The State of e-Government Security in South Africa: Analysing the National Information Security Policy

Bukelwa Ngoqo(✉) and Kennedy Njenga

University of Johannesburg, Johannesburg, South Africa
bukelwa.ngoqo@gmail.com, knjenga@uj.ac.za

Abstract. As a result of the growing reliance by public sector organisations on technological resources for capturing and processing information, protection of information in the public sector has become an issue of national concern. While considering the South African national strategy for protecting this state asset ('information') this paper contrasts existing local, provincial or national e-Government information security policies against the adopted national guidelines. The paper postulates that with sound policies and guidelines in place 'interpretation and application' remain as two barriers that pose a threat to state information. The main question addressed in this paper is whether e-Government information security policies adequately address prescribed key security components. To achieve a comprehensive understanding of the pillars underpinning the protection of national information security in South Africa, the authors followed systematic procedures for reviewing and evaluating existing e-Government information security policies. The objective of this paper is to investigate whether existing government information security policies are aligned to national policy or guidelines. This paper will contribute empirical evidence which supports the notion observed by the South African Auditor General that (Auditor-General 2012) security weaknesses in government departments and state entities are attributed to the lack of formally designed and implemented information security policies and standards. The results of this preliminary investigation indicate that although information security policies exist in the majority of state entities, there is no consistency in the application of the 'security controls', as outlined in the national guidelines.

Keywords: National information security · Information security policy
e-Government · Information security legislation · Security controls

1 Introduction

E-Government has transformed the traditional views of 'service delivery' by government institutions. Mutula and Mostert [12] refer to an 'inextricably intertwined' relationship between e-Government and service delivery. This suggests that the role government plays in meeting the needs of its citizens cannot be separated from its application of e-Government. According to Crous [5] this role would encompass the implementation of laws and the actual provision of services and products by

V. Odumuyiwa et al. (Eds.): AFRICOMM 2017, LNICST 250, pp. 29–46, 2018.
https://doi.org/10.1007/978-3-319-98827-6_3

government. The topic of e-Government has been discussed by researchers since the mid-1990s, thus e-Government research is still maturing in terms of theory development and empirical research [22]. The definition of e-Government adopted for purposes of this study is the World Bank [21] defining e-Government as; "The use by government agencies of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions."

South Africa is recognised by Cloete [4] as one of the early adopters of e-Government with policy change recommendations made as early as 1998 by the Presidential Commission on the Transformation of the Public Service (PRC 1998, Sect. 6.9). While there are possible benefits of e-Government as highlighted in the World Bank definition quoted above, [14] caution that an inherent threat to information security persists and attacks will continue as long as technologies continue to develop. This threat is further accentuated for state entities where information is captured, processed, stored and retrieved electronically. This study adopts the definition of information security as the set of processes, procedures, personnel, and technology charged with protecting an organization's information assets [20]. The information security policy is prescribed by researchers as a formal document that details acceptable and unacceptable behaviour of users in relation to dealing with information assets in a secure manner [2].

Information security is recognised as being an important aspect of IT governance [2]; however, government entities still struggle to design and implement effective controls that are aimed at optimising such security. This challenge is echoed in a report by the Auditor-General [3], in which security weaknesses in government departments and state entities are attributed to the lack of formally designed and implemented information security policies and standards. Shava and Van Greunen [16] suggest that despite security policies being in place in most organisations, there are concerns relating to the lack of user awareness on the meaning and implications of such policy implementation. This stance is echoed in the reference to 'two barriers that pose a threat to state information' (interpretation and application) mentioned earlier in this paper. This paper suggests that in cases where information security policies are in place as prescribed by government and government entities still face information security challenges, investigation into the cause must go beyond user awareness and include an analysis into the contents of the information security policy. The problem addressed by this paper is that even in cases where the relevant policies exist, if they fail to address key security concerns then they cannot be used as a benchmark for assessing any measure of information security effectiveness (e.g. user awareness). National security and service delivery can be negatively affected in cases where the operational integrity of the state is compromised by a lack of effective IT controls [3].

To gain a better understanding of the current South African information security landscape, this paper initially examines existing literature relating to South African e-Government research, the national information security landscape, information security linked legislation and the prescribed national information security constructs. This is followed by a discussion of the research methodology and the study findings, and some concluding remarks.

2 e-Government Research

Cloete [4] further raises concern about how South Africa has gradually lagged behind in e-Government implementation despite its early start. While research efforts continue in the field of e-Government in South Africa, some areas of global e-Government interest still remained marginally explored in the South African case. Zhao *et al.* [22] mention six critical topics of e-Government research: e-Government technology; infrastructure and resources; socio-economic issues such as access issues and digital divide; policies and strategies; user behaviour and intentions; and cultural issues. Table 1 below identifies the themes in South African e-Government research and aligns them to the key topics of e-Government research as outlined by [22].

Table 1. South African e-Government research focus (1).

Topic	Title	Year	Author(s)
Technology	*Smart card initiative for South African e-governance - a study*	2006	Nkomo, Terzoli, Muyingi and Rao
	Semantic-driven e-government: A case study of normal representation of government domain ontology	2011	Dombeu and Huisman
	The use of focus groups to improve and e-Government website	2011	Pretorius and Calitz
	A study of some e-Government activities in South Africa	2012	Thakur and Singh
	Next generation citizen centric e-Services	2014	Sharma, Guttoo and Ogra
	Towards a "Smart Society" through connected and smart citizenry in South Africa: A review of the National Broadband strategy and policy	2016	Manda and Backhouse
Infrastructure & resources	*Case study: Assessing and evaluating the readiness of the ICT infrastructure to provide e-government services at a local government level in South Africa*	2012	Monyepao and Weeks
Socio-economic issues	*Challenges and opportunities for e-government in South Africa*	2010	Mutula and Mostert
	The e-Government evaluation challenge: A South African Batho Pele-aligned service quality approach	2011	Kaisara and Pather
	e-Government development in Sub-Saharan Africa (SSA): Relationships with macro level indices and possible implications	2016	Verkijika and De Wet

(*continued*)

Table 1. (*continued*)

Topic	Title	Year	Author(s)
Policies and strategies	*South African e-Government policy and practises: A framework to close the gap*	2003	Trusler
	Questioning the pace and pathway of e-government development in Africa: A case study South Africa's Cape Gateway project	2008	Maumbe, Owei and Alexander
	Comparison of Sub-Saharan Africa's e-government status with development and transitional nations	2008	Mutula
	Are e-Government investments delivering against expected payoffs? Evidence from the United Kingdom and South Africa	2010	Naidoo and Palk
	Measuring the public value of e-government: Methodology of a South African case study	2010	Friedland and Gross
	A conceptual ontology for e-government monitoring of development projects in Sub Saharan Africa	2010	Dombeu
	South Africa's e-development still a futuristic task	2011	Abrahams
	Innovation in monitoring and evaluation for e-development and transformational government	2012	Abrahams and Burke
	Strategic planning for transformational government: A South African perspective	2012	Mawela
	e-Government implementations in developing countries: Success and failure, two case studies	2012	Rajapakse, Van Der Vyver and Hommes
	e-Government lessons from South Africa 2001–2011: Institutions, state of progress and measurement	2012	Cloete
	An exploration of critical success factors for e-Governance Project Initiation: A preliminary framework	2015	Hatsu and Ngasaam
User behaviour and intentions	*Use of e-government services: the role of trust*	2015	Mpinganjira
Cultural issues	*Diffusing the Ubuntu philosophy into e-Government: A South African perspective*	2010	Twinomurinzi, Pahlamohlaka and Byrne
	Global survey on culture differences and context in using e-Government systems: A pilot study	2011	Herselman and Van Greunen

South African researchers investigated a wide variety of related topics aligned to the six key e-Government research areas. These research efforts have concentrated mainly in topics related to *Technology* as well as e-Governance *Policies and strategies*. The progression of South African e-Government research has gradually evolved with researchers progressively exploring the following research areas:

2003–2015: The initial focus of South African researchers was on Policies and strategies. This early e-Government research addressed pertinent questions such as: *Do we have the policies in place? Are we implementing e-Government quickly enough compared to other developing nations? Are we getting value from e-Government investments? How can we monitor and evaluate e-Government implementation? What are the critical success factors for e-Government investments?* While areas of focus have changed over time the topic of e-Government Policies and strategies continues to be a relevant one. This paper further adds to the Policy and strategies debate but drawing specific attention to the area of e-Government information security policies.

2006–2016: Applicable technologies were subsequently discussed by South African researchers. The focus of research was on the following technologies/technology related topics: *Smart cards, semantic-driven e-Government, e-Government websites, e-Services and Smart societies.*

2010–2016: South African is referred to as a 'rainbow nation' due to the number of diverse cultures that form part of the national social fabric. This is evidenced in the staggering number of official languages in the country which currently stands at eleven. The resultant socio-economic and cultural issues also filter through to the e-Government research sphere. Linked to the socio-economic issue e-Government researcher explored: *e-Government challenges/opportunities, Batho Pele-aligned e-services, and e-Government relationships with macro level indices*. Researchers focusing on cultural issues discussed principles such as: *Ubuntu philosophy in e-Government, Culture differences and context in using of e-Government systems.*

2012: The topic of infrastructure & resources appears in later e-Government researcher where the important question of '*Do we have the infrastructure to support e-Government services?* is examined.

2015: Initially the focus of e-Government research was on policies and technology, the focus eventually shifted to the e-Government user. The role of trust is discussed user behaviour and intentions *(The role of Trust).*

The least researched topics in the case of South African e-Government research are *Infrastructure & resources* and *User behaviour & intentions*. South African research in the field of e-Government can be deemed as sporadic two additional e-Government areas have been explored by South African researchers (*2010–2014*): *Security* and *m-Government* (see Table 2).

Table 2. South African e-Government research focus (2).

Topic	Title	Year	Author(s)
Security	*South African eGov: Secure e-services*	2010	Dlamini, Ngobeni and Mutanga
	Secure e-government services: Towards a framework for integrating it security services into e-government maturity models	2011	Karakola, Kowalski and Yongstrom
m-Government	*Mobile government for improved public service provision in South Africa*	2010	Nkosi and Mekuria
	Mobi4D: A next generation service delivery platform for mobile government services: An African perspective	2011	Ogunleye, Makitla, Botha, Tomay, Fogwill, Seetharan and Geldenhuys
	Exploring the success, failure and factors influencing m-Government implementation in developing countries	2014	Ogunleye and Van Belle

The literature shows that most research has been concentrated on e-Government Policy and strategy. This observation further accentuates the problem identified in this paper where information security is deemed as an inherent policy issue that has been overlooked in previous e-Government research. This paper links two of the topics mentioned above namely: Policies and strategy and Security. It also adds clarity to these two broad topics by specifically focusing on the information security as it relates to the information Security Policy. The next section outlines the background to the South African national information security landscape.

3 National Information Security

In South Africa, the Department of Public Service and Administration (DPSA) is responsible for the development and coordination of the government's overall e-Government strategy [17]. The Department of Communications [17] also mentions two complementary statutory bodies established to coordinate the implementation of e-Government projects, namely, the State Information Technology Agency (SITA), which is responsible for the acquisition, installation, implementation and maintenance of public sector IT assets, and the Government Information Technology Officers (GITO) council, which is responsible for consolidating and coordinating IT initiatives in government to facilitate service delivery.

Information security management is one of the IT governance processes [3] identified in the framework presented below (Fig. 1), which is endorsed by the DPSA and the GITO council.

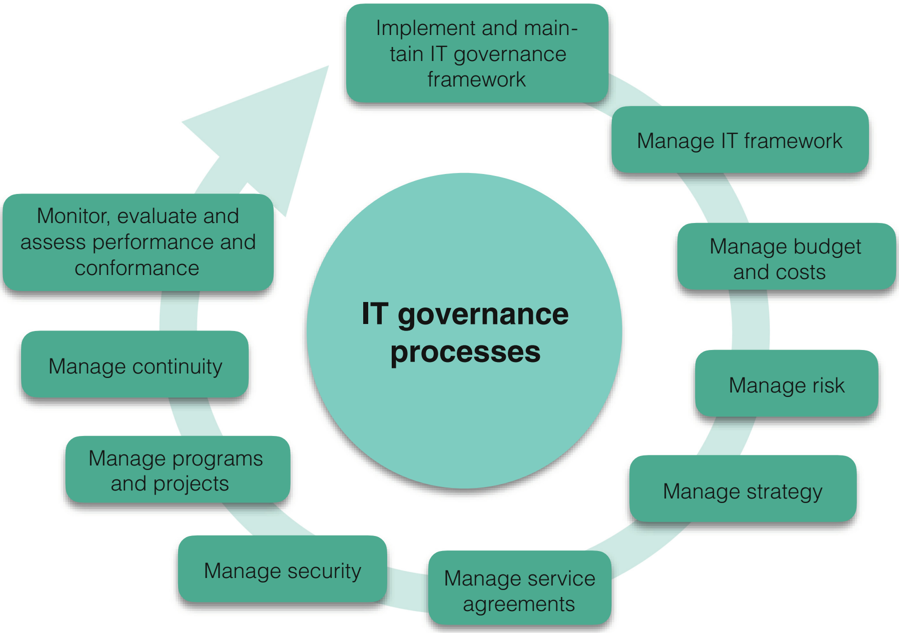
IT governance processes
Implement and maintain IT governance framework
Manage IT framework
Manage budget and costs
Manage risk
Manage strategy
Manage service agreements
Manage security
Manage programs and projects
Manage continuity
Monitor, evaluate and assess performance and conformance

Fig. 1. Information technology governance process [3]

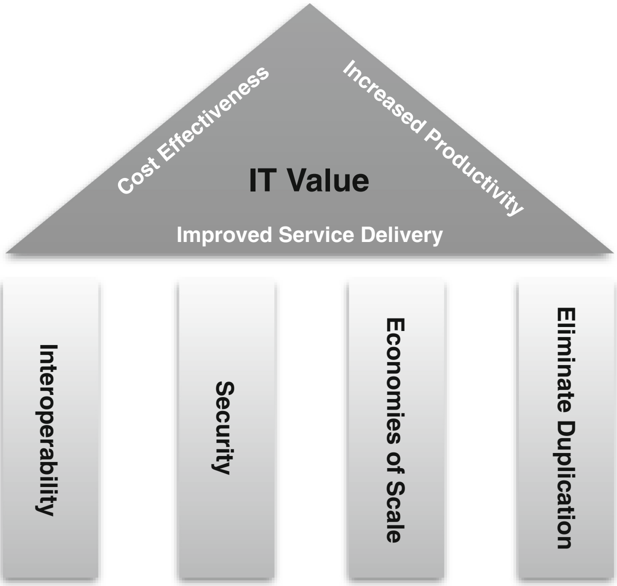

Fig. 2. e-Government Pillars (DPSA 2011)

Security is also identified as one of the four pillars (Fig. 2) of e-Government in South Africa cited by [17]. For the purposes of this study, information security refers to the measures adopted to prevent the unauthorised use, misuse, modification, or denial of knowledge, facts, data or capabilities [10]. Although policies, standards and procedures are terms that are commonly used in the information security domain, it cannot be assumed that the interpretation of these is common to all information security stakeholders (including end users, information security practitioners, management and external parties). Existing South African legislation that informs the construction of e-Government information security policies is presented in the following section.

4 Information Security Linked Legislation

South African legislation that influences the area of national information security is fragmented across multiple disciplines, including communication, cyber security, protection of information and the constitutional rights of citizens. Existing research in the area of cyber security has assisted in identifying areas where government has lagged behind in the development of security protocols and standards, as well as in implementing such protocols and standards [9]. Based on the areas of concern identified by [18], government has adopted a more proactive stance to information security with "adequate information security policies" being viewed as an important contributor to the security and wellbeing of government information resources. The DPSA [18] highlights eight pieces of South African legislation that are relevant to the information security policies of government entities (Table 3):

Table 3. South African information security linked legislation.

Legislation (Question addressed)	Purpose of legislation
The Public Service Amendment Act of 2007 *(Who is responsible for the policies?)*	Assigns responsibility for policies relating to information management and electronic government in the public service to the Minister of Public Service and Administration (s 3(1)(f)(g) of the Public Service Amendment Act, 2007). The Minister of Public Service and Administration is the custodian for e-Government in South Africa
The State Information Technology Agency (SITA) Amendment Act 38 of 2002 *(Who is responsible for securing national information assets?)*	Dictates that the responsibility of securing state information assets lies with the State Information Technology Agency (SITA). The objective of this Act "(a) is to provide information technology, information systems and related services in a maintained information systems security environment to departments and public bodies".

(*continued*)

Table 3. (*continued*)

Legislation (Question addressed)	Purpose of legislation
	The objective of the principal SITA Act 88 of 1998 was revised to in the SITA Amendment Act 38 of 2002 to firstly change the wording of the objective to make SITA relevant to all departments and public bodies, versus the initial proclamation which referred to '… participating departments and organs of state…'. The amendment (SITA Amendment Act, 2002) subsequently include a key sub-section (b) which states: "(b) to promote the efficiency of departments and public bodies through the use of information technology." This revision to the SITA Act is indicative of the evolving stages of e-Government implementation, hence confirming the importance of e-Government to National Government
The Minimum Information Security Standards (MISS) *(Preventative measures)*	Set out a range of measures to protect classified information, including the classification and reclassification of documents, handling of classified documents, access to classified information, storage of classified document and removal of classified documents from premises. The MISS also provides for the security vetting of personnel. The MISS sets out security measures to protect classified information, including physical security, access control, computer security and communication security (Protection of Information Bill 6, of 2010)
National Strategic Intelligence Act 39 of 1994 *(What happens if the threats are realised?)*	This Act describes the counterintelligence role of the National Intelligence Agency in measuring and undertaking activities to neutralise threats and protect classified information from hostile or foreign intelligence operations
National Archives of South Africa Act 43 of 1996 *(Records management & preservation)*	"Aims to provide for a National Archives, the proper management and care of the records of governmental bodies and the preservation and use of a national archival heritage." This Act covers details on topics such as the "classification of records", the "management of electronic records" and the "electronic reproduction of records"

(*continued*)

Table 3. (*continued*)

Legislation (Question addressed)	Purpose of legislation
Protection of Information Act 84 of 1982 *(Protection of public information)*	Provides for the protection from disclosure of certain information. Some of the offences/prohibitions mentioned in the Act include prohibited places and the obtaining or disclosure of certain information. The Protection of Information Act stipulates regulations, permissions and prohibitions on how public information can be obtained, used and when or how it can be disclosed
Electronics Communications and Transactions Act of 2002 *(Critical data)*	In this act the Minister of Communications is given the power to deem information to be "critical data" and discretion in guiding the way critical databases are managed. In the Act, critical data is defined as "data that are of critical importance to the national security of the Republic, and/or the economic and social well-being of its citizens"
Interception and Monitoring Bill 50 of 2001 *(The 'Big Brother' role of the state)*	With the South African government embracing "the use of information and communication technologies in the public service to improve its internal functioning and to render services to the public" (Public Service Amendment Act, 2007) e-Government as a necessary part of service delivery. Securing information that is transmitted through telecommunications services should also be a national information security concern. The Interception and Monitoring Bill 50 of 2001 regulates the following areas of certain communication (postal or telecommunications) or matters connected therewith: *"...the interception and monitoring of certain communications"* *"...to provide for the interception of postal articles and communications and for the monitoring of communications in the case of a serious offence or if the security or other compelling national interests of the Republic are threatened"* *"to prohibit the provision of certain telecommunication services which do not have the capacity to be monitored"* *"to regulate authorised telecommunications monitoring"*

State entities' information security policies are crafted based on the legislation mentioned above as well as guidelines that can be obtained from national government structures. These guidelines are based on existing information security frameworks. For example, the DPSA used the ISO 17799 framework as a basis for establishing its information security policies. The next section introduces the ISO 17799 constructs.

5 National Information Security Policy Constructs

Da Veiga [6] relies on the ISO/IEC/ 27001 (2013) description of the role of the information security policy as a document which outlines the organisation's approach to information security that provides a framework for setting control objectives and controls. The South African Department of Public Service and Administration [18] adopts the ISO 17799 framework in conceptualising security management controls for public entities. In examining the contents of various e-Government information security policies this paper uses the DPSA's (ISO 17799 adapted) security controls (securing hardware, peripherals and equipment; controlling access to information; processing information documents; purchasing and maintaining commercial software; developing and maintaining in-house software; combating cybercrime; complying with legal and policy requirements, planning for business continuity; addressing personnel issues relating to security; controlling e-transaction information security; delivering training and staff awareness; dealing with premises related considerations; detecting and responding to information security incidents; and classifying information and data) to contextualise key information security policy components.

Having clearly defined the fifteen key constructs of an e-Government information security policy, as recommended by the DPSA guidelines, this paper suggests that possible weaknesses in e-Governance information security can be attributed to poorly constructed (designed) information security policies that do not adequately address all the necessary information security controls. In the next section, the methodology used for collecting the data during the first phase of this study is described.

6 Methodology

This study employed content analysis as an approach to study the web presence of Information Security Policies of various South African state entities. Qualitative content analysis was used to analyse the contents of existing information security policies for 56 government department and municipalities sourced on the web. Content analysis describes a family of analytic approaches ranging from impressionistic, intuitive, interpretive analyses to systematic, strict textual analyses [15]. In this research, the qualitative content analysis is applied through the interpretation (subjective) of the content of text data through and subsequently the systematic classification process of coding and identifying themes or patterns [8]. Based on this approach to gathering data this study systematically analysed published e-Government information security policies.

There are currently 278 metropolitan, district and local municipalities in South Africa. The sample taken during this preliminary data collection stage of the study represented 20% of the total population. The secondary data collected during this stage by collecting South African (e-Government) Information Security Policies through conducting online searches. The policies were accessed by using conventional search engines, which provided links to the policies, and then the researchers traced them to the respective government department or municipality website. Considering that there are various types of government entity, including parastatals and government agencies, the first criterion for choosing a policy as a potential candidate was that it should belong to a national/provincial government department or a metropolitan/district/local municipality. A second criterion was that candidate policies should specifically address information security concerns. After refining our search results according to these criteria, we ended up with 56 information security policies for our content analysis.

While the literature phase of this paper provided insight into the South African e-Government landscape, second phase to addresses the following sub-research questions:

- Is there an existing information security policy?
- Do these policies contain information exclusively related to information security?
- To what extent does the policy address the key security controls stipulated in the DPSA guidelines?

In answering these sub-research questions the main question in this paper (*Do e-Government information security policies adequately address prescribed key security components?*) will be addressed. The findings presented in the next section include an objective analysis that compares the DPSA set “standard” against the actual contents of e-Government information security policies of various South African state entities.

7 Findings

Analysis of Textual Data: Existing Policies Within Municipalities

Is There an Existing Information Security Policy?

Based on the data collected online at least 56 South African government entities had policies that addressed information security concerns. The data collected thus disputes the Auditor General’s (2015) assumption of non-existent information security policies and standards within state entities as this was found not to be applicable to the departments or state entities in this study sample.

The findings above (Fig. 3) indicate that in the case of the sample taken in this study, only five percent of the entities considered did not have information security policies in place. The ‘No policy’ finding was applied in cases where on closer analysis the policies found online were deemed not to be information security policies. However, the majority of the sample had policies in place. While the information security linked policies are found for this study population the next section interrogates the contents ‘design’ of these policies. Discounting the first part of the Auditor General’s concerns, the ensuing question becomes: *“Do these information security policies provide clear guidance on critical information security controls?”*

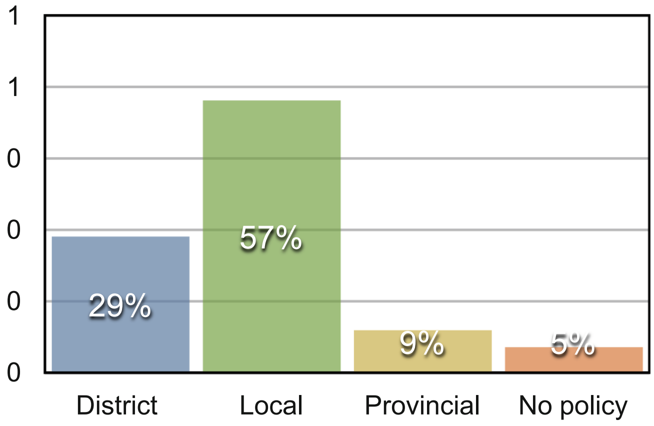

Fig. 3. Is there an existing information security policy?

Do Policies Contain Information Exclusively Related to Information Security?
The findings (see Table 4) further show that just over fifty percent of the policies analysed contained information that was exclusively related to information security. Various names were used to describe these policies, and this is also an indication that ambiguity may exist within state entities regarding the intended use of these information security policies. The use of different names hints at the ambiguity that possibly exists around the interpretation and/or implementation of these policies. Further insights on how the stakeholders perceive the information security policy is beyond the scope of this paper. The DPSA [18] proposes a clear structure for what should be included in an e-Government information security policy. The structure of the 56 policies examined was compared to the 15 key controls (see Fig. 4) provided in the DPSA guidelines. The findings discussed below answer the following question: *"In cases where the information security policy is in place, to what extent does it address the key security controls stipulated in the DPSA guidelines?"*

Table 4. Does the policy contain information exclusively related to information security?

Total number	Name of document
Yes (28)	Information and Communication Technology Security Policy, IT Data and System Security Policy, Information Security Policy, Information Security Management Policy, Security Policy, Information Security Policy, Policy on ICT Security, Information Security Controls Policy, Information Technology and Security Policy, User Security Policy, Information Technology Security Management Policy, Information Systems Security Policy, IT and Information Management Security Policy
No (25)	Security Policy & Standard Operating Procedures, Security Policy, ICT & Information Security Policy, Information and Communication Technology Security Policy, Information Technology Policy, ICT Acceptable Use Policy

8 Alignment with DPSA Guidelines

An analysis (see Fig. 4) of e-Government information security policies shows that some security controls are a priority, with more than sixty percent of state entities making reference to them in their policies. These priority security controls seem to me to be (1) security hardware, (2) controlling access, (3) combating cybercrime, (4) premise-related considerations and (5) responding to information security incidents. However, the majority of the security controls were only partially addressed by most state entities, with scores for inclusion ranging between twenty and fifty percent for the following security controls in the policy: peripherals and equipment, processing information documents, purchasing software, developing in-house software, business continuity, personnel issues relating to security, training and awareness and classification of information and data. The most neglected of the key controls (as per the DPSA guidelines) are (1) complying with legal and policy requirements and (2) e-transaction security, with both scoring below ten percent.

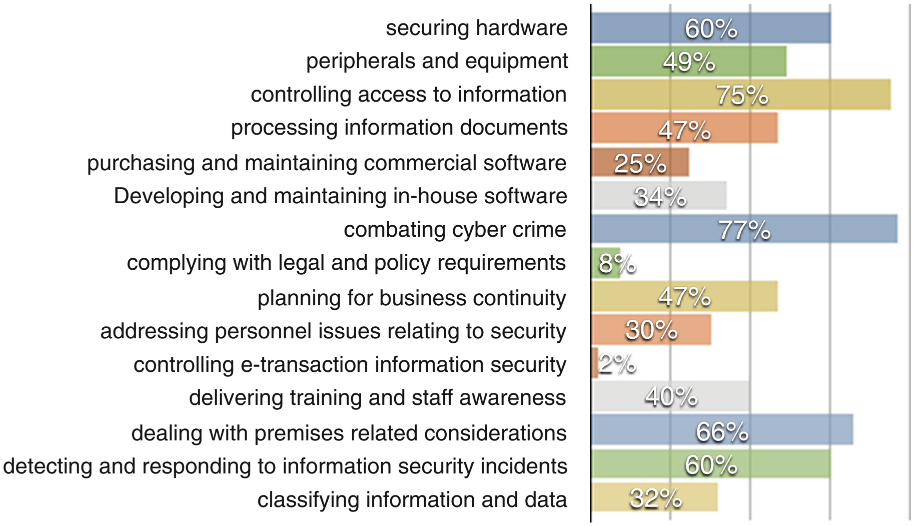

Fig. 4. Alignment with DPSA guidelines

9 Discussion of Findings

Making reference to the initial question raised in this paper 'Do e-Government information security policies adequately address prescribed key security components?' The findings show that in the case of South African e-Government information security policies department and/or entities observed in this study do have information security related policies in place. However, there is misalignment between the prescribed DPSA guidelines (key security controls) and the controls actually put in place through these policies. Of particular concern are the two controls (*controlling e-transaction information security* and *complying with legal and policy requirements*) which both we mentioned in the information security policy by less than ten percent of the departments or entities considered in this study. An additional observation based on these findings is that the people who draft these policies (IT Department representatives) put more of an emphasis on the 'Technology related/Infrastructure' aspects of information security with controls like: *include security hardware, controlling access, combating cyber-crime, premise-related considerations* and *reporting to information security incidents* scoring sixty percent and above for inclusion in the information security policies of the study population. While the majority of stakeholder related security controls were only partially addressed: *personnel issues relating to security, training & awareness, classification of information & data* and *processing of information documents*.

This paper suggests the use of the overall classification scale, 'low priority', 'medium priority' and 'critical', as a tool for analysing the findings. The ratings used in this scale are based on the coverage (i.e. number of key security controls) of 15 key information security controls in each department or state entity policy from the 56 analysed in this study. This scale (Table 5 below) has been used in this study to give an indication of areas that have been insufficiently covered by the information security policies of a group of state entities.

Table 5. Analysis scale

	Scale	*Score (information security controls)*
Low priority	50–100%	8–15
Medium priority	20–49%	4–7
Critical	0–20%	1–3

Applying this scale to the data (Table 6 below), the following inferences can be drawn. Based on the number of security controls that were addressed in the information security policies of the state entities in the sample, only seventeen percent fits the 'critical' category in that less than twenty percent of the information security controls are mentioned in their policies. The 'medium priority' category includes those state entities that have scored above twenty percent but less than fifty percent in their coverage of the key security controls in their information security policies. Forty per cent of the sample fell into the medium priority category.

Table 6. Application of findings to analysis scale

	Critical	Medium priority	Low priority
District municipality	2	9	13
Local municipality	7	11	5
Provincial department		1	4
Metropolitan municipality			1

Forty-three per cent of the sampled state entities scored above fifty percent, meeting the minimum criteria for the ‘low priority’ category. The evidence confirms that most (57%) of the state entities sampled have information security policies that fail to address even half of the security controls delineated in the DPSA guidelines.

This analysis provides a good summary of key information security control ‘coverage’ in existing e-Government information security policies. This paper proposes that in the e-Government environment, an information security policy that does not adequately address key security controls is as effective as no policy at all. These findings give a good indication of inherent (within state entities) security policy weaknesses that could potentially result in the weaknesses identified by the Auditor-General.

10 Implications for Practice

South African researchers have explored the topic of information security policy from various angles: *policy development* [13, 19] *conceptual threat assessment framework development* [11] and *legal implications* [7]. Limited research exists in South Africa that explores the links between the development of policy, and its the application in the e-Government environment.

This paper presented an environmental overview on the way the information security policy should be structured, as well as the underlying legislation that influences its development. The paper concludes by highlighting the gaps that exists in the information security policies of various government entities. The contribution made by this paper should stimulate further research on the application of information security policies in the e-Government environment.

11 Conclusion

The information security policy is an instrumental document that guides the process of effective information security management in the e-Government environment. While guidelines have been provided by the DPSA, as the state entity responsible for the development and coordination of government’s overall e-Government strategy, including e-Government information security, responsibility for selecting the controls that are most suitable for consideration in their respective environments rests with the state entities themselves. This paper presented an analysis of existing South African e-Government information security policies. The analysis highlighted the areas in which key security controls had been overlooked in the majority of the information security policies of state entities examined. This paper argues that these weaknesses are not necessarily limited to the lack of formally designed and implemented information security policies, but that the contents of these information security policies should scrutinised to ensure that key security controls have been addressed.

The progress that has been made in this research thus far and the findings of this particular study are encouraging and the intention is to proceed with a follow-up study aimed at measuring e-Government information security policy awareness focusing on the areas referred to in this study as the ‘two barriers that pose a threat to state information' (interpretation and application). Specific goals of the follow-up study are to (1) conduct an in-depth study into the factors that influence information security policy awareness within the e-Government context; and (2) develop e-Government information security behaviour profiles based on empirical data collected. The broader objectives of the study outside the scope of this paper include measuring the information security policy awareness levels of government employees and identifying possible vulnerabilities based on user information security behaviour profiles.

References

1. Ajzen, I.: The theory of planned behavior. Organ. Behav. Hum. Decis. Process. **50**, 179–211 (1991)
2. Alotaibi, M., Furnell, S., Clarke, N.: Information security policies: a review of challenges and influencing factors. In: Proceedings of the 11th International Conference for Internet Technology and Secured Transactions (ICITS-2016), 5–7 December 2016, Barcelona, Spain (2016). ISBN 978-1-908320-73-5
3. Auditor-General South Africa: The Drivers of Internal Control: Information Technology Management as a Driver of Audit Outcomes. Consolidated General report on the 2011–12 national and provincial audit outcomes (2012). https://www.agsa.co.za/Portals/0/MFMA2011-12Extracts/MFMA_2011-12_consolidated_reports/AGSA_MFMA_CONSOLIDATED_REPORT_2011_12.pdf. Accessed 12 July 2016
4. Cloete, F.: E-government lessons from South Africa 2001–2011: institutions, state of progress and measurement. Afr. J. Inf. Commun. **12**, 128–142 (2012)
5. Crous, M.: Service delivery in the South African public service: implementation of the Batho Pele principles by statistics South Africa. J. Publ. Adm. **39**(4.1) (2004)
6. Da Veiga, A.: Comparing the information security culture of employees who had read the information security policy and those who had not Illustrated through an empirical study. Inf. Comput. Secur. **24**(2), 139–151 (2016)
7. Etsebeth, V.: Information security policies - the legal risk of uninformed personnel. In: Proceedings of the ISSA 2006 from Insight to Foresight Conference, 5–7 July 2006, Sandton, South Africa (2006). ISBN 1-86854-636-5
8. Hsieh, H., Shannon, S.E.: Three approaches to qualitative content analysis. Qual. Health Res. **15**(9), 1277–1288 (2005)
9. Kortjan, N., Von Solms, R.: A conceptual framework for cyber-security awareness and education in SA. South Afr. Comput. J. (SACJ) **52**, 29–41 (2014)
10. Maiwald, E.: Fundamentals of Network Security. McGraw-Hill Education, New York (2004)
11. Mbowe, J.E., Zlotnikova, I., Msanjila, S.S., Oreku, G.S.: A conceptual framework for threat assessment based on organization's information security policy. J. Inf. Secur. **5**, 166–177 (2014)
12. Mutula, S.M., Mostert, J.: Challenges and opportunities of E-Government in South Africa. Electron. Libr. **28**(1), 38–53 (2010)
13. Ngobeni, S.J., Grobler, M.M.: Information security policies for governmental organisations: the minimum criteria. In: Proceedings of ISSA, 6–8 July 2009, Johannesburg, South Africa, pp. 455–466 (2009)
14. Njotini, M.N.: Protecting critical databases: towards risk based assessment of Critical Information Infrastructures (CIIS) in South Africa. Potchefstroomse Elektroniese Regsblad (PER) **16**(1), 451–481 (2013)

15. Rosengren, K.E.: Advances in Content Analysis. Sage Publications, Beverly Hills (1981)
16. Shava, F.B., Van Greunen, D.: Designing user security metrics for security awareness at higher and tertiary institutions. In: Proceedings of the 8th International Development Informatics Association Conference, 3–4 November 2014, Port Elizabeth, South Africa, pp. 280–296 (2014)
17. South Africa. Department of Communications: National Integrated ICT Policy. Government Gazette, No. 37261, 24 January 2014
18. South Africa. Department of Public Service and Administration: Draft position Paper on Information Security. Version 0.3 (2015)
19. Tuyikeze, T., Pottas, D.: An information security policy development life cycle. In: Proceedings of the South African Information Security Multi-Conference (SAISMC), Port Elizabeth, South Africa, pp. 165–176, 17–18 May 2010. ISBN 978-1-84102-256-7
20. Whitman, M.E., Mattord, H.J.: Principles of Information Security. Course Technology, Boston (2003)
21. World Bank: New-Economy Sector Study: Electronic Government and Governance: Lessons for Argentina (2002). http://documents.worldbank.org/curated/en/527061468769894044/pdf/266390WP0E1Gov1gentina1Final1Report.pdf. Accessed 17 Feb 2017
22. Zhao, F., Scavarda, A.J., Waxin, M.: Key issues and challenges in e-Government development: an integrative case study of the number one eCity in the Arab world. Inf. Technol. People **25**(4), 395–422 (2012)