Africa's Public Service Delivery and Performance Review
ISSN: (Online) 2310-2152, (Print) 2310-2195

The role of data and information security governance in protecting public sector data and information assets in national government in South Africa

Authors:
Lucia Masilela[1]
Danielle Nel[1]

Affiliations:
[1]Department of Public Management and Governance, School of Public Management, Governance and Public Policy, University of Johannesburg, Johannesburg, South Africa

Corresponding author:
Lucia Masilela,
luciamasilela@gmail.com

Dates:
Received: 11 Feb. 2020
Accepted: 15 Sept. 2020
Published: 21 Jan. 2021

How to cite this article:
Masilela, L. & Nel, D., 2021, 'The role of data and information security governance in protecting public sector data and information assets in national government in South Africa', *Africa's Public Service Delivery and Performance Review* 9(1), a385. https://doi.org/10.4102/apsdpr.v9i1.385

Background: The deployment of information and communications technology (ICT) in the public sector, has been exposed to increasing security breaches and cyber-related crimes that have resulted in unauthorised access, theft, fraud and misuse of highly confidential, classified and sensitive public sector data and information (PSDI) assets. The government, as one of the biggest collectors and distributors of PSDI assets, needs to be constantly aware of the risks associated with the collection, classification, storage and dissemination of critical PSDI assets. The lack of sufficient data and information security measures could pose significant security risks that could impact on state security, thus causing national working relationships to be strained, which presents gaps and opportunities for external intruders to capitalise on the mistrust of the government to infiltrate further attacks on critical Information Technology (IT) infrastructure and systems. In order to mitigate and counteract critical and sensitive data and information-related crimes, the government must understand and analyse the importance of data and information security governance (DISG) and how it should be institutionalised through an integrated approach to improve and protect PSDI assets.

Aim: The aim of this article is to analyse the institutionalisation of DISG measures government has implemented towards the protection of PSDI assets.

Setting: The research setting is in three national government departments, namely the Department of Energy (DoE), the Department of Environmental Affairs (DEA) and the Department of Science and Technology (DST). This study investigates how the strategic combination of data governance (DG) and information security governance (ISG) practices and principles could be implemented and incorporated as one of the various approaches in public sector institutions to improve the DISG management functions of an organisation's overall data and information systems and processes.

Methods: The research approach is qualitative, and the research methodology includes a multiple case study design. Data were collected through semi-structured interviews and was triangulated with literature review. Primary data was analysed using thematic analysis.

Results: The research findings are presented according to the McKinsey 7S model, which served as the analytical framework in the study. The research findings indicate that the institutionalisation of DISG management practices and functions in the South African public sector context are very limited, and there is a dominant focus on IT and IT security. It was also identified that DISG policies, practices, and systems have been found to be lacking in public sector management and governance functions.

Conclusion: The study concludes that there is currently a lack of sufficient DISG policies, management practices and systems, particularly in the national sphere of government.

Keywords: information technology; digital government; data governance; information security; information and security governance.

Introduction

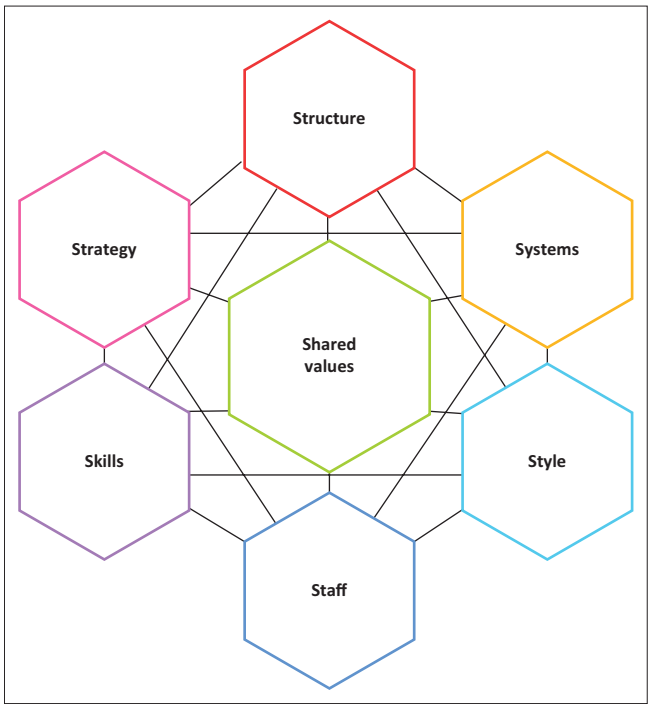
The changing global environment influenced and driven by the Fourth Industrial Revolution (4IR) through the introduction of new and advanced technological theories, processes, systems and practices requires the government to formulate and implement conducive policies, frameworks, laws, rules and regulations in order for the 4IR to successfully achieve, accommodate and transition South Africa's efforts towards improved security

practices and measures towards its public sector data and information (PSDI) assets. The security landscape of information technology (IT) on both local and international scale is constantly evolving and changes daily. This requires consistent efforts to keep up with best practices to adequately protect PSDI assets and to minimise the risks associated with the theft, misuse, unauthorised access and fraudulent activities associated with cybercrime. The government must therefore implement proactive measures and approaches towards the protection of its PSDI. The purpose of this study is therefore to determine how the institutionalisation of data and information security governance (DISG) management functions and practices in the public sector can effectively and efficiently provide best practices and measures for improved PSDI security. Firstly, this article will provide a brief discussion on the theoretical perspective of the McKinsey 7S Model that is used as an analytical framework in the analysis and presentation of research findings in this article. Secondly, the chosen scientific and methodological approach for this study will be discussed. Thirdly, this article will discuss the research findings according to the McKinsey 7S Model. Lastly, conclusions and recommendations will be provided on how to improve DISG practices within the public sector.

Theoretical perspective: The McKinsey 7S model

The McKinsey 7S model is an analytical framework used to gain in-depth analysis of organisational functionality and the integration of systems. The model is based on organisational theory, which states that if an organisation is to perform at its optimum best, the seven elements of structure, systems, style, staff, skills, strategy and shared values must be integrated and aligned and mutually reinforced to achieve and maintain organisational synergy. The McKinsey 7S model has gained popularity in the academic and professional fields of study as a strategic planning tool because the model comprehensively illustrates and indicates how the seven elements of structure, systems, style, staff, skills, strategy and shared values are aligned and integrated as a whole to achieve and maintain efficiency and effectiveness in an organisation (De Vlieger 2013; Ravanfar 2015:8–9; Waterman et al. 1980:14–20). Furthermore, the McKinsey 7S model emphasises that organisations must consider that internal changes to one or more areas of the model will ultimately have an impact of the functionality of the other areas in the model. As a result, when organisational management intends to make any strategic changes to its internal processes, systems and functions, it must analyse, compare and contrast how these changes will have a positive or negative influence and impact on the functionality of the other areas before committing to the final roll-out plan chosen by the management (De Vlieger 2013; Ravanfar 2015:8–9; Waterman et al. 1980:14–20).

Figure 1 illustrates the significant features of the McKinsey 7S model in that it represents the interrelatedness and connectedness of the seven areas in an institution's organisational design.



Source: De Vlieger, R., 2013, *McKinsey 7S Model*, viewed 22 June 2019, from https://www.calltheone.com/en/consultancy/7s-model

FIGURE 1: The seven elements of the McKinsey 7S model

The interdependency of these seven areas has been further broken down and categorised as either soft or hard elements of the McKinsey 7S model.

The hard factors of the McKinsey 7S model

The hard elements or factors of the McKinsey 7S model have been said to be easier to identify and analyse and can be found in the form of documentation. The hard factors include the organisation's strategy, structure and systems.

Strategy

An organisation's strategy consists of a well-developed plan designed by Senior Organisational Management (SOM) for the firm towards achieving a competitive advantage in its respective industry market. According to the McKinsey 7S model, strategy therefore particularly looks at the vision, mission, goals and objectives of an organisation; a sound decision-making channel and structure by management; the feasibility and sustainability of long- and short-term strategic programmes; and projects' goals and objectives. The key to determining whether an organisation's strategy is compatible with the McKinsey 7S model requires an analysis of how the organisation's strategy links, integrates and transitions with the other six areas of the model and if these elements are aligned to the overall production, feasibility and functionality of the organisation (De Vlieger 2013; Ravanfar 2015:8–9; Waterman et al. 1980:14–20).

Structure

The word 'structure' refers to how an organisation is organised to fulfil and perform its roles, functions and responsibilities. The McKinsey 7S model analyses structure by examining:

- the organisational chart and the interconnections between various departmental functional activities;
- hierarchical structures from senior, middle and lower levels of management;
- the conjunction of decentralised decision-making structures (bottom-up approaches), as well as centralised decision-making structures (top-down approaches);
- the combination of pyramidal, matrix or networked structures to collectively achieve and accomplish organisational goals and objectives; and
- the lines, channels and structures of communication between the different levels, positions and functions of an organisation's departments (De Vlieger 2013; Ravanfar 2015:8–9; Waterman et al. 1980:14–20).

Systems

Systems in an organisation can be described as those elements that define the functional flow of activities related to the daily operations of an organisation. These often include the organisation's core functions, support systems, procedures, processes and routines that are integrated to ensure the functionality and management of the organisation. Organisations' systems can include:

- human resources;
- financial management systems;
- supply chain;
- transport;
- procurement; and
- information and communications technology (ICT) processes (De Vlieger 2013; Ravanfar 2015:8–9; Waterman et al. 1980:14–20).

The soft factors of the McKinsey 7S model

This section discusses the 'soft' factors of the McKinsey 7S model, which are style, staff, skills and shared values. According to the McKinsey 7S model, these factors are considered to be more difficult to identify because the elements are consistently evolving, developing and changing in an organisation's internal environment. These elements have been found to be influenced and determined by the employees of the organisation and the manner in which their work is performed. It is therefore imperative that organisational management exercises caution when making changes to one or more of the above-mentioned elements as they have a great influence and impact on the hard factors of the McKinsey 7S model (De Vlieger 2013; Ravanfar 2015:8–9; Waterman et al. 1980:14–20).

Style

According to the McKinsey 7S model, style refers to the organisational culture of a firm, and there are two components of an organisation's style or culture, namely organisational management and management style. Organisational management refers to values, beliefs, norms, opinions and standards that develop and become heavily present, active and practised in an organisation. These elements create unique organisational features, social events and the shaping of values throughout the entire organisational structure. Managers' management style and the culture of the organisation can be related to the behaviour of senior management and managerial staff in achieving and maintaining an organisation's goals and objectives, as well as how they interact with subordinate staff (De Vlieger 2013; Ravanfar 2015:8–9; Waterman et al. 1980:14–20).

Staff

An organisation's staff consists of job families that develop over time and that play a significant role in the collective success of an organisation's overall goals and objectives. The McKinsey 7S model examines factors such as:

- how many employees an organisation has;
- what the internal recruitment processes and procedures are that must be adhered to;
- how employees are encouraged and motivated to perform at their optimum best; and
- how employees are recognised and rewarded for their efforts and contributions towards the organisation's goals and objectives (De Vlieger 2013; Ravanfar 2015:8–9; Waterman et al. 1980:14–20).

Skills

The skills of an organisation's workforce consist of the distinctive competencies that staff at all levels of an organisation can contribute to the organisation that make it distinctively unique from other firms through the offerings of new and untapped knowledge, skills and capabilities that lead to the development, advancement and investment in staff development, skills and leadership skills (De Vlieger 2013; Ravanfar 2015:8–9; Waterman et al. 1980:14–20).

Shared values

An organisation's shared values consist of elements that act as an organisation's conscience and provide senior management, managerial staff and employees with guidance in times of turmoil and crises to handle and overcome internal challenges. Shared values are an organisation's guided concepts, themes, principles and practices that are considered the foundational building blocks upon which an organisation is firmly built (De Vlieger 2013; Ravanfar 2015:8–9; Waterman et al. 1980:14–20).

Scientific and methodological approach

The methodological approach determined the data-collection techniques that were used in this study; the chosen

methodological approach for this research study was a qualitative research approach. The qualitative research approach was selected for this particular research study because it is primarily concerned with how the social world is interpreted, perceived, understood and experienced by others. Because of the nature and requirements of this research project, the qualitative research method was chosen. According to Aktinson, Coofey and Delamont (2001:7), 'qualitative research is a form of social inquiry that focuses on the way people interpret and make sense of their experiences and the world in which they live'. Qualitative research is therefore said to be an umbrella term that covers numerous approaches, strategies and frameworks that exist in a qualitative research study (Aktinson et al. 2001:7). The unit of analysis in this study comprised three national government departments in South Africa, namely the Department of Energy (DoE), the Department of Environmental Affairs (DEA) and Department of Science and Technology (DST), at the national sphere of government. These research participants included SOM who were primarily responsible for the protection of PSDI in their respective departments. Furthermore, the sample included the chief directors (CDs), directors general (DGs) and deputy directors general (DDGs) of each department. These participants were chosen on the basis of investigating how DISG management's functions and practices are embedded to protect its PSDI against the risks associated with the misuse, theft, loss and damage of critical PSDI assets in each respective government department. The use of semi-structured interviews enabled primary data collection through direct communication and interaction with the chosen participants (De Vos et al. 2011:397).

The use of interviews allowed the opportunity to conduct semi-structured interviews with CDs, DGs and DDGs in the DoE, DEA and DST to gain a rich understanding of their views, opinions, roles and responsibilities. These questions were designed to guide the direction of the data collection from senior management officials for the purposes of finding answers to the research question and objectives. The goal of using interviews in qualitative research is therefore to view the research topic from the perspective of the interview participants, and, in the case of this study, to understand their perspective of DISG in their respective departments. Furthermore, the study made use of thematic analysis of interview data. Braun and Clarke (2006) developed a six-phase framework for conducting a systematic and iterative analysis of data in a qualitative research study to identify and present patterns or themes in a researcher's data set. The interview responses were analysed by using thematic analysis. In qualitative research, thematic analysis can be used as a method to analyse present classifications, themes and patterns that are relevant and related to the raw data that were collected during the research process.

Findings

The interview data for this study were collected through one-on-one interviews with SOM in the DoE, DEA and DST. The participants were identified as skilled, knowledgeable and experienced personnel who specialise in protection of PSDI assets in their respective departments. The interview results and interpretations discussed below do represent a generalisation of the interview data. The interview results and interpretations are derived from the semi-structured interview questionnaire. The following section aims to present the interview results according to the McKinsey 7S model.

Strategy

All three departments are situated at the national sphere of government and are primarily involved in policymaking and implementation. These departments are therefore required to ensure that there is transparency in the departments and throughout the government holistically. As a result, all data and information assets are subject to numerous internal and external rules, laws and regulations.

Strategy of the Department of Environmental Affairs

In the DEA, the following have been implemented as departmental policies and frameworks for ensuring DISG:

- **Governance of Information Technology Policy and Information Technology Governance Framework:** These frameworks have been established as tools to achieve and ensure the protection of data and information assets. These IT strategies have been developed to assist in the guidance of the DEA's long-term strategic plans, tools and mechanisms that can be developed, implemented or amended in an attempt to improve current IT and IT security protection strategies.
- **State Information Technology Agency Act (RSA 1998a):** This Act stipulates the rules, laws and regulations to public sector institutions for the provision of IT and information systems as tools for the delivery of public sector goods and services in the related field and area of ICT.
- **Public Financial Management Act of 1999 (RSA 1999):** Particularly Chapter 4 is adhered to in order to provide the DEA with the stipulated rules, laws and guidelines regarding the regulation of financial management and budgeting of national departments. The Public Finance Management Act (PFMA) therefore provides guidelines in terms of annual IT infrastructure spending and budgeting in a national department.
- **Department of Public Service and Administration Framework for Information Technology Security:** This is used as a guideline to achieve and ensure the protection of data and information assets through ICT systems and infrastructure. These IT strategies have been developed to assist in the guidance of the DEA's long-term strategic plans, tools and mechanisms that can be developed, implemented or amended in an attempt to improve current data and information protection strategies.

Strategy of the Department of Science and Technology

The DST is guided and advised by its legal department to ensure compliance with all current and existing laws and

regulations in the public service. The legal department further assesses and evaluates the DST's compliance and provides feedback and makes the necessary recommendations. The Auditor-General as an external entity also conducts an annual assessment and evaluation of the DST's compliance with laws and regulations and provides a feedback report with its own findings, conclusions and recommendations for compliance. Furthermore, the DST has implemented the following internal policies:

- **Email, Intranet and Internet Policy:** This policy stipulates and has guidelines as to how departmental staff can use or should be using their work email addresses, and the types of data and information that can be distributed through the DST's email server (this also protects and ensures that all electronic communication and the context in emails are therefore the property of the DST). With regard to intranet and Internet usage, the policy stipulates and gives guidelines regarding the Internet sites that employees may and may not access. The policy also has a detailed contact list that is made available to all employees in order for them to be knowledgeable and resourceful regarding who they can contact if there are any queries, problems or risks that have been identified.
- **Computing Asset Replacement Policy:** This policy was established and implemented for cases such as the loss or theft or upgrading of an electronic device belonging to the DST, where all data and information assets are cleaned or wiped physically or remotely.
- **Infrastructure Protection Policy:** This policy deals with the physical infrastructure of the DST, particularly its critical rooms or departmental floors or levels. This policy indicates and specifies the rules, regulations and procedural steps that must be adhered to when an employee wants to enter a particular departmental floor or room to strengthen the DST's efforts towards securing its physical security measures.
- **Security Policy:** This policy deals with all matters relating to the length of passwords, how often the password must be changed, encryption of documents, upgrading of software and hardware, firewalls, etc.
- **Clean Desk Policy:** This policy requests all employees to ensure that they do not leave classified or confidential or critical or sensitive data and information assets unattended on office desks and that these must be locked up in their departmental safes situated at each of their own desks. The Security Unit enforces these measures by conducting random spot-checks to identify and determine if any classified or confidential or critical or sensitive data and information have been left unattended and it also provides internal reports to management and relevant parties.

Strategy of the Department of Energy

To ensure that the DoE's strategic planning processes are adequately implemented throughout the entire organisation, the DoE, through its Executive Committee, has established a Strategic Steering Committee. The Strategic Steering Committee has been tasked with the responsibility of driving the entire strategic agenda and planning processes in the organisation and includes branch representatives from both support and line functionaries. Furthermore, the Strategic Steering Committee has formulated a 'Strategic Alignment Document' for ensuring that the DoE's strategic plans and its annual performance plans are aligned to the Medium-Term Strategic Framework, as well as the National Development Plan (GCIS 2015:32).

The DoE has implemented the following five departmental policies for the protection of its data and information assets:

- **Information Security Policy:** This policy stipulates and provides guidelines related to the implementation and use of patch management programmes and systems, the use of vulnerability assessments regarding the DoE's IT systems and infrastructure, as well as the implementation and use of intrusion detection systems to protect the department's internal systems against viruses and phishing attacks.
- **Firewall Policy:** This policy stipulates the rules and regulations regarding the DoE's ability and authorisation to enable or disable certain types of network traffic from accessing the department's systems and server bases to effectively mitigate the risks associated with cyber viruses from external sources.
- **Backup Policy:** This policy consists of the guidelines related to predefined and set schedules for backing up the DoE's internal servers and other electronic systems and devices. This is done to ensure that employees are knowledgeable and aware of when backup processes must take place to adequately protect and safeguard the DoE's data and information assets.
- **Logical Access Control Policy:** This policy is used as a guideline regarding the implementation and use of uniquely designed tools and protocols for the identification, authorisation, accessibility and authentication of departmental staff related to the department's internal hardware, systems and programs.
- **Acceptable Use Policy:** This policy is used to guide all department staff regarding the restrictions and permissions of using external networks, websites, systems and third-party applications.

Structure

Each of the three government departments, situated at the national sphere of government, has therefore implemented certain structures for the handling of its data and information assets to ensure that departmental staff have an understanding of their respective roles, responsibilities and functions in the processes of collecting, classifying and storing the government's PSDI assets. All government departments have their own unique internal processes for the classification of classified or confidential or critical or sensitive data and information assets.

Structure of the Department of Environmental Affairs

The DEA is situated at the national sphere and has policymaking and implementation roles, responsibilities and

functions that are derived from section 24 of the Constitution, which is geared towards the protection of South Africa's oceans, biodiversity and ecosystems. The purpose of the DEA's structural context is to ensure that it provides strategic leadership and centralised administrative functions and executive support and efficient corporate services that will facilitate achieving effective governance management practices, theories and functions towards environmental protection. The following departmental structures have been identified in the DEA:

- **Unit of Financial Management Service (Chief Financial Officer [CFO]):** The CFO manages and monitors the provision of sound financial management practices and principles related to the department's funds both at head office in Pretoria and in Cape Town, South Africa.
- **Branch: (Chief Operating Officer [COO]):** The COO manages the provision of operational support services related to strategic business planning, risk management and organisational performance management.
- **Branch: Legal Authorisations and Compliance Inspectorate:** The purpose of this branch is to develop and foster an enabling legal and licensing or authorising system that will ensure the promotion, enforcement and compliance of citizens, private sector businesses, supply chain partners and various other stakeholders in South Africa.
- **Branch: Oceans and Coastal Management:** This branch establishes and implements effective management systems, programmes and mechanisms for ocean and coastal environmental management.
- **Branch: Climate Change, Air Quality, and Sustainable Development:** The purpose of this branch is to identify, analyse, collect, refine, collate, store, popularise and distribute data and information assets on current and existing climate change, air quality and sustainable development data.
- **Branch: Biodiversity and Conservation:** This branch ensures the regulation and management of the country's biodiversity, heritage and conservation matters in an effective, efficient and sustainable manner by mitigating the risks, threats and challenges that impact the achievement of sustainable and inclusive socioeconomic growth and development for the country's citizenry.
- **Branch: Environmental Programmes:** This branch identifies and implements tools and mechanisms that can be developed for and targeted at poverty alleviation by exploring avenues through accelerating job creation and developing and improving skills and knowledge.
- **Branch: Chemicals and Waste Management:** This branch develops and implements processes and systems that ensure the effective and efficient functionality of administrative activities of the department's authorisation of waste management activities and ensures the reduction of hazardous and contaminated waste streams into the environment and conserved ecosystems (DEA 2016: internet source, 2018:9–10, 15–17).

Structure of the Department of Science and Technology

The DST's national policymaking and implementation functions, roles and responsibilities are derived from the White Paper on Science and Technology of 1996 (RSA 1996). The DST has therefore ensured that it provides best practices, leadership, resources and a conducive environment for research in science, technology and innovation (ST&I) projects and programmes throughout South Africa.

The following departmental structures have been identified in the DST:

- **Programme 1A and 1B: Institutional Planning and Support and Corporate Services:** Institutional Planning and Support Corporate Services are involved in the identification, formulation and implementation of strategic plans, annual performance plans and the operational plans of the DST and its public entities by ensuring that they are aligned to those stipulated in the national priorities.
- **Programme 2: Technology and Innovation:** This programme is responsible for identifying and implementing measures that will enable the DST to provide research and development initiatives and outputs in key strategic and emerging areas such as space science, biotechnology, nanotechnology, robotics, indigenous knowledge systems, intellectual property management, technology transfer and technology commercialisation.
- **Programme 3: International Cooperation and Resources:** This programme strategically develops, promotes and manages all matters related to international relationships, opportunities, as well as science and technology agreements that are aimed at strengthening the National System of Innovation.
- **Programme 4: Research Development and Support:** This programme is responsible for providing a conducive and enabling environment for the production of high-quality and standardised research and knowledge outputs geared towards the strategic development and growth of basic and priority science areas.
- **Programme 5: Socioeconomic Innovation Partnerships:** This programme is responsible for identifying, formulating and committing to strategic partnerships with other government departments, industry partners, research institutions and other committees that are involved in scientific, technological and innovative research projects and programmes (DST 2018:28–87).

Structure of the Department of Energy

The DoE's national policymaking and implementation functions, roles and responsibilities are derived from the White Paper on Energy Policy of 1998 (RSA 1998b), the White Paper on Renewable Energy of 2003 (RSA 2003) and the National Energy Efficiency Strategy. The purpose of the DoE's structural context is to ensure that it provides good corporate governance practices and principles towards achieving sustainable energy supply in South Africa.

The following departmental structures have been identified in the DoE:

- **Programme 1: Administration:** This programme provides executive coordination, facilitation and administrative support services to the Ministry's office and the offices of the DGs and DDGs.
- **Programme 2: Energy Policy and Planning:** This programme is responsible for providing evidence-based planning, policy formulation and setting, as well as investment decisions in the energy sector.
- **Programme 3: Petroleum and Petroleum Products Regulation:** This programme manages the regulation of petroleum and petroleum products to ensure that there is a sufficient petroleum supply and a well-managed and functioning petroleum industry.
- **Programme 4: Electrification and Energy Programme and Project Management:** This programme is responsible for managing, coordinating and monitoring all programmes and programmes related to the access of energy.
- **Programme 5: Nuclear Energy:** This programme assists in managing the South African nuclear energy industry, as well as controlling nuclear material by aligning and integrating departmental functions with international best practices and principles.
- **Programme 6: Clean Energy:** The Clean Energy Programme is responsible for managing and facilitating in the formulation, development and implementation of clear energy initiatives, programmes and projects within the energy sector (DoE 2015:23–83).

Systems

From an IT perspective, it is not the responsibility of the IT department to determine the internal processes of data- and information-classification processes. The only function that the IT department has is to develop and implement the security measures and systems needed for the protection of critical assets as indicated by the Records Management Directorate's processes. The processes related to the classification of data and information assets are therefore explicitly facilitated by the Records Management Units.

Systems of the Department of Environmental Affairs

The DEA implemented a number of systems that are utilised to ensure intensive, effective and efficient efforts towards the protection and sustainability of South Africa's environment and ecosystems. Through the use of advanced and improved DISG infrastructure and resources, the DEA has uniquely designed and implemented information systems that allow the consistent, free flow of data and information assets throughout the department. The DEA has an array of directorates, department divisions and functional responsibilities that require accessible, user-friendly and effective information systems for the delivery of environmental goods and services, as well as for ensuring the operational efficiency and productivity of the DEA. The following were identified as data and information systems that have been developed to aid to the protection of PSDI in the DEA:

- **Email Archiving Solution:** The Email Archiving Solution was implemented by the IT department as a system that collects and stores all data and information transmitted via email between the DEA, citizens, supply chain partners, private investors and various other stakeholder partners. This was implemented to assist in compliance with the Electronic Communications and Transactions (ECT) Act, as well as the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) of 2002 (RSA 2002), to protect both employees at the DEA and South African citizens in the transmission of electronically communicated data and information.
- **The Data Linkage Prevention Solution:** This is a software program and system developed by the IT department that can be installed internally on all the DEA's technological bases (desktops, laptops, mobile handsets and handheld tablets) to keep record of all the types of data and information that are electronically transmitted or shared between SOM, internal staff and external persons. The Data Linkage Prevention solution allows the DEA to place restrictions on the sharing of confidential or sensitive or secret or classified data and information assets through email, printing, scanning, saving and copying of data and information assets onto flash drives, hard drives, etc.
- **Access Control Systems:** The Access Control Systems are used to determine and decide who has access to what types of data and information assets in the DEA, as well as the level of access that the employee will be granted to confidential or top secret or critical or sensitive data and information assets. This system is administered and facilitated by the IT department.
- **Electronic Document Management System (EDMS):** All data and information asset submissions and approvals are compiled and completed via the EDMS. These documents are therefore uploaded and backed up onto the EDMS; the server is located on the department's premises. All the documents that are collected and stored onto the EDMS are sent to an offsite vendor on a weekly basis. The EDMS is administered and facilitated by the Records Management Unit.

Systems of the Department of Science and Technology

The DST has heavily invested in the development and implementation of a number of scientific, technological and innovative data and information systems that are geared towards the provision of highly standardised knowledge and research outputs in the areas of ST&I. The data and information systems that have been established by the DST are targeted at formulating a rich knowledge base that makes use of groundbreaking ST&I research outputs as a tool for assisting the government towards its long-term socioeconomic goals and objectives. The deployment of advanced ICTs has given the DST the opportunity of utilising accessible, user-friendly and effective information systems for the delivery of

highly standardised ST&I strategies, programmes and projects. The DST has an array of directorates, department divisions and functional responsibilities that have uniquely designed information systems that are custom made for the needs of freely exchanging data and information assets internally in the DST as well as externally to the country's citizenry, private sector institutions, supply chain partners, academic and research institutes, international bodies and various other stakeholders.

The following were identified as data and information systems that have been developed to aid the protection of PSDI in the DST:

- **Document Management System:** The Document Management System is a documentation system where all classified or confidential or critical or sensitive electronic data and information assets are stored and actioned on the system. The system is also integrated to action other important data and information pertaining to the department. The system is adequately protected with strong security controls and measures to mitigate hacking and theft of valuable data and information assets.
- **Intrusion Detection System:** The Intrusion Detection System is a uniquely designed system that identifies, mitigates and provides detailed feedback reports regarding potential electronic attacks on the department's IT-related systems. This system also informs the DST when the attack was attempted, what type of attack it was and when it was mitigated.
- **Enterprise Content Management System:** This system is utilised to conduct internal audit trails and feedback reports of which data and information systems have been accessed by which employees. Furthermore, this system has a secure repository with audit trail access control.

Systems of the Department of Energy

The DoE is mandated to ensure the provision of secure and sustainable energy supply sources in South Africa to achieve and encourage the collective socioeconomic growth and development of the country. Furthermore, the DoE is also responsible for ensuring that the same provision of energy supply in the country is managed effectively and efficiently to minimise its impact on the environment through the formulation, implementation and maintenance of sustainable and renewable energy supply technologies, policies, principles and practices. The DoE is tasked with the responsibility of ensuring that it collects, refines, stores and distributes information assets to the country's citizenry data regarding the country's energy sources and environments that are factual, reliable, timely and freely accessible. The DoE has an array of directorates, department divisions and functional responsibilities that constantly need access to reliable, factual and unbiased data and information assets for the purpose of making sound decisions. As a result, the DoE must develop and implement information systems that can be custom made for the purpose of freely exchanging data and information assets internally and to its stakeholder partners in the energy sector.

The following information system was identified in the DoE:

- **The Electronic Document Management System:** The DoE is currently in the middle of a process in which it will implement and make use of the electronic document management system (EDMS) for the classification of its data and information assets. The system is currently manual, whereby data capturers capture the document information and manually upload, categorise and store the documents on the system. Once the EDMS is in place for the classification of the department's data and information assets which will enable an electronic process in the system, the DoE's documents will be adequately protected through uniquely designed security systems. The EDMS will therefore make it easier and more efficient to classify all types of documents, including lowervalue documents and sensitive documents. It must be noted that these types of systems and processes differ from department to department.

Style, staff, skills and shared values

The ability to improve DISG theories, practices and management functions require intensive approaches to developing and instilling DISG cultures, plans, strategies, goals and objectives in public sector institutions. The following have been identified as the style, staff, skills and shared values of the DEA, DST and DoE:

Style, staff, skills and shared values of the Department of Environmental Affairs

Section 24 of the Constitution of 1996 empowers the DEA to explore and apply rigorous policies, laws and regulations in pursuit of effective and efficient tools and approaches for the protection and sustainability of South Africa's natural environment and ecosystems. The DEA's organisational culture is people centric to promote work–life balance, collegiality, empathy and teamwork. The DEA therefore strives to uphold values of integrity, professionalism, ethical conduct and diversity. The DEA also intends to uphold its culture and shared values by consistently striving towards employing principles and practices that are environmentally conscious and sustainable (DST 2018:1).

Style, staff, skills and shared values of the Department of Science and Technology

The White Paper on Science and Technology of 1996 (RSA 1996) empowers the DST to explore and apply rigorous policies, laws and regulations in pursuit of innovative tools and approaches towards the delivery and achievement of ST&I outputs to ensure sustainable socioeconomic growth and development in South Africa. The DST's vision and mission are driven by the need to ensure increased well-being and prosperity of the community's lives through the

strategic use of ST&I. This has been achieved through strong leadership skills, an enabling environment and the efficient use of scarce resources for ST&I in support of South Africa's social and economic development. The organisational culture is one that promotes professionalism through high-quality performance internally and externally to its stakeholder partners through the use of innovative solutions to counteract service delivery challenges to achieve efficiency and effectiveness of public sector goods and services. The DST therefore aims to demonstrate and uphold its ethical behaviour by being accountable, transparent and interactive with its stakeholder partners (DST 2018:26).

Style, staff, skills and shared values of the Department of Energy

The DoE has the legal mandate to ensure secure, sufficient and sustainable energy sources geared towards socioeconomic growth and development for all those who live within the borders of South Africa. This is driven by the DoE's dedication and focus towards the formulation, implementation and overseeing of energy policies, regulatory frameworks, energy security measures and the promotion of environmentally friendly energy sources in its respective sector. The service delivery approach of the DoE is guided and driven by its internal value systems, which include the Batho Pele principles and practices towards improved service delivery in the energy sector. The DoE firmly believes in portraying strong ethical principles, honesty and integrity in its respective fields of work and in the communities it operates and engages with. This has led to the delivery of professional, accountable and transparent public service delivery outputs in the energy sector (DoE 2015:16).

Conclusion

Public sector institutions are particularly focussed on the protection of their IT systems and infrastructure and lack effective DISG systems to improve the protection of PSDI. The formulation and implementation of integrated DISG management practices and approaches could assist the government in its efforts to counteract cybercrime, as well as ensuring its sustainable and long-term goals and objectives towards effective cyber security of its PSDI. Data and information security governance management practices and functions in the South African public sector context are very limited, and there is a dominant focus on IT and IT security. The findings also suggest that DISG policies, practices and systems have been found to be lacking in public sector management and governance functions. Data and information security governance is frequently practised in private sector management functions and not particularly in the public sector. In order for the government to improve its efforts towards the institutionalisation of DISG management practices, its public sector institutions must have clearly defined roles, responsibilities and functions. Government departments are often challenged by the bureaucratic systems and processes embedded in public sector administration functions. This unfortunately results in the duplication of functions and unstandardised public sector outputs and the mismanagement of scarce resources. Data and information security governance practices, principles and functions indicate that the protection of an organisation's critical data and information assets is an interrelated process that cannot be completed in isolation and requires a uniform approach and systematic application. Reinventing the roles, responsibilities and functions of public sector institutions in the protection of their PSDI assets through the institutionalisation of DISG management principles and practices could improve the processes and synergy of data governance (DG), information governance and information security governance (ISG). This will therefore improve the processes, systems and mechanisms related to the collection, classification, storage and transmission of PSDI between the government and its citizenry in creating and maintaining a reliable, factual and unbiased information society. Furthermore, it is recommended that further research be conducted on how DISG policies, practices and systems could be successfully implemented across all three spheres of government as this research article only focussed on the national sphere of government.

Acknowledgements

This article is partly based on a published master's dissertation, 'Data and Information Security Governance in the Departments of Energy, Science and Technology, and Environmental Affairs', by Lucia Masilela, under the supervision of Prof. Danielle Nel-Sanders, at the University of Johannesburg.

Competing interests

The authors have declared that no competing interests exist.

Authors' contributions

All authors contributed equally to this work.

Ethical consideration

This research did not collect or use any sensitive data. It is important to always be honest and give acknowledgment and credit for the work of authors who contributed to a study. According to the Protection of Personal Information (PoPI) Act (No. 4 of 2013), no personal details were used for this study without the acknowledgment and consent of the participants. Informed consent documents were used that uphold the principles of the University of Johannesburg's Ethics Research Charter to protect the university, the researcher, and the participants of the study, who may be who may be individuals or organisations as a whole.

Funding information

This research was funded by the National Research Foundation (NRF), under the Thuthuka Grant Scholarship.

Data availability statement

The data results and interpretations presented in this article are those that have been collected from a qualitative research study by the student. These data findings are therefore research results from a master's dissertation that was completed in 2019 at the University of Johannesburg.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any affiliated agency of the authors.

References

Aktinson, P., Coofey, A. & Delamont, S., 2001, 'A debate about our canon', *Qualitative Research* 1(1), 5–21. https://doi.org/10.1177/146879410100100101

Braun, V. & Clarke, V., 2006, 'Using thematic analysis in psychology', *Quantitative ResearchinPsychology*3(2),77–101.https://doi.org/10.1191/1478088706qp063oa

Department of Energy (DoE), 2015, *Strategic plan 2015–2020*, Government Printer, Pretoria.

Department of Environmental Affairs (DEA), 2016, *Overview of the department*, viewed 25 June 2019, from https://www.environment.gov.za/aboutus/department

Department of Environmental Affairs (DEA), 2018, *Strategic plan (2019/2023/24) and Annual performance plan 2019/20*, Government Printer, Pretoria.

Department of Science and Technology (DST), 2018, *Department of Science and Technology Vote No. 30: Annual report 2017/2018 financial year*, Department of Science and Technology, Pretoria.

De Vlieger, R., 2013, *McKinsey 7S Model*, viewed 22 June 2019, from https://www.calltheone.com/en/consultancy/7s-model

De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L., 2011, *Research at grass roots for the social sciences and human service professions*, Van Schaik, Pretoria.

Government Communications and Information Systems (GCIS), 2015, *South African year book 2014/5*, Government Printer, Pretoria.

Ravanfar, M.M., 2015, 'Analysing organisational structure based on 7S model of McKinsey', *Global Journal of Management and Business Research: Administration and Management* 15(10), 7–12. https://doi.org/10.6007/IJARBSS/v5-i5/1591

Republic of South Africa (RSA), 1996, *The white paper on science and technology of 1996,* Government Printer, Pretoria.

Republic of South Africa (RSA), 1998a, *The Minimum Information Security Standards (MISS)*, 2nd edn., Government Printers, Pretoria.

Republic of South Africa (RSA), 1998b, *The white paper on energy policy of 1998,* Government Printers, Pretoria.

Republic of South Africa (RSA), 1999, *The Public Finance Management Act (PFMA), No. 1 of 1999*, Government Printer, Pretoria.

Republic of South Africa (RSA), 2002, *The Regulation of Interception of Communication and Provision of Communication-related Information Act (RICA), No. 70 of 2002*, Government Printers, Pretoria.

Republic of South Africa (RSA), 2003, *The White Paper on Renewable Energy of 2003,* Government Printer, Pretoria.

Waterman, Jr. R., Peters, T. & Phillips, J.R., 1980, 'Structure is not organisation', *Business Horizons* 23(3), 14–26. https://doi.org/10.1016/0007-6813(80)90027-0