the organisation can achieve success and be sustainable in the competitive business world (Rocha-Bello-Bertin, 2019). Progressive international governments recognise the significant obligation that rests upon organisations as information stewards. Hence, legislation and regulations are developed to facilitate the practice of good information governance (MacLennan, 2014). Sadly, this cannot be said about organisations in developing countries such as South Africa.

For example, Mullon and Ngoepe (2019) are of the view that coherent and integrated information governance, as an ideal, has not been achieved by organisations, let alone some countries in the world. The failure to achieve the aforementioned ideal could be attributed to the fact that information governance has not yet been clearly defined or practised in the global south. As a result, in most organisations, information governance is fragmented into different units such as records management, information management, enterprise content management, privacy (data protection), freedom of information, corporate governance, information risk, information security, and e-discovery. Several scholars, such as Iannarelli and O'Shaughnessy (2014), Lomas (2010), and Ngoepe (2014), point out that the implementation of information governance in organisations provides an opportunity to define and streamline processes and activities in organisations around the world to create a coherent body of knowledge. Its elements include, but are not limited to, records management, information management, enterprise content management, privacy (data protection), freedom of information, corporate governance, and corporate social responsibility.

Similarly, Hagmann (2013) found that although information governance has been universally accepted and embraced by its practitioners, there is a relative immaturity in the definition of corresponding concepts and theories, coupled with practical experience in the field. Other factors that contribute to non-coherence and non-integration in information governance include power dynamics at play in various organisations. More recent evidence, including that of Maurel and Zwarich (2021), suggests that in some circumstances, records managers, librarians, and archivists, who are deemed crucial organisational actors in the information governance sector, do not play an influential and strategic role in determining policies and implementation strategies. Therefore, the resultant gap in roles and competencies contributes to the disjointed information governance.

Previous studies, such as MacLennan (2014) and Bennett (2017), have highlighted that information governance constitutes activities that practitioners have developed in their attempts to manage the utilisation of information in accordance with the law. Bennett (2017) views information governance as the outlining of decision rights and the process of conferring accountability to those who have been delegated authority in the information area of expertise. Information governance, as an organisational function and strategy, is developed to guarantee legally compliant conduct in the design, utilisation, assessment, archiving, and disposal of information that is in the possession of the organisation. Kogi *et al.* (2025) put information governance as a subset of corporate governance.

The information governance processes are underpinned by strategies, guidelines, operational procedures, criteria of standards, and levels of accountability that facilitate the optimal use of information in the attainment of organisational goals and provide support to the organisation to perform optimally (Gartner, 2009). This means that every activity that pertains to data and information in the organisation must be streamlined under information governance auspices. Lederman (2012) supports this notion by stating that information governance must be treated as an intentional strategic function that incorporates benchmarks, procedures, responsibility roles, and assessment indices. This framework must include clearly spelt out job specifications that inspire and keep practitioners liable to develop, structure, protect, manage,

and safely delete information in line with the vision and mission of organisations. The noble principles mentioned often accompany new disciplines, but they are not without defects.

As an emerging discipline, Smallwood (2014a) frames information governance like other technical sectors, which often encounter various challenges in the form of design weaknesses and liabilities that can lead to potentially serious organisational costs if information governance policies are not properly designed and observed. The consequences resulting from an oversight of information governance regulation and enforcement are best demonstrated in a universally well-known example where, as Smallwood (2014b, p. 9) points out, a theft of confidential United States National Security Agency documents was committed by Edward Snowden in 2013. This lapse could have been avoided by means of watertight confidentiality processes and enforcement regimes.

Several governments around the world are faced with information governance related challenges that are best illustrated by Australia, which is focusing on mitigating its critical information threats. In December 2015, the Australian Government released its Public Data Policy Statement as part of the National Innovation and Science Agenda. The main aims of Australia's national mission remained to accord governmental data and its national strategic resource status that constitutes a significant value for economic advancement, enhance national service implementation, and improve policy outcomes (dama.org 2020). Australia ratified the Digital Continuity Policy 2020 with the specific aim of supporting the digital transformation strategy for all government agencies. The policy states that government information and data must be valued as a national treasure, thereby managed as an asset by all government agencies, certifying that it is deliberately designed, applied, and secured for the duration that is beneficial to the government's official requirements, as previously asserted by Bennett (2017).

Similarly, Allen and Allison (2018) showed that the United States of America's Federal Government regards information governance as a framework that facilitates strategic decision-making, systematically records departmental activities, and supports governmental units to comply with statutory and regulatory decrees. This practice is standardised and consistent with all federal records, as created and consented to in the Memorandum of Understanding (MOU) for the Heads of Executive Departments and Agencies that was endorsed and sanctioned by President Obama in 2012. The memorandum authorises an array of modernisation measures, which also include the decommissioning of paper and the transition of all government transactions to electronic formats.

Mullon and Ngoepe (2019) highlight that the South African government exhibits the classical tendencies of a developing country, wherein sections of the information governance are fragmented, and separate state agencies are delegated to implement the distinct responsibilities of the information governance as a whole. For instance, the Information Regulator in South Africa is responsible for access to information and privacy, whereas the National Archives and Records Service (NARS) is solely focused on regulating records management in governmental bodies. Another information and data agency in the South African government is the State Information Technology Agency (SITA), which solely oversees Information Technology (IT) apart from other related agencies. This shows the fragmentation of the responsibility for information governance in South Africa at the national level. This situation is perpetuated further at the organisational level; hence, this study sought to explore information governance at an air traffic company in South Africa. While these aspects are fragmented at an organisational level, their related dependence is important for successful information governance. The absence of structure among these functions not only leads to operational inefficiencies but also weakens organisational accountability and alignment with strategic goals.

Contextual setting

The contextual setting of this study is an Air Traffic and Navigation System (ATNS) company that is governed by South Africa's legislative and administrative framework in order to plan,

manage, and operate safe and efficient airspace services. The South African government, through the Ministry of Transport, is the sole shareholder, according to ATNS Act No. 45 of 1993. ATNS operates in a highly regulated environment governed by national and international regulators, policies, and standards (ATNS, 2019). The company was founded in 1993 under the Air Traffic and Navigation Services Company Act, 1993 (Act No. 45 of 1993), to provide air traffic management solutions and associated services on behalf of the South African government, in accordance with the International Civil Aviation Organisation (ICAO) Standards and Recommended Practices (SARPs) and South African Civil Aviation Authority (SACAA) Regulations and Technical Standards (ATNS, 2019). SARPs are designed to help states manage aviation safety risks in collaboration with their service providers. The growing complexity of the global air transportation system and interconnected aviation activities necessitate a strong assurance of aircraft safety, support for safety management provisions, and proactive strategy development to improve safety performance (ICAO.int 2020). For ATNS to provide safe and efficient air traffic management solutions, it requires, among others, the implementation of an information governance framework. In performing its mandate, ATNS produces a volume of information that supports projects, financial activities, and other functions of the organisation. The information needs to be governed properly from creation to disposal according to the required information and archival legislation, as well as international best practices. Failure or inadequacies in governing information can expose ATNS to potential risks related to legal and regulatory obligations, continuity of business operations, and accountability to shareholders. As ATNS has a unique mandate, it was necessary to establish information governance within the organisation with the view to developing a framework that can serve as best practice within the aviation industry. Although entities within the industry fall under the auspices of information legislation in South Africa, they are often neglected and left on their own, while more focus is on municipalities and government departments. The findings may provide insight for the organisation to be on par with international best practices, attain clean audits and maintain accreditation from the International Standards Organisation.

Problem statement

The fragmented state of South Africa's information and data agencies hurts the application of information governance and related statutory outcomes within individual organisations. As a result, roles overlap and clash, and task repetition becomes commonplace, to the detriment of the organisation. According to Ngoepe (2016), it is not uncommon for some state agencies to never find a specific official who is accountable for information access. A functional and effective integrated information governance framework at ATNS would ideally enable an organisation to effortlessly comply with legal precepts while also establishing a supportive environment for employees to handle and manage information as an organisational asset. In line with Mullon and Ngoepe's (2019) observation, this study identified a challenge at ATNS: the lack of a clearly defined information governance framework that outlines a comprehensive structure for managing information and implementing policies, processes, roles, and responsibilities.

As Ngoepe (2014) discovered in South African public sector organisations, information governance facets are fragmented and operate in silos. Anecdotal evidence suggests that information management and governance are fragmented within ATNS, with information governance facets and principles managed in disjointed units with no clearly defined job spheres and descriptions. At ATNS, for example, the legal department handles all external information requests while the IT department handles internal information requests and information administration. Effectively, there is a notable lack of centralised integrated policies, procedures, standards, defined office capacity, and strategic directives to guide ATNS in the management and governance of information at various levels of the organisation. The obvious need for ATNS to become a more effective, resourceful, and operationally efficient

organisation has necessitated the establishment of an integrated information governance and related management structure. This is due to the fact that, in the current configuration, ATNS information assets are stored in decentralised locations in uncoordinated variable storage in fragmented designs and formats. Accessing ATNS information has become an administrative challenge, highlighting the consolidation and integration conundrum. According to anecdotal evidence, ATNS employees are unaware that information created and stored on their personal repositories (e.g. laptops or external hard drives) is a valuable asset to ATNS. As a result, it is the sole property of the organisation and must be a component of ATNS' corporate memory and repositories.

Purpose and objectives of the study

The purpose of this study was to explore information governance practices at ATNS with the view of developing a framework. ATNS, as a state-owned organisation, has the responsibility of ensuring that the information is safely kept and accessible. In achieving the purpose of this study, the specific objectives were to:

(1) Identify the roles and responsibilities for information governance facets within ATNS;

(2) Assess information governance infrastructure within ATNS;

(3) Identify the risks associated with information governance within ATNS; and

(4) Suggest an integrated information governance framework for ATNS.

Literature review

In recent years, there has been a significant amount of literature published internationally on information governance. A critical exploration of theories, studies, and peer-reviewed works by various authoritative theorists, authors, and scholars to establish views, insights, understanding, and approaches within the context of information governance is included in this study's review of the literature. A literature review process identifies and categorises relevant themes based on their similarity and relatedness to extract insights from existing knowledge and use it to build new knowledge that contributes to the discipline of information governance. In this study, themes for the literature review emanated from the objectives that were constructed from the Cor Concept Information Governance model.

Roles and responsibilities for information governance facets

Franks (2018, 2025) frames information governance as a high-level, strategic role that incorporates stakeholders from all areas of the organisation, each with their specialities and duties. The Sedona Conference Commentary on Information Governance (2014) recommends that the information governance programme should strive to incorporate all organisational components (business units, departments, functions, and so on) with a stake in the company's information. This may necessitate varying degrees and types of involvement from stakeholders. According to Hagmann (2013), practical experience highlights the importance of carefully sizing information governance frameworks by balancing the representation of all relevant parties, particularly lines of business, and concentrating investment in projects that promote an information management and governance culture. Responsibilities must be assigned for each information governance facet within an organisation. Chauke and Ngoepe (2025) identify facets of information governance such as risk management, data management, records management, information management, knowledge management, data analytics, and business intelligence. Failure to assign responsibilities for such facets may result in the roles not being fulfilled. A good approach is to establish a policy that clearly defines the responsibilities involved. For example, Chauke and Ngoepe (2025) contend that with the right

information governance policy in place, adopting the facets of information governance can be used to address concerns related to information integrity in the short and medium terms.

Information governance infrastructure within organisations

According to Johnston (2010), information governance infrastructure is a grouping of people, systems, policies, practices, and relationships that work together to enable information governing operations. All organisations, big and small, have a vast potential universe of information that has to be regulated, according to Gartner (2020). In a time when information is increasingly considered a strategic resource, maintaining extremely large volumes of data can be complicated and difficult, according to Polzonetti and Sagratella (2017). The new organisational imperative for gaining a competitive edge and getting the most out of the use of big data is to implement data governance procedures that maintain a balance between value generation and risk exposure.

According to Polzonetti and Sagratella (2017), information governance is impossible without flexible infrastructure. Organisations must be prepared to host, analyse, and convert information from many sources, produced for various purposes, within a single context as the infrastructure and application boundaries become more open. One may argue that outsourcing, cloud-based services, and/or hybrid infrastructure techniques and solutions offer well-known flexibility and scalability advantages.

To enable technological infrastructure for information management, controls and monitoring points must be included. The following areas should be the focus of an information governance infrastructure:

(1) IT Architecture, Standards, and Integration: this area entails information, metadata, storage, transport and system standards;

(2) Data or Information Quality: this area entails the criteria for, the measurement of, and the maintenance of data or information quality;

(3) Data or Information Access: Information sourcing, access privileges, permissions and usage;

(4) Reporting: periodic assessment of the availability and quality of information sources for business decision-making;

(5) Security and Privacy: planning, controlling, and responding to security and privacy needs and directives; and

(6) Legal and Compliance: planning, controlling, and responding to information risk factors, and the legal and regulatory retention and disposition of information.

Risks associated with information governance

Information is a valuable resource for any organisation, but it can also be detrimental if not handled and supervised properly. Millican (2016) defines information governance as an integrated strategy for coordinating, meeting legal and regulatory requirements for information, managing information risks, and maximising information value. According to Cruz (2017), risk management identifies, analyses, and quantifies risks that may impact, be connected to, or be related to the development, storage, retrieval, distribution, disclosure, retention, disposition, or protection of information assets within an organisation. Smallwood (2014a) describes a risk profile method for generating and ranking the top 10 information security concerns. Failures in information management pose a significant risk, which information governance can help to mitigate. The risks may include information leaks, which could arise from ignorance, lack of ethics, wherein employees either unwittingly share information with others or deliberately pass it on to make some gains (Sithipolvanichgul *et al.*, 2024).

Records administration, a critical competency in organisations, is an important and strategic component in the detection of hazards, according to Ngoepe (2014). A strong records management regime should be put in place and used as the primary tool for identifying and managing risks. As a result, the development of records management as a risk reduction strategy must be incorporated into the organisational information governance framework.

Conceptual framework

COR Concepts integrated information governance framework was used as a conceptual framework for this study. The Cor Concept information governance framework was developed by Mullon (2017) after implementing many of its constructs in government entities in southern Africa. Mullon and Ngoepe (2019) highlight that the model is implemented in various organisations in southern Africa, including the Reserve Bank of South Africa and the eSwatini Revenue Authority, to mention just the two. The Cor Concepts framework includes four essential pillars, that is, Key Success Factors, Structures and Instruments, Principles and Disciplines. This model is consistent with the specific aims and parameters of information governance as they relate to the ATNS context. Globally, numerous information governance frameworks have been used in various settings to address information governance flaws in various organisations. Mullon and Ngoepe (2019) list various information governance frameworks and models that are frequently used to assess and measure information management and governance processes. These include the King IV report on corporate governance, ARMA Principles and Information Governance Maturity Model, the Electronic Discovery Reference Model, Information Governance Reference Model, Information Governance Initiative, and Control Objectives for Information Technology.

The intended outcome of this study is an integrated information governance framework that is custom made to support ATNS in managing and governing information appropriately, as well as setting optimum and legally compliant standards for information management. The Cor Concept information governance framework was chosen because it has been used as best practice for the implementation of information governance in many South African organisations. The four pillars of the Cor Concepts model have guided the objectives, literature review, and data collection of this study.

Methodology

This qualitative case study, anchored on the interpretivism research paradigm, sought to explore information governance practices, with a view to suggesting an integrated information governance framework that allows the organisation to govern and manage its information. The goal of a qualitative single case study is to guarantee that the subject of interest is thoroughly investigated and that the phenomenon's core is made clear (Ngulube, 2015). Case studies are beneficial for conducting in-depth analyses of bounded entities, such as organisations or specific incidents or events, according to Quinlan *et al.* (2015). Qualitative data were collected through interviews and document analysis. Quotes which emphasised key issues relating to the objectives of the study were presented with verbatim. Tables are also used to present data.

The study sample was purposively selected from ATNS employees who occupy various levels of positions within the organisation's organogram or hierarchy. In research that is premised on producing grounded theory, Creswell (1998) and Dworkin (2012) recommend 20 to 30 interviews and 25 to 30, respectively. At the time of conducting this study, ATNS employed 1322 staff members in total, divided among executives, senior managers, managers, specialists, technicians, administrators, and support workers. The criteria for selecting participants for this study were based on how long the employee had been employed by the organisation, which must have been for a minimum of two years. Along with years of experience, the justification for the selection criteria was based on employee participants who directly handle, manage and make choices on ATNS information assets. For trustworthiness the study applied the Lincoln and Guba

recommended criteria (Alexander, 2019) by using a combination of interviews and document analysis for credibility, as well as dependability established by maintaining a transparent audit trail of the data collection and analysis processes, while confirmability was ensured by basing findings on the responses of participants and transferability supported through comprehensive contextual descriptions. For interviews, ATNS departments, including legal and compliance, risk, finance, corporate secretarial, air traffic services, engineering, operational technology, records management, and human resources were targeted. A total of 26 ATNS employees were interviewed, as reflected in Table 1, with two departments, Audit and Company Secretary, declining to participate in the study for unknown reasons.

The data collection strategy employed enabled data triangulation and assured the reliability of the findings (Creswell and Plano Clark, 2007). According to Pattan (2002), data collection is varied and includes document reviews, observations, and qualitative research interviews. Data were analysed and interpreted based on the objective of the study to create themes. The process of analysing data included interpreting and summarising it to communicate the most important features of the data. Interview responses were transcribed as a way of preparing data for subsequent analysis. Transcripts made it easier to search for specific themes, patterns or keywords and speed up the data analysis process. Transcripts also enhanced data coding, or the categorisation of data based on content, themes, and patterns. Following this, there are limited verbatim quotes from participants with data augmented through the analysis of documents such as information management related policies, procedures and taxonomies.

Findings and discussions

The results of this study are presented and discussed in accordance with the study's objectives.

Roles and responsibilities for information governance facets

The objective of this study was to explore the roles and responsibilities associated with information governance at ATNS. According to Mullon (2017), clearly defined roles and responsibilities are essential for the successful implementation of an information governance framework. The findings indicate that the roles and responsibilities related to information governance within ATNS are currently unclear and fragmented. There are no specific positions designated for information governance. For example, one participant noted that:

> Different roles in different departments within the organisation deliver different facets of information governance, which eventually leads to inconsistency and irregularities in information governance implementation. There are structural flaws that limit the organisation's ability to implement information governance.

Table 1. A summary of interviewed participants per department

Department	Number of participants
Audit	0
Aviation training academy (ATA)	3
Air traffic services (ATS)	5
Air traffic management (ATM)	1
Commercial services	1
Company secretary	0
Finance	2
Information technology	5
Legal counsel	1
Operations technology (OT)	2
Risk	2
Strategy and Optimisation (S&O)	4

Source(s): Authors' own work

While participants indicated that there was no information governance committee, which is critical for overseeing the implementation of information governance within the organisation, one participant indicated that:

> Obviously, the CEO's office, because of its accounting role, is in charge of leading and implementing information governance. However, this responsibility is delegated to the Strategy and Optimisation Unit.

When participants were asked to identify and list the organisations to which ATNS is accountable in terms of information governance, the following organisations were identified:

(1) International Civil Aviation Organisation (ICAO) – the role of ICAO is to research new air transport policies and standardisation innovations and ensure that all affiliated air traffic management member states implement them. It is therefore critical for ATNS to ensure that organisations' information is managed and governed to meet the set policies and standards of ICAO.

(2) Air Transport Association (IATA) – ensures the growth of a safe, secure and sustainable air transport industry. ATNS's priority is to ensure that the South African skies are safe and free from any accidents. ATNS is obligated to adhere to IATA regulations and standards, which require that the internal information environment be compliant.

(3) Information Regulator of South Africa – ensures and enforces compliance of Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) and the Protection of Personal Information Act (2013) (Act No. 4 of 2013) to all public and private organisations.

(4) South African Civil Aviation Authority (SACAA) - regulates civil aviation safety and security in support of the sustainable development of the aviation industry, including the annual safety audits that are conducted on all aviation agencies in South Africa. ATNS has the obligation of ensuring that information required during the SACAA audit is easily available and accessible.

(5) National Archives of South Africa – ensure that all government bodies or departments manage records in line with the National Archives Act. ATNS, as a state-owned organisation, has an obligation to ensure that records are managed to meet the set compliance requirements as outlined in the act. NARSA approved all the file plans and disposal schedules of government entities.

(6) South African Bureau of Standards (SABS) – ATNS, as an ISO 9000 certified organisation, has the responsibility of ensuring that the Quality Management System is compliant and meets the requirements of all conducted audits by SABS as scheduled.

(7) Department of Transport (DOT) – DOT is the major shareholder of ATNS. ATNS reports to the DOT, and the Board of Directors of ATNS is appointed by the DOT. It is therefore critical for ATNS to respond to all enquiries and information requests that DOT needs. Management and governance of information is of paramount importance to meet all information requests.

Table 2 is a summary of responses of the opinions of participants on how they view the interaction of ATNS with the external organisations they had chosen.

Information governance infrastructure

According to Franks (2025), information governance infrastructure is a collection of technologies and systems, people, policies, practices, and relationships that work together to

Table 2. Nature of the relationship of ATNS with external stakeholders

Agency name	Relationship
The international civil aviation organisation (ICAO)	Participants linked their understanding of ATNS and ICAO. ICAO creates regulations for aviation industry safety, security, efficiency, and regularity and environmental protection. ICAO provides technical standards, codes, specifications, and related documents
Air transport association (IATA)	Participants identified IATA as an international body that is responsible for the future growth of a safe, secure and sustainable air transport industry. ATNS is an active member of IATA and ensures that guidelines and standard procedures developed and outlined by IATA are implemented at an organisational level. On an annual basis, ATNS attends the annual general meeting (AGM) and the World Air Transport Summit (WATS)
Information regulator of south Africa	The responsibilities of the information regulator are to enforce compliance with the POPI Act by the public and private sectors, to issue codes of conduct for different sectors, and to make guidelines to assist or guide organisations with the development and application of codes of conduct. ATNS, as a government entity, is expected to comply and report to the information regulator about the POPI Act
South African civil aviation authority (SACAA)	The SACAA mandate is to provide Standards and Recommended Practices (SARPS) of the international civil aviation organisation (ICAO), considering the local context. Controlling, promoting, regulating, supporting, developing, enforcing and continuously improving levels of safety and security throughout the civil aviation industry in South Africa. CAA conducts regular audits of ATNS that are in line with the SARPS
National archives and records service (NARSSA)	The role of NARSSA is to preserve national archival heritage, including records that are created by organisations and deemed to be archival resources for use by the government and people of South Africa. ATNS is complying with NARSSA's requirements, which include, amongst others, the approved file plan and disposal authorities
Department of transport (DOT)	ATNS reports to dot and dot is the determining shareholder of ATNS. Dot leads the development of efficient integrated transport systems, including the aviation industry, by creating a framework of sustainable policies and regulations. DOT is mandated to implement standards that support an efficient transport system in South Africa
South African bureau of standards (SABS)	As the national standardisation authority, the SABS is responsible for maintaining South Africa's database of national standards, developing new standards, and revising, amending, or withdrawing existing standards as required. ATNS is an ISO 9000 organisation and complies with SABS standards to ensure that the organisation qualifies for the certification requirements

Source(s): Authors' own work

support information governance activities. The IT department is responsible for centrally managing and reporting on security and privacy needs and directives. In this regard, information governance falls short. The legal and compliance aspects of information governance are handled by various departments throughout the organisation. Planning, controlling, and responding to information risk factors is coordinated between IT and the Risk department, and the organisation's legal and regulatory universe, including information governance regulatory, is coordinated by the legal department, while information retention and disposition is coordinated by the Information and Knowledge Management function within the IT department.

The researchers asked participants to identify the current information governance infrastructure available within ATNS, as well as highlight their understanding of information governance infrastructure within ATNS. An effective and robust information

governance infrastructure allows a company to manage high volumes of content, on or off-site premise storage, backup technology for system failure and data loss recovery, archiving technology to manage inactive content, manage social media content, information security and privacy, impose retention schedules, including litigation holds and eDiscovery, and provide audit reports and analysis (Franks, 2018).

Another participant noted:

> The organisation is not clearly outlining how to use information. This lack of direction is limiting the potential use of information for performance.

Participants were asked to share their understanding of information governance infrastructure within ATNS, as well as identify the current information governance infrastructure available within ATNS. The responses to this question were only from IT participants. Those who responded defined information governance infrastructure as IT architecture, IT standards, metadata, storage, IT systems, information quality, information access privileges, regulatory information retention and disposition, permissions, and usage. Participants demonstrated limited knowledge and understanding of the information governance infrastructure. One participant went as far as saying that:

> We don't need another unit for information governance. Each section within the CIO can manage information with the CIO as its umbrella. It is working well, as records management is already implementing its responsibility.

Risks associated with information governance

Zouari-Hadiji and Mroua (2026) highlight that internal governance is about recognising that information is subject to risks that can affect proper use and application. Information plays an important role in supporting the audit process. The significance of organisational risk management in terms of protecting information is to mitigate the degree of threat exposure and loss of organisational information (Sithipolvanichgul *et al.*, 2024). Risks associated with information governance within ATNS comprise loss of intellectual property through the lack of governance; sensitive and personal information not being properly managed; poor records management; information lifecycle; creation of information for preservation or disposal; lack of metadata management to increase findability; application of security, accessibility controls, and managing retention; harm to information from malicious access and unauthorised persons; storage of information in locations or formats that increase loss, cost, and limited access; failure to preserve information relevant to litigation, compliance, and government proceedings; disaster recovery; over-preservation of information relevant to litigation or government proceedings; and management of unstructured content. If information is not protected, regulations can be broken, data can be lost, and compliance can fall short, all of which can lead to potential harm from the disclosure of personal information. Lawsuits, investigations, following rules, keeping private information private, protecting intellectual property, and managing change are among the risks identified. Records management is listed as one of the risks that the organisation is facing in its risk register.

Another participant noted:

> The risks associated with information governance within ATNS include a lack of proper management of sensitive personal information and poor records management.

These risks can lead to regulatory breaches, data loss, insufficient compliance, and potential harm from the disclosure of personal information, contributing to lawsuits and other legal challenges. Records management is specifically noted as a risk in the organisation's risk register.

Table 3 reflects responses from participants on how to mitigate information governance risks.

Table 3. Risks mitigation and opportunities of information governance within ATNS

Risks	Mitigation (control activities)	Opportunities
Loss of data, information, and intellectual property	To develop and implement policies and procedures that are aligned with the relevant legislation and ISO standards, clearly outlining the organisation's information, incorporate information ownership and data handling policies, and ensure proper backup procedures are in place and communicated org wide	Relevant, policies, procedure, and standards
Information lifecycle (creation of information to preservation or disposal)	To develop Standard Operational Procedures (SOP) on information lifecycle management (ILM) refers which will ensure that information from creation through to archiving or disposal is optimally used at a low cost and meet the legal compliance	Information lifecycle management SOP will provide the organisation with an overall information value chain and be able to manage the risks as information moves through the lifecycle and have an action plan to mitigate the risks
Lack of metadata management to increase findability, apply security, accessibility controls, and managing retention	The IT department will deploy and implement modern technology with metadata functionality. Train employees on basic metadata standards and requirements and why it is important to include metadata in the information that is saved in all organisational systems to ensure accessibility and retrievability	Quality control measures – easy access to information and searchability
Harm to information from malicious access and unauthorized persons	Access control policies and guidelines	Limit access based on the role of the employee and the responsibilities in the organisation. Create an audit trail. Eliminate security vulnerabilities by putting strict control measures in place
Storage of information in locations or formats that increase loss, cost and limited access	Strengthen security on all storage facilities by implementing the following • Identity and access control • Use of multi-factor authentication • Use of strong passwords; and • Remove unused storage space and ensure that the information lifecycle principles are implemented	Security control policies and procedures – that will limit unauthorised information access
Failure to preserve information relevant to litigation, compliance and government proceedings	Ensure that the information retention policy is in place with proper controls Outline e-discovery processes and communicate with businesses for proper implementation	Retention and e-Discovery policies
Over-preservation of information relevant to litigation or government proceedings	ATNS will develop and implement the Information Retention and Archive Policy. The purpose of this policy will be to ensure that all information created in the organisation is monitored through its lifecycle and is disposed of or archived as and when required	Information Retention and Archive Policy
Disaster recovery	Evaluating the hazard, exposure, and vulnerability of the organisation's information. Planning ahead to ensure that any disaster that could occur should not destabilise the use and access of information for operational efficiency	Disaster Recovery Plan (procedure)

(*continued*)

Table 3. Continued

Risks	Mitigation (control activities)	Opportunities
Information vulnerabilities that impacts data and information confidentiality, integrity, access, and availability	Implement information access control and permission control, activity monitor privileged information system users, implement Information Destruction Policy, training employees on information vulnerabilities, confidentiality, integrity, access, and availability	Information Destruction Policy Training and awareness to all employees
Management of unstructured content, e.g. emails and correspondence	Training of all employees on enterprise content management (ECM)	ECM training
Any missing risk, specify	There were no comments on this section	Not applicable

Source(s): Authors' own work

Discussions of the results

The study established that there is a lack of information governance leadership and strong executive sponsorship for information governance, which harms the successful implementation of information governance. The lack of information governance leadership and strong executive support for information governance is unavoidable and will have an impact on the successful implementation of information governance. An examination of the records management policy and the IT policy reveals that responsibilities for these facets are clearly defined for staff members in various categories. The records management policy, for example, outlined responsibilities for the chief information officer, records manager, and all ATNS employees. However, no information governance specific policy exists.

Only some aspects of information governance are implemented in the organisation, and the maturity of each implemented aspect of information governance varies. One of the information governance aspects that is currently being implemented is records management. Participants identified Information Technology (IT) as the department in charge of information governance in the organisation. Currently, the Chief Information Officer (CIO) is in charge of the organisation's information infrastructure and technology. The CIO is in charge of Information and Knowledge Management (IKM). Records management, knowledge management, data analytics, business intelligence, a digital library, and enterprise content management are all provided by the IKM function. IKM is also responsible for developing organisational policies and procedures for information management. The organisation's CEO is designated as the accounting officer for all related legislative frameworks and is responsible for ensuring compliance with information governance related legislation, such as archival, privacy, and freedom of information legislation. This aligns with Mullon and Ngoepe (2019), who argue that fragmentation is a defining characteristic of information governance in developing contexts. It further reinforces Hagmann's (2013) assertion that lack of integration undermines governance maturity.

The study clearly shows that ATNS has strong information technology systems and software. Everyone creates information on various platforms, which are fully managed by the IT department. However, it was indicated that the business is not fully digitally transformed. IT infrastructure is used throughout the organisation to access and manage data. The IT department has complete control over information access, retrievability, and security. There is no specific contextual access to information provided by providing the right information to the right people at the right time in a secure manner. There is no retention schedule in place to ensure that information is retained in the organisation in accordance with its value and lifecycle. The information kept in the organisation should be as valuable as possible so that it can be used to provide new insights and value. ATNS utilises Microsoft tools, including SharePoint, for collaboration to access the content and information of the organisation. SharePoint is used, and is developed, and configured for the management of documents and

records. The process of raising awareness and training employees to use SharePoint as the central information repository is currently underway. More development and content management are required to ensure that records management is fully implemented and embedded in the organisation, which will lead to the implementation of information governance.

It is clear that ATNS has identified several risks relating to information governance, as highlighted by the participants and also reflected in the risk register. Such risks relate to loss of information, lack of disaster preparedness, storage, and compliance with information legislation. Due to a lack of storage space, proper information management, for example, may be compromised, resulting in difficulties in retrieving information and negatively impacting service delivery. Furthermore, the organisation may resort to making use of cloud storage at additional costs.

Suggested information governance framework

The ultimate aim of this study was to propose an integrated information governance framework (see Figure 1). The proposed framework highlights the various activities that should be developed and implemented for the information governance framework to be successful. The framework's main components are the legislative framework, policies, and standards; information governance roles and responsibilities; information governance infrastructure; risk management; change management; and information governance domains. Participants highlighted facets or key elements of information governance that should be included in the framework, which are: information governance strategy, legal, eDiscovery, risk management and compliance roles and responsibilities, records management, ECM (Archiving and Long-term Digital Preservation), data analytics and business intelligence, knowledge management and change management. The conception of an information governance framework is crucial for addressing information management deficiencies.

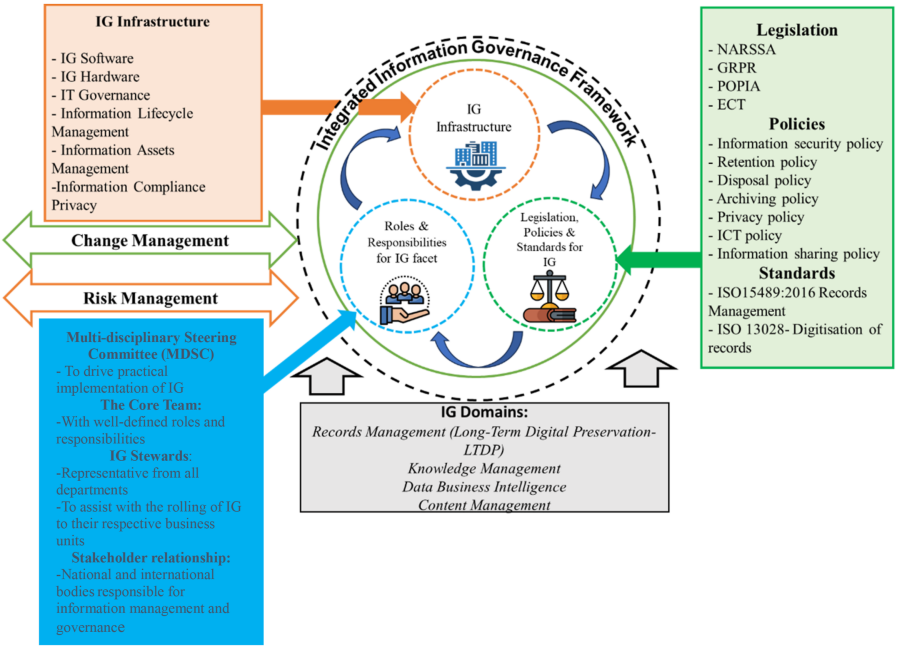

Figure 1. A proposed integrated information governance framework (Synthesised by the researchers, 2025)

Information governance legislative frameworks, policies and standards. ATNS, as a statutory body, must comply with the regulatory universe affecting the organisation's operations, including information governance requirements. Information governance seeks to align business objectives with organisational strategy to deliver business value. The focus on legislative frameworks, policies, and standards is to ensure compliance, that the organisation follows applicable laws, regulations, and internal policies.

Electronic discovery (e-discovery) readiness, records, and information retention policies, legal hold notification, and legally defensible disposition practices are all critical legal processes governing the preservation and discovery of records and information during a legal proceeding. Policy and standard alignment and implementation should support and drive the desired future behaviour of information governance. This goal is achievable in the medium term.

Roles and responsibilities of information governance. The roles and responsibilities of ATNS's information governance function must be agreed upon, defined, and formalised. There will be no successful implementation of an information governance programme in the organisation without well-defined information governance roles and responsibilities. The roles and responsibilities are as follows:

(1) Multi-disciplinary Steering Committee (MDSC): This committee was formed to make critical decisions for information governance; it is expected to meet regularly and will be empowered to make and enforce some key information governance decisions. The committee should include senior-level managers from all departments, including IT, Legal, Compliance, Risk, IKM, Internal Audit, and Quality.

(2) The Core Team: The information governance team will be in charge of coordinating all information governance related functions and responsibilities. This team will be responsible for ensuring that all aspects of the information governance activities, changes, and communications are carried out.

(3) Information governance Stewards: individuals from all internal departments who will facilitate the implementation of the information governance programme and functions in respective business units.

(4) Stakeholder relationships: national and international organisations in charge of information management and governance. To ensure that all information governance related standards, legislation, and regulations are aligned at the national and international levels.

The above can be developed and established in a short period.

IT infrastructure. The IT department will be vital in assisting the information governance function in successfully implementing information governance in the organisation. IT must ensure that users who will need to manage information electronically daily have computers, screens, and networks that are compatible with the information governance responsibilities. Furthermore, users must be fully trained in computer use before being expected to conduct business electronically. This will be incorporated into the Adoption and Change Management strategy. IT is a critical enabler of information governance implementation in the digital workplace. IT should supply the most essential IT infrastructure, network, software, and applications. According to Johnston (2010), information governance infrastructure is a collection of technologies and systems. Infrastructure includes, but is not limited to, the following:

(1) Concentrate on controlling information access (identity and access management) and ensuring the security of confidential information and communications.

(2) It also addresses Digital Signatures, Document Encryption, Data Loss Prevention (DLP), known as leak prevention, and Information Rights Management (IRM).

(3) Is primarily concerned with identifying and safeguarding personally identifiable information (PII).

(4) It entails creating Data Breach Response Plans and responding to breaches.

Achieving this recommended intervention requires executive buy-in, a reassessment of technical strategy, hardware and software needs analysis, and a budget to be committed. For this reason, IT infrastructure upgrades to support information governance can be done in the medium term.

Risk management. According to Hagmann (2013), risk management maintains a balance between internal and external uncertainties or threats and potential business opportunities. Because information management and governance are not structured and prevalent within ATNS, there is a high level of risk associated with information governance. Risk management is critical for the success of information governance implementation. Risk management will guide and aid in the development of a risk management plan to address the identified risks. Risk management is a strategy for dealing with strategic uncertainties and addressing the process of identifying and analysing risks, as well as implementing appropriate risk management plans to mitigate the potential consequences of the identified risks (Ngoepe, 2014). Since "risk management" is a fundamental and urgent need to fortify and secure ATNS information as a strategic asset, management is urged to place it high on the plan to implement it in the short term.

Change management. To successfully implement information governance, a solid change management plan is required. Change management is viewed as the fundamental building block of any programme and will be included in all information governance activities (Hagmann, 2013). Change is unavoidable, and change management is vital to ensure that smart organisational plans succeed. Information governance and change management are inextricably linked, to alter the structure, guidelines, and rules under which employees operate (Smallwood, 2014a).

Information governance domains. Mullon and Ngoepe (2019) emphasise the importance of the integration of all domains and aspects of information governance. It is recommended that all of the information governance domains and facets listed below be formalised for gradual implementation over the next five years. It is recommended that they are reviewed every 5–10 years to be updated to reflect changes in legislation, technological advancement, and ATNS's strategic goals.

Records management (RM) and records and information management (RIM)

(1) Foundational component of information governance.

(2) Primarily concerned with the identification, classification, retention, use, and eventual disposition of records and information.

Content management

(1) Primarily concerned with the storage and access of electronic records and information.

(2) Incorporates security, access controls, retention and disposition, and legal holds for electronic information.

Data management

(1) Alias "Data Integrity" - processes and controls to be in place to ensure data is true, accurate, and unique.

(2) It often involves data cleansing (scrubbing) to remove corrupted, inaccurate, or extraneous data and duplication to eliminate redundant data.

(3) Often referred to as Master Data Management (MDM), it is used to ensure reports, analyses, and conclusions are based on clean, reliable, and trusted data normally contained in databases.

Long-term digital preservation

(1) Long-Term Digital Preservation methods, best practices, and standards should be applied to preserve an organisation's historical and vital records (those without which it cannot operate or restart operations) and to maintain its corporate or organisational memory.

(2) Uploading permanent electronic records into the digital records centre.

(3) Digital preservation is a process and not a technology, addressing format, media, software, and hardware obsolescence associated with digital information.

Business intelligence

(1) Primarily concerned with data analytics to identify insights and emerging trends.

(2) Can provide solid information for decision-makers to use in times of crisis or opportunities.

(3) Has a desire to retain all information to provide better analytics.

(4) Drive a culture of legislative compliance by implementing a variety of strategies, such as employee training in this area.

Knowledge management

(1) Provides agility in accessing organisational knowledge and information.

(2) Improves productivity as knowledge and information are managed, stored, and safeguarded for better and quicker problem-solving.

(3) With a well-established knowledge management structure and processes, there will be a culture of openness to sharing knowledge across the organisation and the preservation of knowledge from any loss.

The proposed framework addresses the structural disconnection highlighted in the findings by establishing a coordinated governance approach that combines strategic, operational, and compliance requirements. In contrast to current models, it is specifically designed for the aviation regulatory landscape, where safety, accountability, and real-time decision-making are essential.

Implications for theory and practice

The purpose of this study was to develop an integrated IG framework for ATNS in South Africa because a solid IG framework is a critical foundation that allows the organisation to govern and manage its own information. The results of this research highlighted and illustrated the importance of information governance for organisations and, in particular, ATNS. Organisations create data and information that should be managed throughout its life cycle. Based on the findings, law and policy makers are persuaded to develop policies that will

address the deficiencies that organisations are facing. For government entities have a critical role in ensuring that the created information is captured and managed in line with the prescribed laws and policies to ensure compliance. This study uncovered critical areas that need attention for policy makers to consider addressing the alignment of various facets of information governance in the organisation, including managing information as organisations asset.

The proposed IG framework for ATNS, as compiled by the researcher, can be utilised for further discussion with regard to theory development and application in the field of information science, with more specific to information governance. This study adds value to the existing theoretical and conceptual issues that constitute the ongoing discourse on information governance at the organisational and national levels in developing countries. The study has identified issues that require further investigation, including the changing information culture of an organisation. With the lack of knowledge and understanding of information governance, there is a need to research how information governance can be appreciated in the organisation or create the appetite for information management and governance thereof. One of the issues that did not come out clearly in the study includes digital transformation to enhance information governance. Digital transformation can be an effective strategy for reducing the burden and risks of information governance (Shibambu and Ngoepe, 2025). The issue of digital transformation should be interrogated further in another context within South Africa. In addition, a strong information governance framework for air traffic management plays a crucial role in enhancing aviation safety, ensuring compliance with regulations, and fostering public trust. In the context of South Africa, this is especially relevant for bolstering governance within state-owned enterprises. It is concluded that the development and implementation of an information governance framework may ensure that ATNS creates, stores, uses, and disposes of information in accordance with regulatory and compliance requirements, risk management, and operational workflow requirements.

Conclusion

The study's findings demonstrate the importance of establishing key policies, activities, and a control framework for information governance. Setting up proper policies, procedures, and practices is critical to creating a culture of proper information governance in an organisation. The study revealed that ATNS lacked an information governance framework and that there is no short or long-term plan to develop one. However, there are a variety of activities developed and delivered in silos that could contribute to the information governance framework. While some aspects of information governance are already in place within ATNS, it is essential to centralise the development of information governance strategy, functions, and implementation. Collaboratively implementing information governance will ensure that information is accurate and secure, that legislation is followed, and that fragmented and siloed information governance initiatives are addressed and coordinated.

The proposed information governance framework addresses the fragmentation of roles and responsibilities by integrating previously isolated activities such as records management, knowledge management, and information technology under a single governance model, thereby improving accountability and minimising redundancy. Additionally, the framework describes important facets, including governance structures, defined roles, supportive infrastructure, risk management, and compliance measures, which, combined, facilitate effective oversight and execution. By establishing clear lines of accountability and encouraging cross-functional collaboration, it enhances strategic alignment and operational effectiveness within the organisation. Importantly, the framework is designed to be practically applicable, making it suitable for implementation within ATNS and adaptable for other organisations functioning in a highly regulated environment. Additionally, it offers a scalable and context-responsive model that can enable better decision-making, regulatory compliance, and the responsible management of organisational information assets.

The researchers acknowledge that information governance facets exist in various forms within ATNS and other state enterprises, but no integrated information governance framework is currently in place. As a result, it is recommended that ATNS intentionally incorporate the facets of the information governance framework. The study recommends an information governance framework to ensure that the organisation meets legislative requirements and compliance, secures its information assets, makes information easily accessible, saves money on storage, and makes insightful and correct decisions based on well-managed information.

This study contributes to the information governance discipline by offering empirical insights from a critical but underexplored context. The suggested framework presents a practical model for unifying disparate governance functions within ATNS. Future studies should investigate the influence of organisational culture, digital transformation, and leadership in enhancing information governance maturity in comparable settings.

Finally, the overview given in this study has obvious limitations relating to the representation of participants across organisational functions. Most participants from the line functions (nine participants) had challenges responding to the interview questions due to a lack of understanding of information governance. The reliance on IT personnel responses, may have introduced a degree of bias, potentially skewing the findings towards a technology-centric perspective of information governance. This limitation is acknowledged and provides an opportunity for future studies to cover other areas ensure a more balanced functional representation.

References

Air Traffic and Navigation Services (2019), ATNS official website, available at: http://www.ATNS.com/ (accessed 11 May 2019).

Alexander, A.P. (2019), "Lincoln and Guba's quality criteria for trustworthiness", *IDC International Journal*, Vol. 6 No. 4, pp. 1-6.

Allen, L. and Allison, K. (2018), "IG in US federal agencies: balancing information value and risk", *Information Management Journal*, Vol. 52 No. 5, pp. 38-40.

Bennett, S. (2017), "What is information governance and how does it differ from data Governance?", *Governance Directions*, Vol. 69 No. 8, pp. 462-467.

Chauke, T. and Ngoepe, M. (2025), "Integrating facets of information technology governance at a professional council in South Africa", *Global Knowledge, Memory and Communication*, Vol. 74 No. 11, pp. 101-120, doi: 10.1108/gkmc-08-2023-0270, (accessed 8 November 2024).

Creswell, J. (1998), *Qualitative Inquiry and Research Design: Choosing Among Five Traditions*, Sage, Thousand Oaks, CA.

Creswell, J.W. and Plano Clark, V.L. (2007), *Designing and Conducting Mixed Methods Research*, Sage, Thousand Oaks, CA.

Cruz, R. (2017), "Best practice in information governance", *KM World*, Vol. 26 No. 8, pp.22-23.

DAMA.org (2020), "Data management association international (Dama) official website", available at: Https://dama.org/ (accessed 10 April 2020).

Dworkin, S.L. (2012), "Sample size policy for qualitative studies using in-depth interviews", *Archives of Sexual Behavior*, Vol. 41, pp. 1319-1320, doi: 10.1007/s10508-012-0016-6.

Franks, P.C. (2018), *Records and Information Management*, 2nd ed., ALA Neal-Schuman, Chicago.

Franks, P.C. (2025), *Records and Information Management*. 3rd ed., ALA Neal- Schuman, Chicago.

Gartner (2009), *Toolkit: Information Governance Project*, April 2009, available at: www.gartner.com/id¼933912 (accessed 21 April 2021).

Gartner.com (2020), "Gartner official website", available at: Http://www.gartner.com/ (accessed 25 May 2022).

Hagmann, J. (2013), "Information governance – beyond the buzz", *Records Management Journal*, Vol. 23 No. 3, pp. 228-240, doi: 10.1108/rmj-04-2013-0008.

Iannarelli, J.G. and O'Shaughnessy, M. (2014), *Information Governance and Security: Protecting and Managing Your Company's Proprietary Information*, Butterworth-Heinemann, Oxford.

ICAO.Int (2020), "ICAI official website", available at: https://www.icao.int/about-icao/Pages/default.aspx (accessed 2 February 2020).

Johnston, E. (2010), "Governance infrastructures in 2020", *Public Administration Review*, Vol. 70 No. s1, pp. 122-128, doi: 10.1111/j.1540-6210.2010.02254.x.

Kogi, S.K., Kristanto, A.B. and Cao, J. (2025), "A systematic literature review of environmental, social and governance (ESG) research in Africa", *Meditari Accountancy Research*, Vol. 33 No. 7, pp. 199-245, doi: 10.1108/MEDAR-08-2024-2623.

Lederman, P.F. (2012), "Getting buy-in for your information governance program", *Information Management Journal*, Vol. 46 No. 4, pp. 34-37.

Lomas, E. (2010), "Information governance: information security and access within a UK context", *Records Management Journal*, Vol. 20 No. 2, pp. 182-198, doi: 10.1108/09565691011064322.

MacLennan, A. (2014), *Information Governance and Assurance: Reducing Risk, Promoting Policy*, Facet Publishing, London.

Maurel, D. and Zwarich, N. (2021), "Information governance and power relations: reflections on archival education in Québec", *Education for Information*, Vol. 37 No. 1, pp. 33-51, 10.3233/efi-190360.

Millican, B. (2016), "Establishing a plan to mitigate risk with information governance", *Inside Counsel*, Vol. 12 No. 1, p. 1.

Mullon, P.A. (2017), *Integrated Information Governance*, Knowledge Management Summit, Pretoria.

Mullon, P.A. and Ngoepe, M. (2019), "An integrated framework to elevate information governance to a national level in South Africa", *Records Management Journal*, Vol. 29 No. 1, pp. 103-116, doi: 10.1108/rmj-09-2018-0030.

Ngoepe, M. (2014), "The role of records management as a tool to identify risks in the public sector in South Africa", *South African Journal of Information Management*, Vol. 16 No. 1, pp. 1-8, doi: 10.4102/sajim.v16i1.615.

Ngoepe, M. (2016), "Records management models in the public sector in South Africa: is there a flicker of light at the end of the dark tunnel?", *Information Development*, Vol. 32 No. 3, pp. 338-353, doi: 10.1177/0266666914550492.

Ngulube, P. (2015), "Trends in research methodological procedures used in knowledge management studies", *African Journal of Library, Archives and Information Science*, Vol. 25 No. 2, pp. 125-143.

Pattan, M.Q. (2002), *Qualitative Research and Evaluation Methods*, Sage Publications, California.

Polzonetti, A. and Sagratella, M. (2017), "Towards a data-driven enterprise: effects on information, governance, infrastructures and security", *IEEE International Conference on Industrial Engineering and Engineering Management (IEEEM). 2017 IEEE International Conference*, pp. 1480-1484.

Quinlan, C., Babin, B., Carr, J., Griffin, M. and Zikmund, W. (2015), *Business Research Methods*, Cengage Learning.

Rocha-Bello-Bertin, P. (2019), "Towards effective governance of information in a Brazilian agricultural research organisation", PhD thesis, Loughborough University, Loughborough.

Shibambu, A. and Ngoepe, M. (2025), "Enhancing service delivery through digital transformation in the public sector in South Africa", *Global Knowledge, Memory and Communication*, Vol. 74 No. 11, pp. 63-76, doi: 10.1108/GKMC-12-2023-0476.

Sithipolvanichgul, J., Dhir, A., Talwar, S., Srivastava, P. and Kaur, P. (2024), "Knowledge arbitrage: what are the risks, and do they matter?", *Journal of Knowledge Management*, Vol. 28 No. 10, pp. 2818-2842, doi: 10.1108/JKM-05-2023-0411.

Smallwood, R.F. (2014a), *Information Governance for Business Documents and Records*, John Wiley & Sons, New Jersey.

Smallwood, R.F. (2014b), *Information Governance Concepts, Strategies and Best Practices*, John Wiley & Sons, New Jersey.

The Sedona Conference Commentary on Information Governance (2014), "A project of the Sedona conference working group on electronic document retention & production (WG1)", *Sedona Conference Journal*, Vol. 15, pp. 125-169.

Zouari-Hadiji, R. and Mroua, W. (2026), "Audit and financial communication quality: the moderating role of internal governance mechanisms", *EuroMed Journal of Business*, Vol. 21 No. 2, pp. 551-588, doi: 10.1108/EMJB-09-2024-0238.

Corresponding author
Mpho Ngoepe can be contacted at: ngoepms@unisa.ac.za