emeraldinsight



Records Management Journal

An integrated framework to elevate information governance to a national level in South Africa

Paul Anthony Mullon, Mpho Ngoepe,

Article information:

To cite this document:
Paul Anthony Mullon, Mpho Ngoepe, (2019) "An integrated framework to elevate information governance to a national level in South Africa", Records Management Journal, https://doi.org/10.1108/RMJ-09-2018-0030
Permanent link to this document:
https://doi.org/10.1108/RMJ-09-2018-0030

Downloaded on: 22 January 2019, At: 10:03 (PT)
References: this document contains references to 26 other documents.
To copy this document: permissions@emeraldinsight.com
The fulltext of this document has been downloaded 77 times since 2019*

Users who downloaded this article also downloaded:

(2018),"Separating the wheat from the chaff with the winnowing fork: The eeny meeny miny mo appraisal approach of digital records in South Africa", Records Management Journal, Vol. 28 Iss 2 pp. 130-142 https://doi.org/10.1108/RMJ-09-2017-0027

,"Taking archives to the people: The use of social media as a tool to promote public archives in South Africa", Library Hi Tech, Vol. 0 Iss 0 pp. - https://doi.org/10.1108/LHT-11-2017-0228

Access to this document was granted through an Emerald subscription provided by emerald-srm:178063 []

For Authors

If you would like to write for this, or any other Emerald publication, then please use our Emerald for Authors service information about how to choose which publication to write for and submission guidelines are available for all. Please visit www.emeraldinsight.com/authors for more information.

About Emerald www.emeraldinsight.com

Emerald is a global publisher linking research and practice to the benefit of society. The company manages a portfolio of more than 290 journals and over 2,350 books and book series volumes, as well as providing an extensive range of online products and additional customer resources and services.

Emerald is both COUNTER 4 and TRANSFER compliant. The organization is a partner of the Committee on Publication Ethics (COPE) and also works with Portico and the LOCKSS initiative for digital archive preservation.

*Related content and download information correct at time of download.

Downloaded by Iowa State University At 10:03 22 January 2019 (PT)

The current issue and full text archive of this journal is available on Emerald Insight at:
www.emeraldinsight.com/0956-5698.htm

An integrated framework to elevate information governance to a national level in South Africa

Paul Anthony Mullon
COR Concepts, Centurion, South Africa, and
Mpho Ngoepe
University of South Africa, Pretoria, South Africa

Received 23 September 2018
Revised 10 December 2018
Accepted 12 December 2018

Downloaded by Iowa State University At 10:03 22 January 2019 (PT)

Abstract

Purpose – As an emerging discipline, information governance (IG) presents a number of challenges to organisations and countries. For example, IG has not yet been clearly defined and current proponents present the concepts as records management, information management, enterprise content management, privacy (data protection), freedom of information, corporate governance, information risk, information security and e-discovery, to mention just a few areas. At an organisational level, initiatives focus on one of these aspects, often conflicting with the other elements, and are initiated because of some immediate business challenge, such as the introduction of the Protection of Personal Information Act (data protection or privacy legislation) in South Africa. This is compounded by the fact that the country creates many fragmented policies and pieces of legislation on the same IG aspects which are conducted in a disjointed manner. This study aims to present an integrated IG framework at the country level, comprising key success factors, required instruments (policy and legislation), principles and a proposed list of elements or disciplines, which should be managed in a cohesive manner.

Design/methodology/approach – This study adopted the Information Governance Initiative's pinwheel facets of IG to design an integrated framework of elevating IG to country level. The pinwheel helped to identify different facets of information disciplines and the responsible oversight mechanism for implementation in South Africa. The study relied on data obtained through content analysis of policy documents, legislative frameworks, and literature review regarding the identified facets of IG in South Africa.

Findings – The study established that only some aspects/domains/facets of IG are legislated and driven by policy in South Africa. These domains are at different levels of maturity and different stakeholder groups are responsible for each domain; for instance, the National Archives of South Africa is responsible for records management and the State Information Technology Agency is responsible for information technology, while the newly established Information Regulator is responsible for freedom of information and data privacy. There is generally no over-arching structure responsible for overall IG in South Africa as the elements are fragmented in various oversight mechanisms and institutions. As a result, domains compete for limited resources and often lead to "knee-jerk" responses to legislative, legal or risk drivers.

Research limitations/implications – It is concluded that if IG is not regulated and modelled at a country level, it is highly unlikely to filter down to organisations. Implementing IG at country level will go a long way in helping to filter it down to an organisation level.

Originality/value – The study is useful by presenting a framework to ensure that IG is implemented at the country level with a single coordinating body established for oversight mechanisms such as the Information Regulator (which currently has a narrow scope of privacy and freedom of information, although with limited resources).

Keywords Information technology, Records management, South Africa, Freedom of information, Information governance

Paper type Conceptual paper



Records Management Journal
© Emerald Publishing Limited
0956-5698
DOI 10.1108/RMJ-09-2018-0030

1. Introduction

This study stems from the development of an integrated information governance (IG) model for organisations, which was initiated because of a perceived lack of consistent understanding of IG across various industry sectors in South Africa. While there is no standard definition for IG *per se*, there is also no clear model for managing all aspects of IG at the country level. There is no evidence at all of IG having been described at the country level, in any country. Franks (2013, 2015), Hagmann (2013) and Gartner (2018) mostly define IG at an organisational level. As an emerging discipline, IG presents a number of challenges to organisations and countries. For example, IG has not yet been clearly defined and current proponents present the concepts as records management, information management, enterprise content management, privacy (data protection), freedom of information, corporate governance, information risk, information security and e-discovery, to mention just a few areas, at the organisational level (Franks, 2015). The IG approach and focus of the various proponents stem almost entirely from the current mindset and historical expertise of various organisations. Furthermore, the responsibility of IG at the country level, especially in South Africa, is not clear (Mullon, 2017). In South Africa, as described in the King III report, IG has mostly been limited to information technology governance.

The concept of IG is still new but is gaining popularity all over the globe (Hagmann, 2013). Indeed, IG has emerged globally in recent years in various guises, such as records management, freedom of information, e-discovery and information privacy. It encompasses all data activities. Early references to IG appeared in the late 1990s, focusing primarily on health-care information in the UK. Since the mid-2000s, it has been used to describe various disciplines and has been used by the vendor community as a catch-all for information-related services. As a result, it lacks a clear definition and is used to mean many different things. For example, Franks (2015) defines IG as an integrated strategic approach to managing, processing, controlling, maintaining and retrieving information as evidence of all transactions of the organisation. This definition takes its lead from records management, where records are regarded as evidence of the activities of the organisation. Gartner (2018) contents that the concept includes the processes, roles, policies, standards and metrics that ensure the effective use of information to enable an organisation to achieve its goals. In both the definitions, the focus is on an organisation. Changes in corporate governance, new information-related global legislation and regulations and the rapid increase in the amount of information in use in organisations have led to the need to clearly define a framework for IG, with a consistent definition, appropriate inclusion of affected disciplines and an approach to implementation. According to Hagmann (2013), in the absence of a framework, the danger is that organisations just rebrand existing records and information programme into an IG programme. Although a bit ambitious, this calls for elevation of IG to the country level, covering both the public and private sectors. For example, in South Africa, private sector organisations are required to comply with various pieces of legislation, depending on the nature of their business. There is no single law which imposes records retention requirements on all private sector organisations. Even in the public sector, where the National Archives and Records Service of South Africa (NARSSA) Act govern records management, it does not impose retention periods, but rather point to other disparate pieces of legislation.

While working with stakeholders from the public sector, it became apparent to the authors of this article that no single organisation in South Africa has an overarching responsibility for IG at the country level. This was especially evident in 2018 as the country sought to develop regulations for the newly promulgated Protection of Personal Information Act (Act No. 4 of 2013). This Act is administered by the Information Regulator (Regulator),

Downloaded by Iowa State University At 10:03 22 January 2019 (PT)

which is part of the Department of Justice in South Africa (Information Regulator, 2018). The Regulator is also responsible for freedom of information, which in South Africa is governed by the Promotion of Access to Information Act (Act No. 2 of 2000). It is worth noting that previously, freedom of information legislation was the responsibility of the South African Human Rights Commission until 2016 (Mojapelo, 2017; Mojapelo and Ngoepe, 2017). The proliferation of technology has further fragmented the elements of IG as the State Information Technology Agency (SITA) in South Africa is responsible for IT governance. All these functions of IG are interrelated, but executed in *silos* by different organisations. As a result, there is no mechanism of dealing with duplication of functions and intellectual efforts. This study adopted the Information Governance Initiative (IGI) model as a guide to propose a framework for IG that can be applied at the country level, which in turn can be implemented at the organisational level. In this regard, the focus of the study is to identify the various interpretations of IG in use in South Africa and the various existing frameworks that can be used to encompass all related disciplines. The article recognises that issues such as information privacy, freedom of information, IT governance and records management are all important and any one of them could be a catalyst for an IG implementation. It is further recognised that organisations have departments or functions specifically designed to govern and manage these disciplines, often in a *silo* and with little regard for other related IG disciplines. For example, Mojapelo (2017) and Ngoepe and Van der Walt (2009) report that in some government agencies, access to information is managed by the legal departments, while in others, it is either IT or records management departments. This may be due to the absence of a national framework to guide the implementation at the organisational level. The *silo* of business information and processes has long been a hindrance to the management of an organisation's data, and it continues to be a primary barrier to progress in the implementation of IG policies that successfully maximise the value of data and minimise risk (Information Governance Initiative, 2018).

The underlying assumption is that countries are also faced with an IG requirement, which generally translates into laws, regulations and other governance instruments which provide for an element of each IG discipline. Furthermore, administration, monitoring and governance of the discipline fall within the mandate of a specific government entity. In the same way that organisations struggle to implement IG in a cohesive manner because of the "silo" nature of the organisational functions responsible for each discipline, it is expected that the same will apply at the country level. As a result, IG implementations are potentially incomplete and comprise fragmented initiatives leading to often overlapping, conflicting or duplicate initiatives (Mullon, 2017). For example, in the Limpopo Province in South Africa, while the premiere's office is responsible for transversal records management throughout the province, the Limpopo Provincial Archives is also responsible for regulating records management activities in provincial departments and municipalities. There is a clear duplication of functions and effort in this regard. The same applies at the national level where SITA sometimes implements electronic records management without the involvement of the NARSSA, which has a statutory regulatory role regarding records management in governmental bodies (Ngoepe, 2015). Although mitigated through a memorandum of agreement between NARSSA and the Auditor-General of South Africa (AGSA), the situation could have played itself out where the AGSA audits records management in governmental bodies, a function which is the responsibility of NARSSA.

Unless government adopts a cohesive, unified approach to IG at the country level, it is probable that organisations will struggle to implement IG in a unified manner, as each function will be faced with reporting and compliance obligations to a multitude of different government oversight regulatory bodies. This is the case in South Africa, and this study

Downloaded by Iowa State University At 10:03 22 January 2019 (PT)

hoped to identify the responsibilities of each IG element and propose the national framework. For the purpose of this study, IG is the set of multi-disciplinary structures, including oversight mechanisms, policies, procedures, processes, standards and controls available at the country level, to manage information on all media in such a way that organisations can customise to support their immediate and future regulatory, legal, risk, environmental and operational requirements.

2. Models for information governance used in South Africa

A few models and frameworks have emerged from various organisations and initiatives, all focusing on IG from different perspectives. As IG is maturing, various models are changing their direction while retaining their core area of expertise. As the concepts emerge, the definition changes and matures. For example, according to Smallwood (2014):

> IG is a sort of super discipline that has emerged as a result of new and tightened legislation governing businesses, external threats such as hacking and data breaches, and the recognition that multiple overlapping disciplines were needed to address today's information management challenges in an increasingly regulated and litigated business environment.

Without providing a specific definition, the concepts in Smallwood's description provide insight into how IG ties directly to legislation and other governance requirements. As Smallwood (2014, p. 462) expands further:

> IG is a subset of corporate governance and includes key concepts from records management, content management, IT and data governance, information security, data privacy, risk management, litigation readiness, regulatory compliance, long-term digital preservation and even business intelligence.

Perhaps this expansion explains why in South Africa, the corporate governance framework (King Report) initially listed IT governance (as compared to IG) as an umbrella term; hence, Ngoepe (2012) recommends that the proper concept to be used is IG. In this way, it will encompass all other elements of IG rather than curtail it to IT perspective only.

Finally, Smallwood (2014) ties IG once again to legislation, as it includes the set of policies, processes and controls to manage information in compliance with external regulatory requirements and internal governance frameworks. This inclusion of oversight mechanisms emphasises the need to elevate IG to national level. A number of frameworks have been developed for implementation at the organisational level and some are applied by some institutions in South Africa. The following have been identified:

- *COR Concepts information governance framework*: The IG framework was developed by Mullon (2017), and this framework is mainly implemented in various organisations where he consulted on IG in southern Africa, including, the Reserve Bank of South Africa and the eSwatini Revenue Authority. Mullon's framework includes three essential pillars, namely, instruments (policy and legislative framework), infrastructure (technology) and interest (people, change management and accountability).
- *Corporate governance using the King IV Report*: The corporate governance framework in South Africa is the King IV Report, which emphasises the need for information and technology governance, but does not provide detailed guidance (Institute of Directors in Southern Africa, 2009). The previous King reports (I, II and III) placed much emphasis on IT governance as if the concept embraces the wider IG (Ngoepe, 2012). As Ngoepe and Ngulube (2013) would attest, IT does not constitute IG, but it is an enabler and a component within IG.

Downloaded by Iowa State University At 10:03 22 January 2019 (PT)

- *Association of Information and Image Management (2018)*: It provides a certification for IG but does not provide a single framework or model. They focus primarily on enterprise content management, but they have subsequently expanded to include other elements of IG.
- *ARMA principles and information governance maturity model*: This model focuses primarily on records management and has been adapted and aligned to the Electronic Discovery Reference Model (EDRM) e-discovery IG framework.
- *ARMA information governance body of knowledge*: ARMA International (2018) defines IG as a "strategic, cross-disciplinary framework composed of standards, processes, roles, and metrics that hold organizations and individuals accountable for the proper handling of information assets". The framework helps organisations achieve business objectives, facilitates compliance with external requirements and minimises the risk posed by sub-standard information handling practices.
- *IT governance models, with Cobit5 as an initial reference point*: The focus of this model is on IT governance, with awareness of the need to govern information as a core element. Cobit5 does not purport to be an IG framework but is included, as there is often confusion between IT governance and IG as also reflected in the first three corporate governance reports (the King reports) (Ngoepe and Ngulube, 2013). According to Chauke (2018), the Department of Transport in South Africa used Cobit5 in implementing its IT governance.
- *IBM information governance maturity model*: IBM defines IG as "the disciplines, technologies, and solutions that are used to manage information within an enterprise in support of business and legal requirements. Information governance encompasses a broad set of subjects covering information quality, information protection, and information lifecycle management." IBM has had a long-standing interest in data governance, and established the Data Governance Council in 2004. Of particular interest is that IBM changed this to IG in 2010, recognising that "information governance is a business concern, and not just a data concern". The IBM Data Governance Forum has since evolved to become the Compliance, Governance and Oversight Council (GGOC), which has a far broader focus than data governance. The CGOC has adopted the EDRM information governance reference model (IGRM) as a basis.
- *Data Management Association International and Data Management Body of Knowledge framework for data governance*: While Data Management Association International (DAMA) in its widely acknowledged Guide to the Data Management Body of Knowledge (DAMA-DMBOK2) uses the terms "data governance" rather than "information governance", in its preamble and definitions, the Association uses the terms data and information interchangeably. In the DAMA framework, what is described as data governance is described as IG elsewhere.
- *Electronic Discovery Reference Model*: The IGRM emerged from a need in the e-discovery community to have a framework for information management (EDRM, 2018). The primary focus is on e-discovery and, in doing so, it includes a heavy focus on the need to identify, capture and govern all information. The EDRM's IGRM is widely used and has been adopted by both ARMA (where it has been aligned with the Generally Accepted Recordkeeping Principles) and the CGOC (Franks, 2015).

Downloaded by Iowa State University At 10:03 22 January 2019 (PT)

- *Information Governance Initiative pinwheel*: Information Governance Initiative (2018) defines IG as the activities and technologies that people use to maximise the value of their information while minimising associated risks and costs. This initiative has not developed a model or framework *per se*, but is "a think tank and community dedicated to advancing the adoption of IG practices and technologies through research, events, advocacy and peer-to-peer networking". As such, the IGI has produced several industry reports which are of value. The focus is on a multi-disciplinary approach and the think tank has conducted valuable research to determine which disciplines could be part of an IG framework.

Within this emerging IG discipline, the IGA pinwheel infographic reflected in Figure 1 identifies the various potential facets of IG. The pinwheel clearly demonstrates the coordinating role of IG. It represents the promise of IG to finally put an end to the disjointed approach to information management that is witnessed in so many organisations, an approach that leads to poor governance outcomes and a failure to extract value from information (Information Governance Initiative, 2018; Ngoepe and Ngulube, 2013). This pinwheel was adopted in this study and helped to understand and identify the organisational disciplines and functions that should be represented in IG. The identified IG facets then informed the identification of stakeholders responsible for each element and the development of a national framework. The pinwheel offers great value as it identifies the elements/facets/disciplines which potentially comprise IG at the organisational level and, for this study, at the country level.

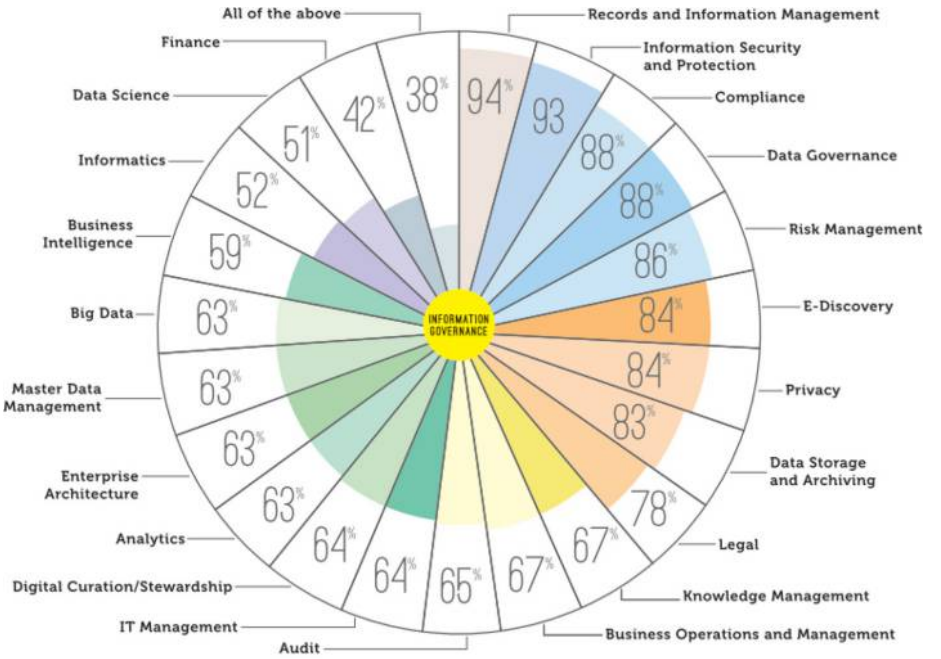


Figure 1.
The various facets of IG

Source: Information Governance Initiative (2018)

Downloaded by Iowa State University At 10:03 22 January 2019 (PT)

3. The role of standards in information governance

The importance of standards in IG has been raised by Lomas (2010) when arguing that:

> [. . .] embedding the international information security standard such as ISO 27001 in conjunction with the records management standard ISO 15489, will deliver a holistic information governance strategy that is responsive to change.

Indeed, most focus areas or disciplines within IG are addressed by at least one international standard or framework. The list reflected in Table I would be too comprehensive for this paper, but some key standards are listed as they highlight the fact that the disciplines are addressed in isolation. It must be noted that this is not designed to be a complete list, and the authors recognise that many industry bodies have developed other standards which are widely recognised and used by their respective communities. Furthermore, these standards are each developed under different technical committees, each with their own focus and area of specialisation. A process and framework for liaisons and stakeholder inclusion is integral to the development of standards; however, the risk always exists that a standard will take a direction to the detriment of some stakeholder requirements.

In South Africa, various governmental bodies have adopted international standards and use them either as guidelines or include them in their policy frameworks. For example, the NARSSA draws heavily on ISO records management standards in the development of policy. As is the case in many countries, the NARSSA Act does not apply to the private sector; hence, records management standards are used for guidance, although there is no legislation dictating that private organisations should use any particular standard. This is the case for almost all legislations having an IG component.

4. Methodology

This study adopted IGIs pinwheel facets of IG to design an integrated framework of elevating IG to the national level. The pinwheel helped to identify different facets of information disciplines and the responsible oversight mechanism for implementation in South Africa. The study relied on data obtained through content analysis of policy documents, legislative frameworks and literature review regarding the identified facets of IG in South Africa. The disciplines identified by the IGI have been used as a starting point

Table I. List of standards and frameworks for IG

Discipline	International standards
Records management	ISO 15489:2016 Records management ISO 30300 Family: Management system standard for records
Information security	ISO/IEC 27001: Information security management system
Information risk	ISO/IEC 27005: 2018 Information technology – Security techniques – Information security risk management
Corporate governance	ISO 19600:2014 Compliance management systems – Guidelines ISO/AWI 37000 Guidance for the governance of organisations (under development)
Privacy	ISO/IEC 29100 Privacy framework ISO 27018 Information technology — Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII Processors
Freedom of information	Few specific standards for FOI, but many related standards can be applied ISO/IEC 27038: 2014 – Information Technology – Security Techniques – Specification for digital redaction
IT governance	ISO/IEC 38500:2008

Downloaded by Iowa State University At 10:03 22 January 2019 (PT)

as this is a comprehensive list of potential disciplines which could be considered in a country-wide IG framework and ultimately implemented in organisations. These disciplines are listed and are used to determine whether they are catered for in the South African country governance framework. The analysis was done thematically as guided by the facets of the IGIs pinwheel. This also helped to identify the facets, related legislation and stakeholders.

5. Facets of information governance and responsible stakeholders in South Africa

There are a number of South African Government entities responsible for implementing various aspects of IG. Different public organisations are accountable for different aspects of IG, as identified in Figure 1. However, there is no coordinating entity to ensure alignment. Furthermore, there is a duplication of effort or conflict between the various resulting laws. For example, while public records can be accessed only after a period of 20 years in terms of the NARSSA Act, the Promotion of Access to Information Act makes provision for access of records without stipulating the age of a record. Table II provides a summary list of public entities responsible for IG facets in South Africa.

Table II. List of public entities in South Africa responsible for different IG facets

Organisation or accountable entity	Legislative mandate	Applicable legislation
Minister of Telecommunications and Postal Services	Facilitation and regulation of e-Government services and electronic communications and transactions with public and private bodies, institutions and citizens	Electronic Communication and Transaction (ECT) Act of 2002
Minister of Public Service and Administration (MPSA)	Mandated to foster good governance and sound administration in the public service Establish norms and standards related to, amongst other, information management and electronic government in the public service	The Public Service Act of 1994
Minister of Public Services and Administration	Sets out regulations for e-Government Requires all departments to manage information technology (IT) effectively and efficiently, taking into consideration that IT must improve the delivery of public services, the productivity of the department and the cost-efficiency of the department	Public Service Regulations of 2001
Minister of Public Services and Administration	Information security whereby the MPSA is required to issue a handbook called the Minimum Information Security Standards (MISS). All persons working with public service information resources will be required to comply with the MISS	Minimum Information Security Standard (MISS) of 1996
Government Information Technology Officer Council	The final area deals with interoperability whereby the MPSA in consultation with the Government	Minimum Interoperability Standards

(*continued*)

Downloaded by Iowa State University At 10:03 22 January 2019 (PT)

Organisation or accountable entity	Legislative mandate	Applicable legislation
SITA	Mandated to provide IT, information systems and related services to, or on behalf of, participating departments and in regard to these services, act as an agent of the South African Government with the Minister of Telecommunications and Postal services as the sole shareholder representing the government SITA Act requires the Agency to set standards for the interoperability of information systems and standards for a comprehensive information systems security environment for departments	SITA Act of 1998
National Planning Commission (NPC)	The strategic framework to form the basis of future government planning Although, the NDP 2030 does not mention e-government as a key enabler to the implementation thereof, it is important that the key elements of the NDP 2030 are taken into consideration in the development of the e-government strategy to ensure that the long-term objectives of the e-government strategy are aligned to those of the country	National Development Plan
Information regulator (Part of Department of Justice)	Development and implementation of privacy legislation	The Protection of Personal Information (POPI) Act of 2013
Human Rights Commission	Development and implementation of Freedom of Information Legislation. NOTE: This will fall under the auspices of the information regulator in future	Promotion of Access to Information Act
Not yet assigned	Freedom of Information implications	Protection of State Information Act (Bill)
Cabinet	National Integrated ICT Policy White Paper by cabinet in October 2016	
N/A	The Information Society and Development (ISAD) Plan of 2007	N
Department of Arts and Culture (DAC)	Records and archives management for government – via the NARSSA, a unit within the DAC	NARSSA Act of 1996 and its regulations
Auditor General of South Africa	Supreme audit institution within South Africa. Looks at strategic government objectives, programmes and initiatives and responds to identified risks	Public Audit Act of 2004
National Treasury	Allocation of budget and responsible for public finance management	Framework for managing programme performance information
Statistics South Africa	Collect statistical data in South Africa	South African statistics quality assurance framework
The Presidency	Monitoring and evaluation system. Aims to provide for oversight. Monitoring involves collecting, analysing and reporting data on inputs, activities, outputs, outcomes and impacts as well as external factors, in a way that supports effective management	Policy framework for the government-wide monitoring and evaluation system

Table II.

Downloaded by Iowa State University At 10:03 22 January 2019 (PT)

It is apparent from the list in Table II that different entities are tasked with different aspects of IG and there is no single coordinating or oversigsht entity. For example, the NARSSA is responsible for regulating records management in governmental bodies. In a study by Ngoepe and Keakopa (2011), it was established that the records management function, which is one facet of IG, would have more weight if it is placed either under the oversight of the AGSA or the Office of the President, as opposed to the NARSSA. In the South African e-government strategy, a number of challenges are identified, which are closely related to IG challenges (Department of Telecommunications and Postal Services, 2017), such as:

> Lack of synchronisation in approaches to digital transformation adopted by different government departments.
>
> Duplication of processes, databases, large-scale system incompatibilities and inefficiencies as major e-Government hindrances.
>
> Fragmentation of e-government initiatives within government has been identified as one of major challenges. e-government programme has not been directed and managed in a collaborative manner which leads to lack of accountability and responsibility due to the overlapping roles between government departments.
>
> There is no dedicated budget allocation for the specific implementation of e- government in South Africa. A number of initiatives are still run under separate budgets.
>
> Currently, there are still a number of government departments which make use of diverse applications, platforms, software and databases. Most of existing ICT systems were not designed to share information across departments. Cross departmental information sharing is essential to the success of e-government, thus there is a need for government to standardise the interchange requirements for the delivery and management of data.

While IG would have different implications for different sectors, the key elements of the framework remain intact. Governance elements remain the same across sectors, while the nature of the information to be managed will change. With regard to other industries, for example, the health-care sector has long been a global proponent of IG. The health-care sector defined IG in the late 1990s (Donaldson and Walker, 2004). In this regard, many references to IG refer to health-care records as IG. The banking industry has also been identified as a candidate for an IG framework (De Abreu Faria *et al.*, 2013) in which key aspects of IG are noted as:

> Information Governance is an emergent concept [...] developing and implementing an Information Governance Framework (IGF) is accepted as a natural course of action, though there is no one-size-fits-all solution [...] IGF is composed of multiple dimensions.

The dimensions identified align with many of the IG facets included in the IGI facets. However, in the public sector in South Africa, there is no evidence of any government IG framework, although most governments have clearly defined records management and information security frameworks.

6. Proposed national framework for information governance

As reflected in the proposed national framework for IG in Figure 2, the government entities identified have been mapped to the IGI facets to see which organisations are responsible for different facets of IG. The analysis clearly shows that there are multiple entities involved.

Downloaded by Iowa State University At 10:03 22 January 2019 (PT)

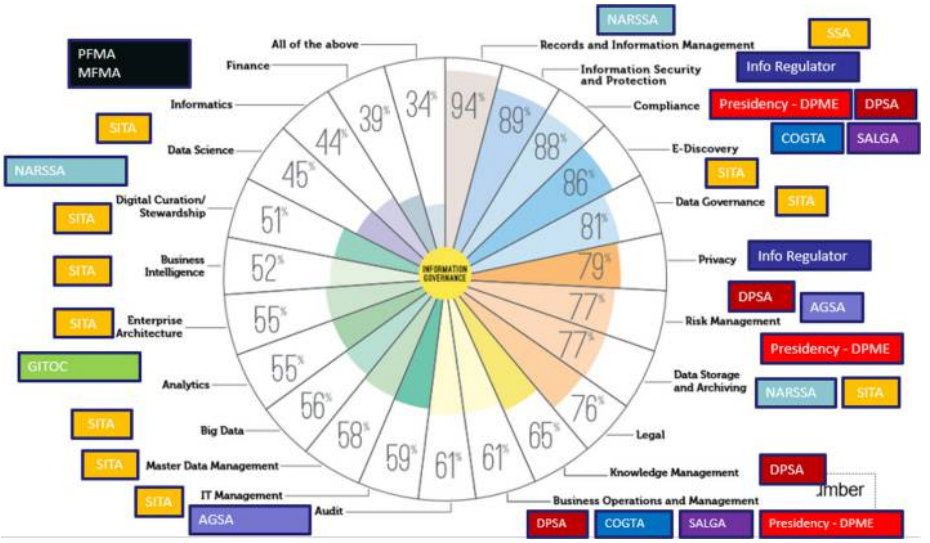


Figure 2.
Proposed national framework for IG

The identified IG domains include corporate governance, records management, IT governance, data privacy, knowledge management, master data management, information security and information risk.

As the facets of IG in South Africa are fragmented, a top-down approach to implementation is recommended as opposed to the current one, which does not yield any positive results. Implementation should start at the government level with legislative instruments, support infrastructure and mandate with the president as ultimately accountable. Then it can be cascaded down to the departmental level (ministerial) with a cabinet minister as the accounting officer. Once cascaded down to the organisational level, an IG business unit can be developed to be responsible for organisation-wide implementation. Currently, at most government entities in South Africa, this role is played by the Chief Information Officer who tends to focus more on IT than other facets of IG (Ngoepe and Ngulube, 2013). The key success factors, as identified by Mullon (2017) and Franks (2015), would be executive buy-in, alignment to corporate goals, integrated approach, change management and stakeholder inclusion. In this regard, information is regarded as a business asset.

7. Conclusion and recommendations

As stated in the discussion, IG is a high-level function with different facets that involve stakeholders across the government, each with its own expertise and mandate. There is generally no overarching structure responsible for the overall IG in South Africa as the elements are fragmented in various oversight mechanisms. The negative consequences of fragmentation or *silo* thinking include duplication of effort and missed opportunities for synergies. As a result, domains compete for limited resources and are "knee-jerk" responses to legislative, legal or risk drivers. As IG is not regulated and modelled at the country level, it is highly unlikely to filter down to organisations. Implementing IG at the country level will go a long way in helping to filter it down to the organisation level.

Downloaded by Iowa State University At 10:03 22 January 2019 (PT)

The study has presented a framework to ensure that IG is implemented at the country level with a single coordinating body established for oversight mechanism.

Finally, this study suggests the development of a country think tank on IG, as well as a centralised and coordinated governance structure. The think tank is to investigate the feasibility of establishment of a single coordinating entity for IG at a country level. For example, the information regulator can be assigned a broader scope as opposed to the current narrow scope of privacy and freedom of information, although with limited resources. A further study for assessing IG implementation at organisational level is recommended, as the elements of IG are not grouped together; for example, there are no IG divisions but chief information officers are mostly IT focused and IT driven. Without a proper IG framework at the country level, organisations are open to risks at various stages. It is concluded that failure to transform this pattern would pose a risk to digital transformation as the IG elements would continue to be fragmented.

Downloaded by Iowa State University At 10:03 22 January 2019 (PT)

References

ARMA International (2018), "Information governance body of knowledge (IGBok: the foundation", available at: www.arma.org/news/388383/ARMA-International-Releases-IGBOK-The-Foundation.htm (accessed 1 September 2018).

Association of Information and Image Management (AIIM) (2018), "Certified information professional by AIIM", available at: www.aiim.org/Education-Section/CIP (accessed 16 September 2018).

Chauke, T.A. (2018), "Integration of information management systems to enhance business intelligence at the department of transport in South Africa", MINF Dissertation, University of South Africa, Pretoria.

De Abreu Faria, F., Maçada, A.C. and Kumar, K. (2013), "Information governance in the banking industry", available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6480379 (accessed 7 December 2018).

Department of Telecommunications and Postal Services (2017), "Government gazette staatskoerant", available at: www.greengazette.co.za/pages/national-gazette-37230-of-17-january-2014-vol-583_20140117-GGN-37230-003 (accessed 28 July 2018).

Donaldson, A. and Walker, P. (2004), "Information governance–a view from the NHS", *International Journal of Medical Informatics*, Vol. 73 No. 3, pp. 281-284, available at: http://dx. doi.org/10.1016/j.ijmedinf.2003.11.009

EDRM (2018), "Information governance reference model", available at: www.edrm.net/frameworks-and-standards/information-governance-reference-model/ (accessed 20 August 2018).

Franks, P.C. (2013), *Records and Information Management*, ALA-Neal Schuman, Chicago.

Franks, P.C. (2015), "Information governance", in Duranti, L. and Franks, P.C. (Eds), *Encyclopaedia of Archival Science*, Rowman and Littlefield, Lanham, pp. 227-231.

Gartner (2018), "Gartner says master data management is critical to achieving effective information governance", available at: www.gartner.com/newsroom/id/1898914 (accessed 16 September 2018).

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

Information Governance Initiative (2018), "IGI state of the industry report volume III", available at: https://iginitiative.com/download-the-state-of-information-governance-report-volume-iii-6/ (accessed 29 July 2018).

Information Regulator (2018), "Information regulator South Africa", available at: www.justice.gov.za/inforeg/ (accessed 26 August 2018).

Institute of Directors in Southern Africa (2009), "King code of governance for South Africa", available at: www.ngopulse.org/sites/default/files/king_code_of_governance_for_sa_2009_updated_june_2012.pdf (accessed 15 June 2018).

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

Mojapelo, M.G. (2017), "Contribution of selected chapter nine institutions to records management in the public sector in South Africa", MINF dissertation, University of South Africa, Pretoria.

Mojapelo, M. and Ngoepe, M. (2017), "The role of the South African human rights commission to records management in the public sector in South Africa", *Journal of the South African Society of Archivists*, Vol. 50, pp. 28-55.

Mullon, P. (2017), "An integrated information governance approach", paper presented at the South African Society of Archivists Conference, Belville, 4-6 July.

Ngoepe, M. (2015), "Deployment of open source electronic content management software in national government departments in South Africa", *Journal of Science and Technology Policy Management*, Vol. 6 No. 3, pp. 190-205.

Ngoepe, M.S. (2012), "Fostering a framework to embed the records management function into the auditing process in the South African public sector", Doctoral dissertation, University of South Africa, Pretoria.

Ngoepe, M. and Keakopa, S.M. (2011), "An assessment of the state of national archival and records systems in the ESARBICA region – a South Africa-Botswana comparison", *Records Management Journal*, Vol. 21 No. 2, pp. 145-160.

Ngoepe, M. and Ngulube, P. (2013), "An exploration of the role of records management in corporate governance in South Africa", *SA Journal of Information Management*, Vol. 15 No. 2, p. 8, available at: http://dx.doi.org/10.4102/sajim.v15i2.575

Ngoepe, M. and Van der Walt, T. (2009), "An exploration of records management trends in the South African public sector", *Mousaion*, Vol. 27 No. 1, pp. 116-136.

Smallwood, R.F. (2014), *Information Governance: Concepts, Strategies, and Best Practices*, Wiley, CA.

Further reading

DAMA (2017), *DAMA-DMBok Data Management Body of Knowledge*, 2nd ed. Technics Publications, Basking Ridge.

Bridges, L. (2014), "Information governance and assurance: reducing risk, promoting policy", *Records Management Journal*, Vol. 24 No. 3, pp. 253-255, available at: https://doi.org/10.1108/RMJ-08-2014-0034

About the authors

Paul Anthony Mullon is a PhD Candidate at the University of South Africa in information governance (IG). He is the Founder of a consulting company COR Concepts, which specialises in IG. He is currently serving in the national committee of the South African Society of Archivists (SASA). Mr Mullon was the Chairperson of SASA from 2015 to 2017. He has implemented a number of IG projects in southern Africa. Mr Mullon is involved in a number of committees in South Africa. He is currently the Convener of the working committee for TC171 at the South African Bureau of Standards for the generation of national standards. He is currently serving in Gauteng Provincial Archives Council, which advises the member of the executive committee on issues relating to archives and records management in the province.

Downloaded by Iowa State University At 10:03 22 January 2019 (PT)

Mpho Ngoepe is a Professor in the Department of Information Science at the University of South Africa (Unisa). Prior to his current position at Unisa, Professor Ngoepe has worked for the United Nations Children's Fund, Auditor-General South Africa and the National Archives of South Africa. He is serving in the national committee of the SASA (2009-2019) and the board of Eastern and Southern Regional Branch of the International Council on Archives (2009-2019) as an Editor of the journals. He also serves on the advisory council of the National Archives of South Africa in his capacity as the Chairperson of Gauteng Provincial Archives. He is the Director of the African team for the multi-national, interdisciplinary research project exploring issues concerning digital records called the International Research on Permanent Authentic Records in Electronic Systems (InterPARES Trust) (2013-2018). Mpho Ngoepe is the corresponding author and can be contacted at: ngoepms@unisa.ac.za

Downloaded by Iowa State University At 10:03 22 January 2019 (PT)

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**