

# **Bridging the Personal Information Governance Gap: A Case Study of a South African University**

by  
Jerall Toi

*Thesis presented in fulfilment of the requirements for the degree of  
Master of Socio-Informatics in the Faculty of Arts and Social Science at  
Stellenbosch University*



Supervisor: Professor Ian Cloete

April 2019

## **Declaration**

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

April 2019

Copyright © 2019 Stellenbosch University

All rights reserved

## **Acknowledgements**

Throughout my career, I have had the good fortune to have access to several mentors—individuals that saw something worth developing in me. Within the context of my research, one, in particular stands out. I would like to acknowledge the guidance and support given by Professor Ian Cloete, not only as my supervisor, but also as a valued mentor. Professor, thank you for giving me this opportunity.

I would also like to thank Cassey, for her love and support, for introducing me to the world of qualitative research, for the sound boarding sessions, and unwavering belief that I could do this. And, look, I did (said as our 4-year old would say it). Cassey, thank you.

## Abstract

Information is arguably the most valuable asset for a university. Yet, historically, South African higher education institutions did not have to formally and explicitly consider and report upon their Information Governance requirements. The relatively recent—for a university, at least—promulgation of the *Protection of Personal Information Act* (4 of 2013) and the *2014 Regulations for Reporting by Public Higher Education Institutions* now forces these institutions to relook at their Information Governance and Management policies and practices. However, these pieces of legislation, and their international counterparts, do not delve into the how of compliance, leaving institutions facing a gap between their current positions and their desired, legislatively compliant positions.

To address this gap, in this study, I discuss the international and local history of and unpack the more recent legislative requirements for Information Governance and privacy to establish the framework for further analysis. The discussion is furthered with a report on a case study investigation into the Information Governance-related initiatives at one South African public higher education institution. With the case study serving as foundation, I conclude by positioning a principles-based approach to privacy. These principles may enable an institution's governing structures to better provide the direction necessary to not only address Information Governance and privacy-related compliance requirements, but also provide scope to consider the risks and opportunities involved and, ultimately, derive value from their Information.

## Opsomming

Inligting is waarskynlik die waardevolste bate vir 'n universiteit. Dit was egter nooit histories 'n vereiste vir Suid-Afrikaanse hoërondewysinstellings om formeel en presies oor Inligtingsoorsigbestuursvereistes te rapporteer nie. Die relatief onlangse promulgasie van die Wet op die Beskerming van Persoonlike Inligting (4 van 2013) en die Regulasies vir Verslagdoening deur Openbare Hoërondewysinstellings wat in 2014 bekend gemaak is, maak dit vir hoërondewysinstellings verpligtend om hul Inligtingsoorsigbestuursbeleide en –praktyke te hersien. Hierdie wette, asook hul internasionale ekwivalente, verduidelik egter nie hoe om aan die vereistes te voldoen nie. Dit laat instellings dus met 'n gaping tussen hul huidige posisies en die wetlike voldoening waarna hulle strew.

Om hierdie gaping aan te spreek, bespreek ek in hierdie studie die internasionale en plaaslike geskiedenis van die onlangse wetgewende vereistes vir Inligtingsoorsigbestuur en privaatheid om sodoende die raamwerk vir 'n verdere analise te vestig. Die bespreking word verder gevoer deur die voorlegging van 'n verslag rakende 'n gevallestudie-ondersoek na verwante Inligtingsoorsigbestuur-inisiatiewe by een van die openbare hoërondewysinstellings in Suid-Afrika. Met die gevallestudie-ondersoek as basis, sluit ek af deur die posisionering van 'n beginselbenadering tot privaatheid. Hierdie beginsels kan die oorsigstrukture van die instellings in staat stel om die nodige rigting te verskaf om, nie net Inligtingsoorsigbestuur- en privaatheidverwante nakomingsvereistes aan te spreek nie, maar ook om die risiko's en geleenthede wat daarmee gepaard gaan te oorweeg en uiteindelik waarde uit hul Inligting te verkry.

## Table of contents

Declaration .....	i
Acknowledgements .....	ii
Abstract .....	iii
Table of contents .....	v
List of figures .....	viii
List of tables .....	ix
<b>Chapter One: Introduction .....</b>	<b>1</b>
Background and motivation for the study .....	1
Problem statement .....	2
Purpose of study .....	3
Research questions .....	3
Research design .....	5
Strengths and limitations of research design .....	7
Unit of analysis .....	8
Role of the researcher .....	9
Significance of research .....	12
Ethical considerations .....	12
Conclusion .....	12
<b>Chapter Two: Defining Information .....</b>	<b>14</b>
The trouble with definitions .....	14
Writing conventions .....	15
Defining Information .....	17
Our Non-Definition for Information (Expanded Writing Conventions) .....	21
Conclusion .....	21
<b>Chapter Three: History of Information Governance .....</b>	<b>23</b>

The origin of Information Management.....	23
The early days of Information Governance: United Kingdom .....	24
The early days of Information Governance: the United States .....	25
The early days of Information Governance: South African Higher Education .....	26
IT Governance recognises that IT Governance is not enough .....	30
Present day IT Governance .....	33
Present day Information Governance.....	37
Conclusion: Technology and Information Governance .....	39
Chapter Four: Theoretical Framework.....	41
King IV .....	41
The <IR> Framework .....	42
COBIT 5.....	44
The Three Lines of Defence.....	46
Institutional values .....	49
Institutional understanding of governance and management.....	51
Conclusion .....	52
Chapter Five: Privacy.....	54
What does the legislation say?.....	55
Personal Information Life Cycle.....	58
Life Cycle in Practice.....	59
Institutional Research and Academic & Learning Analytics.....	61
Funder access to student Information .....	67
Conclusion .....	72
Chapter Six: Recommendations.....	74
The privacy policy—a recommendation.....	77
The privacy policy—principles.....	77

The privacy policy—mapping principles.....	82
The privacy policy—Privacy Impact Assessments.....	82
The privacy policy—potential weaknesses.....	84
Further research opportunities .....	85
References.....	90
Appendices.....	97
Appendix A: King IV recommended practices for Technology and Information Governance.....	97
Appendix B: COBIT 5 illustrative set of enablers for privacy compliance.....	99
Appendix C: Mandatory institutional governance structures .....	102

## List of figures

Figure 1 The DIKW Pyramid.....	17
Figure 2 Governance and Management Spectrum.....	52
Figure 3 COBIT 5 Information Life Cycle .....	59

## List of tables

Table 1 COBIT 5 Governance and Management Interactions.....	37
Table 2 Personal Information Life Cycle.....	58
Table 3 POPIA Conditions to Policy Principles Mapping.....	82
Table 4 Privacy Impact Assessment to Policy Principles Mapping.....	83

# Chapter One: Introduction

## Background and motivation for the study

Information is arguably the most valuable asset for a university. Adapting Ragan's (2013:1) view for organisations in general: a university may find value within its teaching and learning materials, its research outputs, its intellectual properties and patents, or even within its 'customer' databases—prospective students, secondary schools, current students, alumni, donors, suppliers, and partners. Information suffuses the university and remains as one of the university's primary products through its teaching, research, and operational activities. As such, many, if not all, universities have implemented and are currently using a host of Information Management strategies to maximise Information<sup>1</sup> value, while minimising Information-related risks. However, as Sloan (2014:1) argues, within an “increasingly convoluted environment... the inadequacy of traditional strategies for addressing Information compliance, risk, and value is becoming clear, and so too is the need for a better, more holistic approach to governing the organisation's Information.”

Within the South African public higher education sector, we have seen the promulgation of several pieces of legislation which further complicates the environment, including the *Protection of Personal Information Act* (4 of 2013) (“POPIA”) and the 2014 *Regulations for Reporting by Public Higher Education Institutions* (“the Reporting Regulations”). POPIA, for example, aims to give effect to the South African constitutional right to privacy and align the country's stance on privacy with global counterparts (including the European Union's *General Data Protection Regulation* (“GDPR”))<sup>2</sup>. Within the South African public higher education sector, this may affect how universities handle the Information of local and international prospective students, currently enrolled students, alumni, research participants, staff, third parties, and suppliers. The Reporting Regulations, on the other hand, demand that South African universities adopt an Integrated Reporting approach as formally introduced to corporate South Africa through the *King Report of Governance for South Africa 2009* (“King III”) and expanded upon in

---

<sup>1</sup> I purposively capitalised Information here. In Chapter 2, I unpack my arguments for and explain my writing conventions in more detail.

<sup>2</sup> POPIA further balances “the right to privacy against other rights, [such as the right to] access to Information”; regulates “the way in which Personal Information must be processed”; provides “persons with right and remedies if POPIA is contravened”; and establishes “an Information Regulator to ensure that the rights protected by POPIA are respected and those rights are promoted and enforced” (de Stadler and Esselaar, 2015:1).

the *King IV Report on Corporate Governance for South Africa 2016* (“King IV”). These, and other requirements, are forcing South African universities to reconsider how they handle Information. Failure to do so, at least from a POPIA legislative compliance stance, may incur administrative fines of up to R10 million or imprisonment for up to 10 years (Republic of South Africa, 2013:100).

Against this background, this study aims to explore the concept of Information Governance within the context of the South African higher education sector. Moreover, it aims to understand the gap between, for example, a higher education institution’s POPIA compliance assessment report and the institution’s desired state with regards to compliance with POPIA. And from that understanding, recommend a starting point towards bridging that gap. Yet, compliance for compliance’s sake is of questionable value. Thus, this study also places a strong focus on addressing risks, seizing opportunities, and ultimately deriving value from Information. This opening chapter presents an overview of the research conducted during this study.

## **Problem statement**

South African public higher education institutions require a co-ordinated, multi-disciplinary, and integrated approach to address Information-related legislative compliance, while simultaneously managing Information-related risks and optimising the value of Information.

I synthesised the problem statement from the various definitions and arguments for Information Governance identified during this study’s literature review (see Chapter 2). As shall be discussed in more detail throughout this thesis, the need and legislative basis for Information Governance (as a subset of Corporate Governance) emerged in the West, in response to tightened legislation which in turn was promulgated in response to high profile Information Management failures (Kahn and Blair, 2004; Ragan, 2013; Smallwood, 2014). As Sloan (2012:2) summarises, Information Governance consists of three core elements, which were common to the definitions reviewed during this study: compliance, risk, and value. Furthering his argument, Sloan (2012:3) proposes that the “salient feature of the Information Governance approach is that it compels organisations to take a broad, inclusive view of Information issues and to act accordingly; [it] bridges across entrenched silos in the organisation’s various departments and functions... [causing the organisation] to reconcile various Information-focused disciplines, such as Records and Information Management, privacy and data security, intellectual property, and litigation preservation.”

Though many of the Information Governance-related disciplines and sub-disciplines (such as those referenced above by Sloan) are mature and well-defined in and of themselves, the concept of Information

Governance is relatively new, with various definitions in existence. Organisations, as Haggmann (2013:230) argues, “seem to develop their own understanding of Information Governance, according to their internal needs, priorities, ethics, and politics.” With this in mind, we can define the purpose of this study and subsequent research questions.

## **Purpose of study**

The purpose of this study is three-fold:

1. Firstly, it seeks to understand the concept of Information Governance as it pertains to the South African public higher education sector’s context. This includes a review and analysis of South African-specific legislation, codes, and standards and their international equivalents (such as POPIA and the GDPR).
2. Secondly, it seeks to position privacy, or rather Personal Information Governance and Personal Information Management, as an Information Governance-related discipline or sub-discipline; and
3. Finally, recommend a starting point from which a higher education institution may begin tackling privacy-related legislative compliance and Personal Information-related risks while still leaving scope to derive additional value from Personal Information.

## **Research questions**

1. *What are the essential components, of an Information Governance programme, required to adequately enable a privacy legislative compliance initiative?*

Nguyen, Sargent, and Stockdale (2014), in their efforts to develop unified Information Governance and Information Management frameworks, first distinguish between the two concepts. Thereafter, they seek to identify the components universally necessary for all Information Governance and Information Management programmes. They argue that Information Governance components cover, at a broad level, People, Policies, and Technology; Information Management components cover People, Processes & Practices, and Technology. Linked to these components, measurement factors allow organisations to assess the success or maturity of their Information Governance programmes. These include, but are not limited to transparency, accountability, Information quality, security, privacy, and compliance (Nguyen *et al.*, 2014).

Though Nguyen *et al.* (2014) provide a selection of model components and measurement factors, several South African- and sector-specific requirements, including both King III and King IV, caution against the blind, “mindless” implementation of a governance checklist (Institute of Directors in Southern Africa,

2009:7; Institute of Directors in Southern Africa, 2016b:36). Further, the unique-to-the-sector legislative requirements and the positioning of education (and thereby higher education) in South Africa's National Development Plan should be mindfully considered during the implementation, monitoring, and improvement of any governance programme within the South African public higher education sector. Thus, through answering this research question, this study aims to identify those potentially universal, South African-specific, and sector-specific components and measurement factors that could or should form the basis of an Information Governance framework that could adequately enable (at least, but preferably more than) compliance with privacy legislation within a South African public higher education institution.

*2. What is the difference between Information Governance and Information Management (as it pertains to the South African public higher education sector)?*

Nguyen *et al.* (2014) identify areas of conflict in “determining consistent and distinct meanings of Information Governance and Information Management.” Wang (2010, cited in Nguyen *et al.*, 2014), for example, uses Information Governance as a synonym for Information Management. Conflict and misunderstanding in the relationship between these two interlinked concepts may, ultimately, lead to Information Governance and Management failures. For example, through this confusion, governing body responsibilities and accountabilities may be pushed down to management structures which are improperly positioned within the organisation to fully address these requirements. Logan (2010), for example, emphasises the importance of accountability in successful Information Governance programmes (and how the lack of accountability may be the root of all Information related problems and thus ultimately Information Management failures), stating that “unless we make Information Governance someone's job, [it's] not going to happen.”

*3. Do Information Governance accountabilities and responsibilities adequately address the statutory institutional governance structures required by the Higher Education Act?*

Each South African public higher education institution, under the Higher Education Act (101 of 1997), must establish and/or appoint a Council, Senate, Principal, Vice-Principal, Student's Representative Council, an Institutional Forum, and “such other structures and offices as may be determined by the institutional statute” (Republic of South Africa, 1997:22), such as committees of the Council formed under sections 27 and 68 of the Act. The study therefore seeks to determine if the default statutory governance structures could adequately address an institution's Information Governance, and thereby privacy requirements (given the skills, knowledge, and capacity available to those structures) or if the

institution would be better served by delegating Information Governance functions to, for example, a Council subcommittee or even through the establishment of an independent function such as the Data Protection Officer role as recommended under the GDPR.

## Research design

Consider, for example: an institution finds the means to lawfully trade in Personal Information, but, though it would be legal, it may be unpalatable to the people within the institution and contrary to the institutional culture and stance on privacy. Thus, I selected a qualitative design methodology, based within the interpretivist paradigm, to collect and interpret the data necessary to answer the research questions posed in this study. Qualitative methods, as argued by Maylor and Blackmon (2005:220), are “important because research in business and management [deal] not only with organisations but also with the people in them... [people] can ascribe meanings, thoughts, and feelings to the situation in which they find themselves. Organisations are both social systems and the setting for social behaviour.” Further, as will be discussed in detail later in this chapter, the interpretivist tradition in accepting the impossibility of removing the subjective, enables me to own up to my subjectivity, given my position within a higher education institution and involvement with those public bodies that directly and indirectly influence the sector’s Information Governance-related legislative requirements.

I followed a two-fold approach. Firstly, I conducted a review of available literature, including a review of:

- both the academic and professional literature which explore the concepts of Corporate Governance, Information Governance, Compliance Governance, Information Technology (“IT”) Governance, and Information Management;
- South African legislation that establishes the regulatory requirements for Information Governance (or related sub-disciplines, including those that deal with privacy) within the South African public higher education sector; and
- South African and international codes and standards of Corporate Governance, Information Governance, Compliance Governance, IT Governance, and Information Management as referenced within the reviewed legislation, academic literature, and professional literature.

Secondly, employing a grounded case study design, I conducted a single case study within a South African public higher education institution which includes a faculty of health sciences (hereafter referred to as “University X” or “primary case”). Case study research is “well suited to inquiries into processes

and relationships and to broad research questions. Case study researchers recognise the complexity and embeddedness of social truths and the difficulty of capturing these through controlled experiments or statistical analysis. This research approach offers the opportunity to investigate issues where they occur and to produce descriptive and analytical accounts that invite reader judgement about their plausibility” (Cousin, 2009:131). Grounded case study research then allows researchers to “capture evolving insights and determine [their] evolving research design... where data collection and data analysis overlap. Here, grounded refers to a weaving back and forth between theory and data” (Maylor and Blackmon, 2005:253). According to Eisenhardt (1989:548), in their attempts to synthesise earlier work on qualitative methods, including case study research and grounded theory, theory-building in “normal science” relies on:

“...past literature and empirical observation or experience as well as on the insight of the theorist to build incrementally more powerful theories. However, there are times when little is known about a phenomenon, current perspectives seem inadequate because they have little empirical substantiation, or they conflict with each other or common sense... In these situations, theory building from case study research is particularly appropriate because the theory building from case studies does not rely on previous literature or prior empirical evidence... In sum, building theory from case study research is most appropriate in the early stages of research on a topic or to provide freshness in perspective to an already researched topic.”

Though the concept of Information Governance has received much attention from scholars (Nguyen *et al.*, 2014) the South African public higher education context is in a state of disruptive uncertainty, characterised by, for example, the #feesmustfall movements (Habib, 2016) and the perceived and sometimes real threat of losing qualification accreditations (UNISA, 2017). Prior to the promulgation of the Reporting Regulations and Information-related legislation already mentioned, institutions were not forced to consider (let alone adopt) a holistic Information Governance programme. Thus, the investigation into and the (potentially) resultant development of an Information Governance programme provides the ideal case setting to address the research questions. Further, the grounded case study design acknowledges that the research questions may be altered during the iterative nature of the approach. For example, at the initial outset of the research in 2016, the Information Regulator of South Africa had not yet released the regulations which would give effect to POPIA. At the time of writing, the Information Regulator has already released draft regulation for public commentary and the window for commentary has already closed. The formal promulgation of the regulations may push an institution to re-assess its Information Governance stance, which in turn may highlight opportunities for future reference (see Chapter 6).

Thus, this study adopted Eisenhardt's (1989) road map for using grounded case study. Maylor and Blackmon (2005:254), summarise the approach as:

1. Getting started—problem definition;
2. Selecting cases—theoretical sampling;
3. Crafting instruments and protocols—preparing multiple data collection methods;
4. Entering the field—collecting the data;
5. Analysing the data—within-case analysis followed by cross-case analysis;
6. Shaping hypothesis—building evidence and explanation;
7. Enfolding literature—comparing findings with the literature; and
8. Reaching closure—knowing when to stop.

The grounded case study is typified by constant iteration between steps 1 through 7. While steps 1 through 4 are common to all case study research, steps 5 through 7 allowed me to revisit already collected data when and as, for example, local and international regulators promulgated new or amended already existent applicable legislation. This opening chapter focuses on steps 1 through 2. I shall expand further on the other steps within the thesis.

### **Strengths and limitations of research design**

Cousin (2009:148) summarises the strengths of case study research by stating that it “has the potential to generate rich understandings be they of a single case or a set of similar cases; it offers flexible and creative ways of researching live settings; and it licenses evocative write-ups that aim to describe, interpret, and persuade the reader.” To this, one can add Eisenhardt's (1989:546-547) discussion on the strengths of the grounded case study, including:

- the likelihood of it generating novel theory (through the creative insight arising from “the juxtaposition of contradictory or paradoxical evidence”);
- that the emergent theory will likely “be testable with constructs that can be readily measured and hypotheses that can be proven false”; and
- that the resultant theory will likely be empirically valid, as “the theory-building process is so intimately tied with evidence that it is very likely that the resultant theory will be consistent with empirical observation [i.e. the data upon which the emerging theory is grounded].”

However, despite these strengths, Eisenhardt (1989:547) identifies several potential limitations, including:

- the “intensive use of empirical evidence can yield theory which is overly complex” in “attempts to build theory which tries to capture everything”; and
- that “building theory from cases may result in narrow and idiosyncratic theory” or “that the theorist is unable to raise the level of generality of the theory”.

Maylor and Blackmon (2005:261) identify several other disadvantages, including an increased time and resource investment when compared to other methods of research. Stake (1995, cited by Cousin 2009:146) cautions against accumulating a “daunting data mountain”. Pettigrew (1988, cited by Eisenhardt, 1989:540) describes an ever-present danger of “death by data asphyxiation.” Given the time sensitivities surrounding legislative comply-by dates, I thus restricted this research project to a single South African public higher education institution as discussed below.

## **Unit of analysis**

Eisenhardt (1989:540) recognises that “within-case analysis is driven by one of the realities of case study research: a staggering volume of data” made “all the more daunting because the research problem is often open-ended.” Eisenhardt (1989:540) thus recognises “detailed case study write-ups... [as] central to the generation of insight because they help researchers to cope early in the analysis process with the often enormous volume of data.” This allows the researcher to become intimately familiar with the case, which in turn “allows the unique patterns of [the] case.”

I therefore initially restricted this study to a single case— a single South African public higher education institution. Of particular note, the selected institution houses an academic faculty of health sciences, which expands its compliance universe dramatically through the inclusion of the National Health Act (61 of 2003) and supporting regulations and guidelines. Data collection and analysis initially focused on the legislation, industry codes, industry standards, and supporting documentation relevant to the institution. Thereafter, data collection and analysis focused on internal documentation, including but not limited to the institution’s statute, strategic documentation, policy documentation, relevant project and programme documentation, audit and assessment reports, meeting minutes and memoranda, and draft and final versions of the project deliverables.

Due to the iterative nature of the grounded case study approach, however, I did identify merit in conducting some cross-case analysis, albeit limited in nature. Thus, I conducted an additional review of the publicly available institutional Information Governance policies, procedures, and organisational

structures of other local or international organisations, including universities (particularly those based within the European Union).

Though not part of the European Union, South African organisations must still consider the Union's legislation in their operations. For example, consider Recitals 23 and 24 of the GDPR (2016):

Recital 23: “the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.”

Recital 24: “the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.”

With the above in mind South African higher education institutions might be subject to the GDPR if they, for example, specifically market programme offerings to people based in Europe (Recital 23) or track and/or trace institutional alumni. Within the context of international partnerships, including student, staff, and alumni movements, South African institutions must present a measure of GDPR readiness lest potential and current European partners refuse to enter into or renew agreements. Thus, any South African Information Governance programme must consider the position and requirements set by their international counterparts.

Further, through the inclusion of more cases, I am able to apply triangulation (“the use or comparison of more than one method or source of data in the study of social phenomena” (Bryman (2012:392)) to my work, which in turn improved my ability to meet the criteria of trustworthiness (in turn comprised of credibility, transferability, dependability, and confirmability) and authenticity of my work (Bryman, 2012:391-393). These criteria, introduced by Lincoln and Guba (1985 as cited by Bryman, 2012:390) and Guba and Lincoln (1994 as cited by Bryman, 2012:390), present a second position in relation to reliability and validity for the evaluation of qualitative research. It is with these criteria in mind that I unpacked and understood my role as researcher within the study as detailed below.

## **Role of the researcher**

During the course of the study, I was employed at a South African public higher education institution. Within my position, my responsibilities included those of the Deputy Information Officer (under the Promotion of Access to Information Act (2 of 2000) (“PAIA”)). Within the execution of my duties, I was exposed to Information-processing across the institution and contributed directly and indirectly to sector

developments (such as sector engagement with the South African Information Regulator, as part of a Universities South Africa (“USAf”) task team, to develop a sector code of conduct under POPIA). In particular, within my position I was able to provide direct input into the development of the sector code of conduct, make Information Governance-related recommendations to institutional senior and executive management, request and manage funds to introduce and/or enhance Information Governance-related initiatives, and co-ordinate and/or project manage smaller, individual Information Governance-related initiatives.

As already evidenced by my writing style, I have adopted a first person perspective. This first person approach has “fuelled a popular conception that because the interpretivist tradition accepts the impossibility of removing the subjective, it abandons any notion of objectivity” (Cousin, 2009:10). However, as Geertz (1973:16, cited by Cousin, 2009:10) argues:

“I have never been impressed by the argument that, as complete objectivity is impossible in these matter (as, of course, it is), one might as well let one’s sentiments run loose. As Robert Solow has remarked, that is like saying that as a perfectly aseptic environment is impossible, one might as well conduct surgery in a sewer.”

Instead of objectivity, the qualitative researcher should thus practice mindfulness (Bentz and Shapiro 1998, cited by Cousin, 2009:10) and reflexivity (Bryman, 2012:393). Interestingly, within the context of this research, mindfulness is a core concept of governance models found in the global east, such as Thailand’s Sufficiency Economy (Noy, 2011) and has also recently found its way into South African Corporate Governance codes, such as King IV, through the positioning of sustainable capital and Integrated Thinking. Reflexivity, in this context, entails a sensitivity to my “cultural, political, and social context,” acknowledging that the Knowledge from this reflexive position as a reflection of my “location in time and social space” (Bryman, 2012:393). Through reflexivity I acknowledge my role as “part and parcel of the construction of Knowledge” and as somebody who “extracts Knowledge from observations and conversation with others and then transmits Knowledge to an audience” (Bryman, 2012:394).

It is at this point that I should mention that, before accepting my current position within a South African higher education institution, I worked within risk consulting with a particular focus on the audit and governance of Information Technology, related risks, and related sub-disciplines such as Business Continuity and Disaster Recovery Planning. This experience has undoubtedly flavoured my analysis, my writing style, and the recommendations set forth in the concluding chapter of this thesis. Further, in the last few months of my study, I was nominated and then elected to the board of directors of the South African chapter of ISACA. ISACA is an independent, non-profit, global professional association behind

several leading IT Governance-related frameworks and tool sets. As shall become clear in Chapter 4, my theoretical framework relies heavily upon ISACA-developed materials. Though I had settled on my theoretical framework more than a year before the board nomination cycle, this recent appointment of mine, coupled with my previous working experience, also lends a certain flavour to this work.

In attempts to address my concerns about my past work experience, my involvement with the body behind a large portion of my theoretical framework, and my current employment position, I purposefully broadened my literature review to look beyond a potentially too-narrow audit focus on the topic at hand. In doing so, I discovered and also considered Burawoy's discussion on the extended case method. Burawoy (1998:11), during his discussion on his own studies within the post-independence Zambian mining industry, reveals:

“As I discovered, those policies that did exist were constructed in post-hoc fashion, by “experts” like myself, to justify decisions already made. Had I not been a participant in these processes I would still be looking for that elusive company policy, or more likely would have concocted a policy from company rationalizations. In short, with the extended case method, dialogue between participant and observer provides an ever-changing sieve for collecting data. This is not to deny that we come to the field with presuppositions, questions, and frameworks but that they are more like prisms than templates and they are emergent rather than fixed.

By the same token replicability was also problematic. The data I gathered was very much contingent on who I was—a white male recently graduated from a British university with a degree in mathematics, a newcomer to colonialism, and an idealist to boot. Every one of these characteristics shaped my entry and performance in social situations and how people spoke to me of racial issues. More than that, anyone who replicated my study of Zambianization at a subsequent point in time would come up with very different observations. History is not a laboratory experiment that can be replicated again and again under the same conditions. There is something ineffably unique about the ethnographic encounter. It certainly would have been interesting for someone else to repeat the study, either simultaneously or subsequently, not as a replication but as an extension of my own study.”

Similarly, the data I gathered for this study (and how I interpreted and reported upon it) was contingent on who I am/was. Thus, though one could say that this study is very much still a grounded case study, it would also be fair to say that it has been tempered somewhat through a combination of my practicing mindfulness and researcher reflexivity, supported by the lessons learned by other researchers such as Burawoy. With this in mind, and in accounting for the juristic personhood assigned to organisations under South African law, I have strove throughout my study to maintain full compliance with Stellenbosch University policies for responsible and ethical research and the institutional permission and gatekeeper requirements of each of the institution's included within my study.

## Significance of research

In practice, the results of this study may be applied, by the institution reviewed, to its Information Governance programmes. On a larger scale, the results of this study may contribute towards the development of sector-specific codes of conduct (such as those allowable under POPIA) and/or as sector-specific clarifications for, for example, King IV.

## Ethical considerations

Though I have taken every effort to anonymise the institutions under review, there may still be enough contextual clues in this thesis which may enable an individual to correctly identify the institutions. Thus I have taken care to ensure that I do not directly or indirectly expose the institutions to harm in my data gathering, analysis, or my reporting. These potential risks were presented to each institution during my requests for institutional permission and I have adhered to any conditions set forth by each institution.

The primary risk involves highlighting point-in-time Information Governance-related gaps or weaknesses within an institution. Linking such gaps and weaknesses directly to an identifiable institution may expose the institution to reputational harm or other damages (such as an attacker exploiting a vulnerability in an institution's Information- or Cybersecurity). To mitigate this risk, I have aimed to de-identify the institutions as far as possible in my reporting, including the use of generic terms or pseudonyms for institutional functions, and actively exclude active gaps or weaknesses (i.e. I have only discussed gaps and weaknesses that were successfully addressed).

## Conclusion

In this opening chapter, I have introduced the background and motivation behind my research, my research questions, my research design, my unit of analysis, how I have understood my role as researcher, and how I addressed ethical considerations. Within the remainder of this thesis, I build upon this foundation:

- In chapter 2, I position a definition for Information in terms of this study and thereby define my writing conventions to be used throughout the remainder of this thesis;
- In chapter 3, I briefly trace the history of Information Governance in the South African context and use that as a basis to define my theoretical framework based on the Information-related laws, codes, and standards that a South African public higher education institution must comply with and those that it may voluntarily comply with;

- In the following chapters, I report on my analysis of documentation and vignettes drawn from my case studies discussing how the institutions addressed individual Information Governance sub-disciplines, with a particular focus on privacy; and
- In the concluding chapter, I present a set of recommendations and a potential starting point from which a South African public higher education institution could ultimately use to bridge any gaps between its latest POPIA gap assessment and its desired position.

## *Chapter Two: Defining Information*

### **The trouble with definitions**

Information Governance is often defined by the sub-disciplines and related fields that would fall within an Information Governance programme. King III (Institute of Directors in Southern Africa, 2009:54), for example, defines Information Governance:

“[A]s an emerging discipline with an evolving definition. The discipline embodies a convergence of Data Quality [Management], Data Management, Business Process Management, and Risk Management surrounding the handling of Data in a company. Also defined as Data Governance”.

Similarly, in the self-proclaimed “first book to articulate a truly holistic approach to Information Governance,” Smallwood (2014:5) positions Information Governance as a super discipline that:

“...emerged as a result of new and tightened legislation governing businesses, external threats such as hacking and data breaches, and the recognition that multiple overlapping disciplines were needed to address today’s Information Management challenges in an increasingly regulated and litigated business environment. [It] is a subset of Corporate Governance, and includes key concepts from Records Management, Content Management, Information Technology and Data Governance, Information Security, Data Privacy, Risk Management, litigation readiness, regulatory compliance, long-term digital preservation, and even Business Intelligence. This also means that it includes related technology and discipline subcategories, such as Document Management, Enterprise Search, Knowledge Management, and Business Continuity and Disaster Recovery... Information Governance is a policy-based management of Information designed to lower costs, reduce risk, and ensure compliance with legal, regulatory standards, and/or corporate governance.”

While the above two definitions are certainly useful (insofar that they already to some extent define the scope of a potential Information Governance programme), they quickly run into problems. Can we, as King III suggests, refer to Information Governance as Data Governance? If Information Governance includes Knowledge Management, as Smallwood suggests, could we refer to a Knowledge Governance programme instead? If not, why not?

Within the field of Information Science, there appears to be little agreement on definitions for Data, Information, Knowledge, and the relationships between them. There is, however, agreement that the lack of a standardised and agreed definition leads to considerable ambiguity and confusion which potentially inhibits the ability to compare studies or build upon the works of others (Wilson, 1981; Nitecki, 1985;

Buckland, 1991; Meadow and Yuan, 1997; Capurro and Hjørland, 2003; Dinneen and Brauner, 2015). Though this study does not intend to produce universal definitions for Data, Information, and Knowledge, there remains merit in exploring the debate surrounding the terms.

As Braman (1989, as cited by Capurro and Hjørland, 2003:374) cautions, selecting one definition of Information over another may have important consequences as each definition has its own benefits and problems. Braman argues further that the tendency to neglect this problem “results in conflict rather than co-operation; [defining] Information is thus also a political decision” (Capurro and Hjørland, 2003:374). Similarly, Buckland (1991:357) argues, “progress beyond an anarchy of individual opinions concerning what is or is not reasonably treated as Information depends on agreement, or on at least some consensus.” Yet, Felix Cohen (1950, as cited by Meadow & Yuan, 1997:698) suggests that a definition only need be useful in communication:

“Once we recognise that a definition is, strictly speaking, neither true nor false but rather a resolution to use language in a certain way, we are able to pass the only judgement that ever needs to be passed on a definition, a judgement of utility or inutility.”

Thus, this exploration shall serve as the basis for establishing how I have and shall continue to use the terms in this text—my writing conventions. This should enable a shared understanding between author and reader.

## Writing conventions

In this text, I have:

1. capitalised every word used in the naming of disciplines, subjects, frameworks, or fields of study (such as Corporate Governance, Information Governance, Information Science, Information Security, and Knowledge Management);
2. used the lowercase for data, information, and knowledge when referring to a specific instance (such as when referring to the research data in my analyses);
3. capitalised Data, Information, Knowledge, and Wisdom (occasionally abbreviated as D, I, K, and W respectively) when referring directly to the concept; and
4. unless otherwise made explicit by context, used Information to refer to a D-I-K or I-K spectrum or continuity, as argued by some authors and as detailed further below.

The arguments for the first three conventions are straightforward: they reduce ambiguity in my writing. The final convention, however, requires some explanation. As the King III and Smallwood definitions

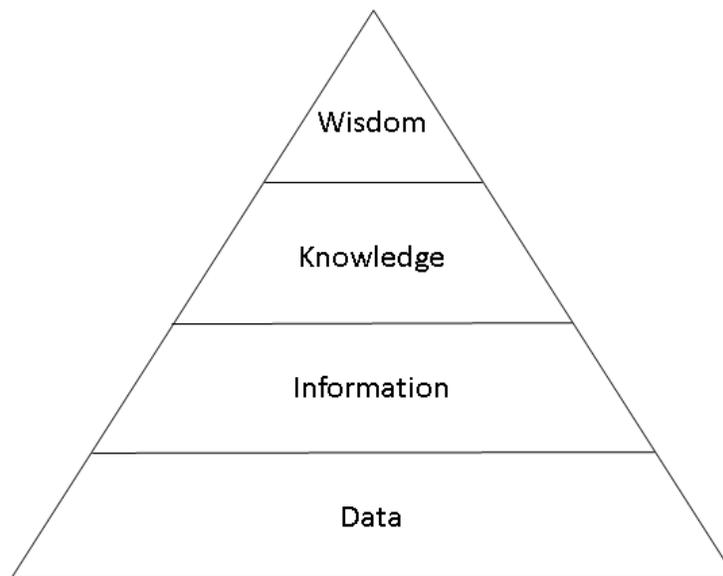
suggest, Information Governance encompasses Data- and Knowledge-focused fields (at least in name). The fourth convention enables me to capture this broad scope of Information Governance succinctly: Information, when used in this way, covers Data, Information, and Knowledge. The literature does provide support for this view as detailed below, providing a starting point for our exploration of the ongoing definition debate.

In 2007, Zins gathered and reported on 130 definitions for Data, Information, and Knowledge from 45 then-prominent Information Science scholars. Badia (2014:1285), in his secondary analysis of Zins' collected definitions, identified a shared "strong sense" of a hierarchical order among the concepts: "Information is derived from Data, and Knowledge from Information". Badia (2014:1285) noted, for the contributing scholars, that:

- Information was seen as playing a connecting role between Data and Knowledge, at times considered as a special type of Data and at other times as a special kind of Knowledge;
- The hierarchy functioned as a feedback loop in which what "we consider Data are influenced by the Information and Knowledge we already have"; and
- Even in agreeing that "Data, Information, and Knowledge are distinct concepts, the authors see them as nodes in a network of interactions, not as ladders in an ascending sequence."

Similarly, in her revisiting of the Data-Information-Knowledge-Wisdom hierarchy ("DIKW")—arguably the most widely recognised visual representation of a hierarchical order between the concepts; also known as the Knowledge Pyramid (see figure 1)—Rowley (2007:174-175) notes that:

"There is a consensus that Data, Information, and Knowledge are to be defined in terms of one another, although Data and Information can both act as inputs to Knowledge... There is however less agreement as to the nature of the processes that convert Data into Information, and Information into Knowledge, to the extent that it is not clear whether there are in fact three distinct concepts... is there a sharp divide between Data, Information, and Knowledge, or do they lie on a continuum with different levels of meaning, structure and actionability occurring at different levels? So [is it] possible to have Knowledge with different levels of meaning and actionability?"



*Figure 1 The DIKW Pyramid*

Nitecki (1985:390-391) argues that when used as a noun, both Information and Knowledge have very similar meanings, standing for a “content of a given message.” When used as verbs, they are used to instead emphasise the process of transference from “something in Information into something else in Knowledge.” Citing and building upon the work of Vinken (1982), Nitecki (1985:396) following the verb usage of Information and Knowledge, argues for an Information-Knowledge continuum:

“The Information-Knowledge continuity starts... with Information generating Knowledge, while Knowledge in turn generates Information on the higher level; thus... new Information supersedes old Knowledge.”

In understanding Data, Information, and Knowledge as a spectrum, continuum, or continuity, it allows one to consider a wider array of Information Governance sub-disciplines (such as Data Governance and Knowledge Management) more easily at our level of investigation, while acknowledging scope for an individual Information Governance (or sub-discipline) implementation to define its own understanding of the concepts, as discussed in more detail below.

## **Defining Information**

The literature suggests numerous views and conceptualisations of Information, including but not limited to the following list, in no particular order:

- Information-as-Data;
- Information-as-thing;
- Information-as-process;

- Information as a resource;
- Information as a commodity;
- Information-as-Knowledge; and
- Information as a pattern of energy and matter.

Universities are unique, in a sense, simultaneously relying on institutional-level Information (such as financial Information) to effectively manage its operations and to meet statutory reporting requirements, while discovering, delivering, and disseminating new Information as one of its core outputs through its teaching, learning, and research initiatives. Thus, within the context of a public South African university, each faculty, academic department, and administrative or support division would find more utility in its own preferred conceptualisation of Information, rather than an attempted universally-applied institutional definition. To illustrate this, I briefly discuss two of the various conceptualisations of Information listed above:

*Information-as-Data:* King III (2009:54) defines Information as “raw Data that has been verified to be accurate and timely, is specific and organised for a purpose, is presented within a context that gives it meaning and relevance and which leads to increase in understanding and decrease in uncertainty.” This definition aligns with the general usage of the word Data to imply a “lower or unrealised category compared with Information” (Meadow & Yuan, 1997:703). However, even Data may have its “semantic and syntactic aspects” (Meadow & Yuan, 1997:703). Take, for example, the following number sequence 9202204720082. In isolation, it may be a meaningless string of 13 digits. However, a South African, may be able to recognise the 13 digits as a South African ID number<sup>1</sup>. Those familiar with the structure (YYMMDDSSSSCAZ) of the ID number may be able to derive far more from the number sequence (Western Cape Government, 2016):

- the first 6 digits (YYMMDD) represent the individual’s date of birth in YY-MM-DD format;
- the following 4 digits (SSSS) represent gender (0000-4999 for female and 5000-9999 for male);
- the 11<sup>th</sup> digit (C) represents citizenship (0 for South African born, 1 for permanent resident);
- the 12<sup>th</sup> digit (A) was once used to denote race, but now defaults to an 8;
- and the final digit (Z) is a Luhn algorithm checksum digit used to validate the accuracy of the number sequence.

---

<sup>1</sup> 9202204720082 is a fictitious ID number used here and by the Western Cape Government for illustrative purposes.

Even with such a simple example, we can illustrate different levels of understanding of, essentially, a single datum. To some, 9202204720082 is a meaningless string of numbers while, to others it represents a South African born woman with a birthdate of 20 February 1992.

Meadow and Yuan (1997:704) thus present three possible definitions for Data:

1. “Data is a set of symbols in which the individual symbols have potential for meaning but may not be meaningful to a given recipient.
2. Data is a set of symbols in which the individual symbols are known, but the combination is meaningless: the semiotics are known, the syntactics are not.
3. Understandable symbols rejected by the recipient as being of no interest or value, typically because redundant or disbelieved.”

Thus, if “the symbols are understood, new, or meaningful to the recipient, they are called Information” (Meadow & Yuan, 1997:704). Expanding upon the above example, while South African ID numbers are powerful identifiers, they may not apply to some of a university’s international students and staff. Institutions additionally assign unique institutional numbers to each student and member of staff. As with ID numbers, institutional numbers could be viewed as Data and/or Information.

For example, at my own institution, Stellenbosch University, institutional numbers are used in the assigning of an e-mail address to each student, using the format [institutional number]@sun.ac.za. From an Information Security or Data Privacy perspective (which are Information Governance sub-disciplines according to Smallwood (2014)), e-mail addresses could be used to launch all manner of cyber-attacks (including spam, phishing, and other unsolicited direct marketing). With the correct institutional context, a list of institutional numbers may be thus considered as Information-as-Data. However, Stellenbosch University institutional numbers are generated algorithmically (i.e. not simply assigned sequentially). A spammer could create a list of potential Stellenbosch University e-mail addresses using the institution’s basic e-mail address structure, but would receive many failed deliveries, making such an approach unattractive. Therefore, from a security and privacy perspective, Stellenbosch University must control access to the algorithm and to lists of valid institutional numbers (especially those linked to active e-mail accounts), even when those lists hold no other Data and no matter how other areas within the institution may use those institutional numbers.

*Information-as-thing:* Buckland (1991:356) asks: if Information is merely Data processed into meaningful form, as suggested by the Information-as-Data discussion, then what do you call “other informative things, such as fossils, footprints, and screams of terror” and how much “processing and/or

assembling is needed for Data to be called Information”? Buckland (1991:351) used the term *Information-as-thing* for “objects, such as Data and documents, [which] are referred to as ‘Information’ because they are regarded as being informative.” He argues that the object can be anything under consideration, using an appropriate example in terms of our investigation into South African higher education:

“Any established university, for example, is likely to have a collection of rocks, a herbarium of preserved plants, a museum of human artefacts, a variety of bones, fossils, and skeletons, and much else besides... objects that are not documents in the normal sense of being texts can nevertheless be Information resources, Information-as-thing. Objects are collected, stored, retrieved, and examined as Information, as a basis for becoming informed” (Buckland, 1991:354).

Buckland (1991) further acknowledges some problems with the Information-as-thing view as anything might be informative and thereby anything may be Information. Dinneen and Brauner (2015) identify further problems with this view such as the context of the objects in question potentially changing what can be learned from the object; and the difference between the contents of a book or DVD-ROM disc being informative, for example, versus the book or disc as objects in of themselves being informative. Similarly, Meadow and Yuan (1997) further highlight the importance of the one doing the regarding of the object within the Information-as-thing view. Buckland (1991:357), not completely discounting other views of Information, therefore argues that Information-as-thing is meaningful in two senses:

“(1) At quite specific situations and points in time an object or event may actually be informative, i.e., constitute evidence that is used in a way that affects someone’s beliefs; and (2) Since the use of evidence is predictable, albeit imperfectly, the term “Information” is commonly and reasonably used to denote some population of objects to which some significant probability of being usefully informative in the future has been attributed. It is in this sense that collection development is concerned with collections of Information.”

Though not without its problems, Information-as-thing may be of particular relevance within the South African higher education sector, as Buckland identified, in the management of physical laboratory samples (potentially including human tissue), works of art, and historical artefacts. Based on an individual university’s understanding of Information, an Information Governance programme’s scope may include only the documentation accompanying the objects, the objects themselves, or both. Practically, universities may have to leave this decision to the experts within each area in question. This of course hints at delegating Information Governance responsibilities, which I shall discuss in more detail in my theoretical framework.

## **Our Non-Definition for Information (Expanded Writing Conventions)**

The manner in which an organisation defines Information may define its Information Governance and Management scope and approaches. Governing and managing things (physical or not) is very different from governing and managing processes. However, given the variety between environments within a university, it may be impossible to or even undesirable to attempt to apply one specific conceptualisation of Data, Information, and/or Knowledge to a university. Thus, this study shall not subscribe to any one or any particular combination of conceptualisations. Or rather, when referring to Information, unless referring to a specific conceptualisation as made clear by context, I shall allow for any conceptualisation. As such, my fourth writing convention, Information as a D-I-K spectrum, also covers Information as a spectrum or continuum of conceptualisations.

This said, the South African Higher Education sector is constrained by South African legislation, international legislation, and leading standards and practices. These pieces of legislation, standards, and practices shall form the basis of my theoretical framework. Many of these documents often define Data, Information, and Knowledge in very specific ways. For example, the South African Protection of Personal Information Act 4 of 2013 clearly defines what the South African government considers as Personal Information. Though, we cannot ignore these definitions in our analysis, an individual environment within a university may still apply its own conceptualisation(s) of Information to Personal Information to give effect to the legislation. In the Health Sciences, for example, should we consider a vial of human blood as Personal Information (i.e. Information-as-thing)? Or is the vial's label the Personal Information? Or is the Personal Information in the analysis of the blood, and report thereof? Or all three? If it is the vial, then physical security and access control is more important. If it is the label, then measures must be taken to remove personal identifiers from the label (such as the use of a participant number system). If it is the analysis, then logical security and access controls are more important. If it is all three, then all security measures are equally important.

## **Conclusion**

To summarise, Information can be conceptualised in a variety of ways. In any given context, any number of those conceptualisations, in isolation or in combination, may be considered useful. As Wilson (1981:4) argues: “the problem seems to lie, not so much with the lack of a single definition as with a failure to use a definition appropriate to the level and purpose of the investigation.” This study thus does not aim to define useful definitions for any particular environment or institution. Instead, in terms of Information Governance, this study argues that it may be more useful for an Information Governance framework or

programme to accommodate multiple conceptualisations of Information, and differences thereof between individual organisational units, provided that such conceptualisations still allows an organisation to, at least, meet its legislative requirements. In later chapters, I lean more heavily on legislative definitions of Personal Information. Interestingly, those legislative definitions would appear to support the argument for multiple conceptualisations of Information.

## *Chapter Three: History of Information Governance*

Given the multidisciplinary and varied nature of Information Governance and the unique requirements of each organisation, as discussed in the previous chapters, there is merit in stepping back and examining the history of the term and concept. In particular, through a review of the available literature, this chapter examines the likely origin of the concept, the ensuing concept drift or forking of the concept, and the history behind the explicit statutory requirements for Information Governance within the South Africa higher education sector. This view will inform the theoretical framework as statutory requirements may push institutions to comply with or adopt specific codes and standards of Corporate Governance, Information Governance, Technology Governance, and Compliance Governance.

### **The origin of Information Management**

Literature suggests that early investigations focused on Information Governance as a means to reduce the chances of Information Management failures occurring; reduce the impact of an Information Management failure should it occur; and strengthen compliance with applicable legislation and other requirements. Thus we begin our examination of the history of Information Governance with a brief look at the history of Information Management.

Kahn and Blair (2004:10) suggest that the concept of Information Management was first popularised by the United States government Commission on Federal Paperwork Report. The Report delivered 770 recommendations aimed at eliminating “needless paperwork while assuring that the Federal Government has the Information necessary to meet the mandate of the law and operate efficiently” (Commission on Federal Paperwork, 1977:1), ultimately addressing the “multi-billion dollar wall of paperwork [that had] been erected between the [US] Government and the people” (in a letter to the then-President of the United States of America preceding the report from the Commission on Federal Paperwork, 1977).

From this point, Information Management evolved, as with Information Governance, along many routes varying between organisations, professional bodies, and academics. Thus, Kahn and Blair (2004), as part of their own investigation into Information Management failures, distil several then-contemporary definitions of Information Management into their own, which we will use as the starting point for our discussion on the history of Information Governance. They argue that Information Management is about:

“...determining which Information created and received by [an] organisation is valuable in some way, based on its content; making sure that this Information is properly protected, stored, shared, and transmitted; and making it easily available to the people who need it, when they need it, and in a format that they can rely on... [it is] an umbrella term that includes a variety of disciplines and activities, each focusing on different kinds of Information and different kinds of management... in the broadest sense, Information Management touches on every business activity where Information is received or created” (Kahn & Blair, 2004:10).

## The early days of Information Governance: United Kingdom

In 1997, the Chief Medical Officer of England commissioned the *Caldicott Committee's Report on the Review of Patient-Identifiable Information* (the “Caldicott Report”) due “to increasing concern about the ways in which patient Information [was] used in the National Health Services (“NHS”) in England and Wales and the need to ensure that confidentiality is not undermined.” The final Report included 16 recommendations to “[develop] a direction of travel, [outline] good practice principles and [call] for regular reviews of activity within a clear framework of responsibility” for the handling of patient Information (Caldicott Committee, 1997:iii).

Kooper, Maes, and Lindgreen (2011:196) suggest that Donaldson and Walker (2004) were the first to scientifically introduce the concept of Information Governance while aiming to develop a series of refined national standards to support the handling of Information within the NHS. In developing their standards, Donaldson and Walker (2004) defined the HORUS model to guide NHS Information Governance policy and practice, which discussed:

- **H**olding Information securely and confidentiality;
- **O**btaining Information fairly and efficiently;
- **R**ecording Information accurately and reliably;
- **U**sing Information effectively and ethically; and
- **S**haring Information lawfully and appropriately.”

Though Donaldson and Walker (2004) did not explicitly reference the Caldicott Report, one can infer that their work (or at least the implementation of the HORUS model within the NHS) was influenced by the Caldicott Report. Subsequent NHS Information Governance related reports, publications, marketing materials, and training materials combine both the standards developed within the HORUS model and the Caldicott Report’s recommendations. Cayton (2006), as the then Chair of the NHS’ Care Record Development Board, defines Information Governance as:

“the structures, policies and practice of the [Department of Health], the NHS, and its suppliers to ensure the confidentiality and security of all records, and especially patient records, and to enable the ethical use of them for the benefit of individual patients and the public good.”

In their 2008 training material, the NHS expanded upon the HORUS model, stating that:

“Information Governance allows organisations and individuals to ensure that Personal Information is handled legally, securely, efficiently and effectively, in order to deliver the best possible care. It additionally enables organisations to put in place procedures and processes for their corporate Information that support the efficient location and retrieval of corporate records where and when needed, in particular to meet requests for Information and assist compliance with Corporate Governance standards” (United Kingdom National Health Service, 2008).

These definitions put a strong focus on confidentiality, security, and compliance, thus reiterating the suggested original goals for Information Governance (prevent or mitigate Information Management failures). These elements are mirrored in the materials emerging from elsewhere in the world as discussed further below.

## **The early days of Information Governance: the United States**

The NHS were not the only ones studying past Information Management failures and concerns in an attempt to determine the way forward. In the context of an environment given shape by high profile business failures such as the Enron-Arthur Andersen scandal of the early 2000’s, and resulting new laws and regulations (such as the Sarbanes-Oxley Act of 2002 (“SOX”)), Kahn and Blair (2004), argued that organisations required a new set of tools and principles for the changing Information Management landscape to learn from and prevent a reoccurrence of such scandals while also creating space to take advantage of new opportunities. Kahn and Blair thus introduced the concept of Information Management Compliance (“IMC”). Though they do not formally refer to it as Information Governance, there remain strong overlaps between IMC and the NHS definitions already discussed. Kahn and Blair (2004:3-4) state that IMC involves:

“...developing Information Management criteria based on legal, regulatory, and business needs; and developing and implementing controls designed to ensure compliance with those policies and procedures.

... a proactive approach which recognises that legal protection and business value will result from taking a formal, disciplined, visible, funded, and sustained approach—an approach that begins with an understanding of how an organisation’s Information Management activities are likely to be judged by the courts, regulators, auditors, and its own executives and shareholders.

...a holistic approach that covers many areas of concern, including: storage management, privacy, Business Continuity and Disaster Recovery Planning, Records Management, Information Security, transaction management, application development and integration, technology purchasing and acquisition, system configuration and management, and many other areas.”

To support this stance, Kahn and Blair (2004) further introduced practical, actionable items that would enable IMC—the seven keys to IMC:

1. Good policies and procedures;
2. Executive-level programme responsibility;
3. Proper delegation of programme roles and components;
4. Programme communication and training;
5. Auditing and monitoring to measure programme compliance;
6. Effective and consistent programme enforcement; and
7. Continuous programme improvement.

These seven keys to IMC were modelled after the United States Federal Sentencing Guidelines, which Kahn and Blair (2004:4) note “are used by federal courts to determine appropriate punishment for individuals and organisations that violate federal law.” This again highlights what appears to be the original focus of Information Governance: protecting Information and thereby preventing or minimising the fallout of non-compliance and/or Information Management failures.

### **The early days of Information Governance: South African Higher Education**

The Institute of Directors in Southern Africa released the King Code of Governance for South Africa 2009 (“King III”) in September 2009. King III, as reported in the Code itself, became necessary to address the demands of changes in international governance trends, the financial global crisis, and the then-newly-promulgated South African Companies Act (Act No. 71 of 2008). Yet, despite the progress made earlier in the decade, Information Governance programmes focused on ensuring compliance with corporate reporting and regulatory requirements (such as SOX), did little to predict, let alone prevent, the “collapse of many leading names in US banking and finance” such as those witnessed during the lead up to and during the 2008 global financial crisis (Institute of Directors in Southern Africa, 2009:8). It is within this context that we begin to see shifts in how the world views Corporate Governance, Technology Governance, and Information Governance. Within the South African higher education sector context, the South African Department of Higher Education and Training (“DHET”) released the 2014 Reporting Regulations and the complementary *Implementation Manual for Reporting by Public Higher Education*

*Institutions* in June 2014. These regulations specifically reference and expect South African higher education institutions to report, through an Integrated Report (discussed further below), against the principles, practices, and requirements of King III. Thus, we begin our specific examination of Information Governance within the South African higher education sector with an examination of the related demands put forward by the Reporting Regulations and, through them, King III.

King III (Institute of Directors in Southern Africa, 2009:9) begins by defining good governance as “essentially about effective leadership. Leaders should rise to the challenges of modern governance. Such leadership is characterised by the ethical values of responsibility, accountability, fairness and transparency and based on moral duties that find expression in the concept of Ubuntu<sup>2</sup>. Responsible leaders direct company strategies and operations with a view to achieving sustainable economic, social, and environmental performance.”

It is within this definition that King III recommends several governance principles and practices that would enable organisational leaders to embody the above definition. Among those principles, practices, and supporting documentation, of particular note, in the context of Information Governance, King III:

- discusses the 2008 global financial crisis within the context of the statutory-based Corporate Governance;
- recommends an “apply or explain” approach to its implementation, rather than a “comply or explain” or “comply or else” approach as seen elsewhere in the world;
- introduces the concept of Integrated Reporting to corporate South Africa; and
- addresses the concept of Information Technology (“IT”) Governance “in detail [in the Code] for the first time” (Institute of Directors in Southern Africa, 2009:15).

King III (Institute of Directors in Southern Africa, 2009:5) opens its discussion on the legislated basis for governance compliance by stating that “governance of corporations can be on a statutory basis, or as a code of principles and practices, or a combination of the two.” In the statutory regime (which King III refers to as “comply or else”), there are “legal sanctions for non-compliance.” Yet, as mentioned previously, SOX and all of its “statutory requirements for rigorous internal controls,” did not prevent the financial collapse within the United States which in turn served as the primary source of the global

---

<sup>2</sup> As defined in King III (Institute of Directors in Southern Africa, 2009:61), Ubuntu is a concept which is captured in the expression ‘uMuntu ngumuntu ngabantu’, ‘I am because you are; you are because we are’. Ubuntu means humaneness and the philosophy of Ubuntu includes mutual support and respect, interdependence, unity, collective work and responsibility.

financial crisis. King III (Institute of Directors in Southern Africa, 2009:6) thus raises the following argument against the “comply or else regime”:

“... a ‘one size fits all’ approach cannot logically be suitable because the types of business carried out by companies vary to such a large degree. The cost of compliance is burdensome, measured both in terms of time and direct cost. Further, the danger is that the board and management may become focused on compliance at the expense of enterprise. It is the duty of the board of a trading enterprise to undertake a measure of risk for reward and to try to improve the economic value of a company. If the board has a focus on compliance, the attention on its ultimate responsibility, namely performance, may be diluted.”

Thus, King III (Institute of Directors in Southern Africa, 2009:6) adopted an “apply or explain” approach to the principles and practices it recommends, describing that its practical execution should be addressed as:

“It is the legal duty of directors to act in the best interests of the company. In following the ‘apply or explain’ approach, the board of directors, in its collective decision-making, could conclude that to follow a recommendation would not, in the particular circumstances, be in the best interests of the company. The board could decide to apply the recommendation differently or apply another practice and still achieve the objective of the overarching corporate governance principles of fairness, accountability, responsibility and transparency. Explaining how the principles and recommendations were applied, or if not applied, the reasons, results in compliance. In reality, the ultimate compliance officer is not the company’s compliance officer or a bureaucrat ensuring compliance with statutory provisions, but the stakeholders.”

It is from this position that King III introduces the concept and requirement for Integrated Reporting to corporate South Africa. However, as the South African Institute of Chartered Accountants (“SAICA”) (SAICA, 2015:9) noted, “organisations that want to produce authentic integrated reports state that implementing its conditions is a journey; [it] takes some years to reach the position of presenting a high-quality report.” In 2013, the International Integrated Reporting Council (“IIRC”) realised the International Integrated Reporting (“<IR>”<sup>3</sup>) Framework to “establish guiding principles and content elements that govern the overall content of an integrated report, and to explain the fundamental concepts that underpin them” (IIRC, 2013:4). The <IR> Framework defines:

“... [An Integrated Report as] a concise communication about how an organisation’s strategy, governance, performance and prospects, in the context of its external environment, lead to the creation of value over the short, medium and long term” (IIRC, 2013:7); and

---

<sup>3</sup> <IR> is the writing convention used by the International Integrated Reporting Council.

... [ Integrated Reporting] as a process founded on Integrated Thinking that results in a periodic integrated report by an organisation about value creation over time and related communications regarding aspects of value creation” (IIRC, 2013:33).

From the above definitions, SAICA (2015) positions Integrated Thinking as the engine that drives value creation in organisations. Similarly, King and Roberts (2013:55) describe Integrated Thinking as “...seeing the connections of the resources and relationships, how they connect to the different functions, departments and operations in the company and getting the company as a whole working together in achieving the strategic objectives.”

The <IR> Framework defines:

- Integrated Thinking as “the active consideration by an organisation of the relationships between its various operating and functional units and the capitals that the organisation uses or affects. Integrated thinking leads to integrated decision-making and actions that consider the creation of value over the short, medium and long term” (IIRC, 2013:33); and
- Capitals as “stocks of value on which all organisations depend for their success as inputs to their business model, and which are increased, decreased or transformed through the organisation’s business activities and outputs” (IIRC, 2013:33).

Though organisations are expected to define their own capitals, the <IR> Framework introduces six model capitals:

- financial capital (the funds available to the organisation);
- human capital (including people’s competencies, capabilities, and experience);
- intellectual capital (including copyrights, licenses, patents, tacit knowledge, and procedures);
- manufactured capital (manufactured physical objects such as buildings and machinery);
- natural capital (all renewable and non-renewable environmental resources); and
- social and relationship capital (including brand, reputation, and social license to operate).

It is clear that organisations require a holistic view of Information, which cuts across intra-organisational silos, to enable Integrated Thinking. Information Management and Information Governance (though only briefly referenced in the reporting regulations, the <IR> Framework, and King III) may enable such a view. Unsurprisingly then, the *King IV Report on Corporate Governance for South Africa 2016* (“King IV”), released in November 2016, seeks to address this, through positioning Integrated Thinking at the fore and through the formal introduction of Technology and Information Governance, Risk Governance, and Compliance Governance requirements within the Code.

## IT Governance recognises that IT Governance is not enough

Before I delve into King IV, it may be prudent to take a closer look at the positioning of IT Governance over the same time period. King III acknowledges the importance and pervasiveness of IT within the modern organisation and therefore also acknowledges the importance of good IT Governance as part of good Corporate Governance. Kooper *et al.* (2010:195) argue that IT Governance is well established and describes “a subset discipline of Corporate Governance focused on IT systems and their performance and risk management.” From this, Hagmann (2013:229) suggests that IT began to lean on the concept of Information Governance to “strengthen the strategic aspects of IT risk and compliance and to treat IT-related disciplines under a holistic view” albeit with much confusion between IT Governance and Information Governance.

But before we delve further, we should first understand and define both the terms ‘technology’ and ‘Information Technology’. Starting with technology, the online version of Merriam-Webster (2017) defines technology as:

1. “a: the practical application of Knowledge especially in a particular area : engineering; medical technology  
b: a capability given by the practical application of Knowledge: a car's fuel-saving technology
2. a manner of accomplishing a task especially using technical processes, methods, or Knowledge: new technologies for information storage
3. the specialised aspects of a particular field of endeavour: educational technology”

Wilson (1981:8) similarly defines technology, as part of an attempt to develop a model for Information Behaviour, as “the general sense of whatever combination of techniques, tools and machines constitute the Information-searching subsystem.” When reflecting on his earlier attempts, Wilson (2005) refines his definition of technology simply to “anything that aids action”. With these definitions for technology in mind (coupled with the previous discussion on a definition for Information), we then find, unsurprisingly, the following definitions for Information Technology:

1. “The hardware, software, communication and other facilities used to input, store, process, transmit and output Data in whatever form” (ISACA, no date);
2. “This is the common term for the entire spectrum of technologies for Information processing, including software, hardware, communications technologies and related services. In general, IT does not include embedded technologies that do not generate Data for enterprise use” (Gartner, 2017); and

3. “Technology used to manage digital Information” (Smallwood, 2014:408).

With the rise of the Internet of Things (“IOT”), the above definitions begin to apply to a host of devices that historically would have fallen solely within another category of technology such as self-driving motor vehicles (automotive technology) and smart refrigerators (refrigeration technology). While Wortman and Flüchter (2015:221) argue that there is “no common definition or understanding of what the IOT encompasses,” Xia, Wang, Yang, and Vinel (2012:1101) provide a useful attempt at a definition for this study: the IOT is the “networked interconnection of everyday objects, which are often equipped with ubiquitous intelligence. [It] will increase the ubiquity of the Internet by integrating every object for interaction via embedded systems, which leads to a highly distributed network of devices communicating with human beings as well as other devices.”

Within the definition of Xia *et al.*, it is difficult to argue that an organisation’s IOT devices falls outside the scope of Information Technology Governance. However, traditional, for lack of a better word, Information Technology Governance frameworks, as they are currently implemented, may not adequately consider IOT and their related security and regulatory risks.

For example, University X concluded a rental agreement for new equipment for the institute’s gymnasium. Most of the procured equipment could be considered as smart, Internet-connected devices providing feedback (detailing how the equipment was used, how often it was used, and how it was functioning) to the gymnasium management. The equipment manufacturer also provided an option to bundle a rebranded instance of the manufacturer’s mobile app along with the equipment rental. According to the manufacturer’s website, the gymnasium may improve member retention and generate additional income, when a member uses both the equipment and app, through using the collected member’s personal information to:

1. Personalising training routines;
2. Monitoring lifestyle data;
3. Pushing personalised content, up- and cross-selling other apps and products, and other advertising.

Despite the above, the internal Information Technology procurement and change management processes only triggered once the gymnasium team began trying to get the app listed on the institution’s Play Store developer’s page (long after the institution’s acceptance of the equipment rental agreement). If it had not been for the attempt to list the app under the institution’s developer’s page, nobody may have informed

the Information Technology Division of the gymnasium equipment, which would have left the equipment excluded from the institution's Cybersecurity and IT Disaster Recovery initiatives.

In the aftermath of large scale IOT-based attacks, such as the October 2016 Dyn Distributed Denial of Service attack<sup>4</sup>, the US Department of Homeland Security released its Strategic Principles for Securing the Internet of Things in November 2016. In its opening paragraphs, and as a precursor to potential future regulation, the Principles (U.S. Department of Homeland Security, 2016:2) clearly outline the importance of adequately securing the IOT:

“Internet-connected devices enable seamless connections among people, networks, and physical services. These connections afford efficiencies, novel uses, and customized experiences that are attractive to both manufacturers and consumers. Network-connected devices are already becoming ubiquitous in, and even essential to, many aspects of day-to-day life, from fitness trackers, pacemakers, and cars, to the control systems that deliver water and power to our homes. The promise offered by IOT is almost without limit.

While the benefits of IOT are undeniable, the reality is that security is not keeping up with the pace of innovation. As we increasingly integrate network connections into our nation's critical infrastructure, important processes that once were performed manually (and thus enjoyed a measure of immunity against malicious cyber activity) are now vulnerable to cyber threats. Our increasing national dependence on network-connected technologies has grown faster than the means to secure it.

The IOT ecosystem introduces risks that include malicious actors manipulating the flow of information to and from network-connected devices or tampering with devices themselves, which can lead to the theft of sensitive data and loss of consumer privacy, interruption of business operations, slowdown of Internet functionality through large-scale distributed denial-of-service attacks, and potential disruptions to critical infrastructure.

Last year, in a cyber-attack that temporarily disabled the power grid in parts of Ukraine, the world saw the critical consequences that can result from failures in connected systems. Because our nation is now dependent on properly functioning networks to drive so many life-sustaining activities, IOT security is now a matter of homeland security.”

From the above, it should be clear IT Governance needs to consider far more than just the datacentre, network infrastructure, end user computers, and the IT services offered. IT Governance (and thereby Technology and Information Governance) must also consider IOT devices in all their forms (including

---

<sup>4</sup> Dyn, a Domain Name System provider, was hit by a Distributed Denial of Service (DDoS) attack on 21 October 2016. These attacks prevented users from accessing Dyn customer sites during the attack. In a statement released on 22 October 2016, Dyn confirmed that one source of the traffic for the attacks came from Internet of Things devices infected by the Mirai botnet (Dyn, 2016).

personal devices owned by, in a higher education context, students, staff, and visitors) and the associated security, privacy, and regulatory risks.

## Present day IT Governance

COBIT is a framework for governing and managing IT. Though COBIT provides only one view of IT Governance, it provides a model example for our discussion, considering its specific mention in King III. Looking at the history of COBIT (“Control Objectives for Information and Related Technologies”), ISACA (ISACA, 2012c) briefly traces the history of COBIT, using the publication of editions as milestones:

- COBIT (1996) and COBIT 2<sup>nd</sup> Edition (1998): an IT audit and control framework, with a focus on control objectives;
- COBIT 3<sup>rd</sup> Edition (2000): an IT Management framework through the inclusion of management guidelines; and
- COBIT 4.0 (2005) and 4.1 (2007): an IT Governance framework through the inclusion of governance and compliance processes (the most likely version(s) referenced within King III).

COBIT 4.1 (IT Governance Institute, 2007):5) defined IT Governance as:

“... the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise’s IT sustains and extends the organisation’s strategies and objectives.”

Both COBIT 4.1 and COBIT 5 open with a discussion on the value of Information and the role technology plays in supporting it. From this argument, COBIT 5 builds upon the previous editions by placing a closer focus on the elements of an organisation that enables IT and those elements that are enabled by or through IT. COBIT 5 understands governance of IT as fundamentally being “concerned with IT value delivery to the business and the mitigation of IT-related risk” (ISACA, 2012a:14). This value delivery and risk-mitigation is “enabled by the availability and management of adequate resources and the measurement of performance to monitor progress towards the desired goals” ISACA, 2012a:14). COBIT refers to these “adequate resources” as interconnected enablers—“factors that, individually and collectively, influence whether something will work” (ISACA, 2013:22). COBIT’s approach to governance (of IT, the greater enterprise, or any individual enabler) relies upon the systemic governance and management of interconnected enablers (ISACA, 2012a:27):

- “[Each enabler] needs the input of other enablers to be fully effective; and

- [Each enabler] delivers outputs to the benefit of the other enablers.”

Not unlike Kahn and Blair’s (2004) 7 keys to Information Management Compliance, the COBIT 5 framework identifies seven categories of enablers (ISACA, 2012a:27):

1. “**Principles, policies, and frameworks** are the vehicle to translate the desired behaviour into practical guidance for day-to-day management;
2. **Processes** describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals;
3. **Organisational structures** are the key decision-making entities in an enterprise;
4. **Culture, ethics, and behaviour** of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities;
5. **Information** is pervasive throughout any organisation and includes all information produced and used by the enterprise. Information is required for keeping the organisation running and well governed, but at the operational level, Information is very often the key product of the enterprise itself;
6. **Services, infrastructure, and applications** include the infrastructure, technology and applications that provide the enterprise with Information Technology processing and services;
7. **People, skills, and competencies** are linked to people and are required for successful completion of all activities and for making correct decision and taking corrective actions.”

Through the publication of the COBIT 5 supplement *Enabling Information* in 2013, the framework delves into the importance of Information Governance and Management, with references to the Data Management Body of Knowledge (“DMBOK”), as a prerequisite for the success of not only an IT Governance initiative, but organisational success as a whole. Within the principles of COBIT 5, *Enabling Information* aims to:

- provide “an Information-centric view of the enterprise [wherein] Information should ultimately support the goal of any enterprise—deliver value for its stakeholders—which translates to enterprise goals that should be achieved, [which cascades and translates into] more tangible enabler goals, in this case, Information quality goals” (ISACA, 2013:15);
- “cover the enterprise end-to-end” and “enable a holistic approach” by providing “a single model to structure Information that is applicable to all types of Information used by the enterprise, including Information used by business functions, Information internal to the IT function and external Information” (ISACA, 2013:16); and

- “focus on Information, [where] all the other enablers also support the Information enabler” (ISACA, 2013:16).

Further, COBIT 5 makes a clear distinction between governance and management as the “two disciplines encompass different types of activities, require different organisational structures and serve different purposes” (ISACA, 2013:16). At the highest level, COBIT 5 (ISACA, 2012a:31-33) identifies three broad categories of governance activities—to (1) evaluate, (2) direct, and (3) monitor—and four broad categories of management activities—to (1) plan (align, plan, and organise), (2) build (build, acquire, and implement), (3) run (deliver, service, and support), and (4) monitor (monitor, evaluate, and assess). Before addressing individual related Information issues (such as Master Data Management, fraud detection, regulatory compliance, and privacy), *Enabling Information* describes that Information Governance ensures that (ISACA, 2013:24):

- “Stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives, which are to be achieved through the acquisition and management of Information resources;
- Direction is set for Information Management capabilities through prioritisation and decision making;
- Performance and compliance of the Information resource are monitored against agreed-on direction and objectives.”

The supplement further describes Information Governance activities as (ISACA, 2013:24):

- “Communicating Information strategies, policies, standards, architecture and metrics;
- Tracking and enforcing regulatory compliance and conformance to Information policies, standards, architecture and procedures;
- Sponsoring, tracking and overseeing the delivery and operational execution of Information Management programmes; and
- Providing an understanding, based on stakeholder needs, of the decisions and priorities associated with Information resources.”

The supplement then defines Information Management as (ISACA, 2013:25):

“Information management plans, builds, runs and monitors the practices, projects and capabilities that acquire, control, protect, deliver and enhance the value of data and Information assets, in alignment with the direction set by the Information Governance body.”

From the above definitions, COBIT argues that governance and management comprise “different activities, with different responsibilities; however, given the role of governance—to evaluate, direct, and monitor—a set of interactions is required between governance and management to result in an efficient and effective governance system” (ISACA, 2012a:31). These interactions are summarised per enabler (as taken from ISACA (2012a:31)) below:

<b>Enabler</b>	<b>Governance-Management Interaction</b>
Principles, policies, and frameworks	“Principles, policies, and frameworks are the vehicle by which governance decisions are institutionalised within the enterprise, and for that reason are an interaction between governance decisions (direction setting) and management (execution of decisions).”
Processes	Interaction within processes are defined in each process’ RACI chart <sup>5</sup> . Even though COBIT distinguishes between governance and management processes, members of management are often consulted on or informed about a governance process and vice versa.
Organisational structures	“[Organisational] structures can sit in the governance space or management space, depending on [each structure’s] composition and scope of decisions. Because governance is about setting the direction, interaction takes place between the decisions taken by governance structures and the decisions and operations implementing the former.”
Culture, ethics, and behaviour	“Behaviour is also a key enabler of good governance and management of the enterprise. It is set at the top—leading by example—and is therefore an important interaction between governance and management.”
Information	COBIT’s process model describes inputs and outputs, including “Information exchanged between governance and management processes” with Information used for evaluating, directing, and monitoring explicitly described.
Services, infrastructure, and applications	“Services are required, supported by applications infrastructure to provide the governance body with adequate Information and to support the governance activities of evaluating, setting direction, and monitoring.”

<sup>5</sup> The RACI chart indicates who is Responsible for, Accountable for, Consulted on, and/or Informed about a particular process (ISACA, no date).

<b>Enabler</b>	<b>Governance-Management Interaction</b>
People, skills, and competencies	“Governance and management activities require different skill sets, but an essential skill for both governance body members and management is to understand both tasks and how they are different.”

*Table 1 COBIT 5 Governance and Management Interactions*

Before continuing, we should briefly relook at the HORUS model. The NHS model placed a strong focus on policy and practice (HORUS placed a strong focus on the processing of Personal Information), which represent but two of COBIT’s enablers. Looking at HORUS today, from the luxurious position of building upon more than a decade’s worth of further Information Governance-related study, the NHS model leans heavily towards Information Management or Data Governance, rather than Information Governance. COBIT’s holistic approach to Governance of Enterprise IT and Information mirrors the advances proposed within the discussions surrounding Integrated Reporting and Integrated Thinking. Such a view may support a response to the new requirements set out by King IV as discussed in the next section.

## **Present day Information Governance**

Revisiting Smallwood’s definition (2014:5-7) (as quoted earlier in Chapter 2, and quoted below in a more complete manner) introduces Information Governance as a super discipline that:

“emerged as a result of new and tightened legislation governing businesses, external threats such as hacking and data breaches, and the recognition that multiple overlapping disciplines were needed to address today’s Information Management challenges in an increasingly regulated and litigated business environment. [It] is a subset of Corporate Governance, and includes key concepts from Records Management, Content Management, Information Technology and Data Governance, Information Security, Data Privacy, Risk Management, litigation readiness, regulatory compliance, long-term digital preservation, and even business intelligence. This also means that it includes related technology and discipline subcategories, such as Document Management, Enterprise Search, Knowledge Management, and Business Continuity and Disaster Recovery... According to the Association of Records Managers and Administrators (“ARMA”), [it] is a strategic framework composed of standards, processes, roles, and metrics that hold organisations and individuals accountable to create, organise, secure, maintain, use, and dispose of Information in ways that align with and contribute to the organisation’s goals... [It] is how an organisation maintains security, complies with regulations, and meets ethical standards when managing Information... Information Governance is a policy-based management

of Information designed to lower costs, reduce risk, and ensure compliance with legal, regulatory standards, and/or corporate governance.”

The above definition, which borrows from the ARMA Generally Accepted Recordkeeping Principles, closely mirrors the definitions from the previous decade, which would suggest that the meaning of the concept has remained consistent since HORUS and IMC. Similarly, Logan (2010) introduced Gartner’s definition for Information Governance as:

“...the specification of decision rights and an accountability framework to encourage desirable behaviour in the valuation, creation, storage, use, archival and deletion of Information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of Information in enabling an organisation to achieve its goals.”

King IV, on the other hand, does not formally define Information Governance. We can, however, infer a definition for Information Governance from the Code’s definition for Corporate Governance (“the exercise of ethical and effective leadership by the governing body towards the achievement of the following governance outcomes: ethical culture, good performance, effective control, and legitimacy” (Institute of Directors South Africa, 2016:11)) and its recommended practices for Technology and Information Governance, which closely mirrors Smallwood’s list of Information Governance-related disciplines and sub-disciplines above. The Code does, however, also add that “the governing body should exercise ongoing oversight of the management of Information and oversee that it results in the... leveraging of Information to sustain and enhance the organisation’s intellectual capital” (Institute of Directors South Africa, 2016:63). This points towards a potential new understanding or focus of Information Governance: one that does not restrict itself to a purely compliance view, but one that also seeks to create value for organisations.

We see this view emulated by Barrenechea (2013:4), who, building upon the Electronic Discovery Reference Model’s 2012 Information Governance Reference Model, argues that at the heart of Information Governance, it is about “effectively using and managing an organisation’s Information assets to derive maximum value, while minimising Information-related risks. It applies to all corporate Information, regardless of form, function, or location. This includes structured and unstructured Information, and ranges from content on file systems and e-mail to Information within productivity and line-of-business systems, on web, social, and mobile environments.”

Kooper *et al.* (2011:199) argue that the traditional, hierarchical approach to governance may not be appropriate for Information Governance “since Information exchange does not restrict itself to the boundaries of an organisation.” Instead, they propose what they (Kooper *et al.*, 2011:195) call a “deviant,

Information based approach, built on the observation that (1) Information is the missing linking pin between business and IT, (2) Information is a business resource, independent of the supporting IT, and (3) Information, being interpreted Data, is, unlike IT and Data an intangible asset.” Kooper *et al.* (2011:197) thus loosely define Information Governance as “a framework to optimise the value of Information in some sense to [all of] the actors involved” (namely the actors that create Information, the actors that receive Information, and the actors that govern the interactions).

While these introductions, definitions, and recommended practices may provide good direction, each organisation faces its own set of unique requirements, challenges, risks, and opportunities, which requires a tailored Information Governance solution. King IV acknowledges this and, in order to make the Code as widely applicable as possible, while lowering the chance that the Code gets reduced to a mindless checklist-based compliance burden, advocates for the “mindful consideration and application of recommended practices [that] harnesses the benefits of Corporate Governance in the interests of the [individual] organisation and [that] applying the Governance Code comes to be seen as a process of adding value rather than subtracting value” (Institute of Directors South Africa, 2016:36). This would allow organisations to consider implementing either, neither, or a combination of both the ‘traditional’ compliance-driven and ‘deviant’ value-driven definitions for Information Governance. It is within this historical context that each institution within the South African Higher Education sector is faced with the opportunity to define Information Governance for itself and to grow its intellectual capital (arguably the primary currency of such institutions).

## **Conclusion: Technology and Information Governance**

As discussed above, King III followed an “apply *or* explain” approach for each of its 75 principles. King IV, on the other hand, follows an “apply *and* explain” approach for its much shorter list of 17 principles for good governance. King IV (Institute of Directors South Africa, 2016:7) argues that:

“...these principles can be applied by an organisation, and all are required to substantiate a claim that good governance is being practised. The required explanation allows stakeholders to make an informed decision as to whether or not the organisation is achieving the four good governance outcomes [ethical culture, good performance, effective control, and legitimacy] required by King IV. Explanation also helps to encourage organisations to see Corporate Governance not as an act of mindless compliance, but something that will yield results only if it is approached mindfully, with due consideration of the organisation’s circumstances.”

Interestingly, as mentioned above, King IV also introduces a Technology and Information Governance principle (as opposed to King III's principles for IT Governance), which states (Institute of Directors South Africa, 2016:62) that:

“The governing body should govern Technology and Information in a way that supports the organisation setting and achieving its strategic objectives.”

This principle and its list of supporting recommend practices, especially when read with the earlier vignette discussing the procurement of gymnasium equipment, hints at the possibility of a new Technology and Information Governance super discipline. Consider the opening paragraphs of this thesis, which argues that Information pervades throughout higher education institutions, along with King III's arguments regarding the pervasiveness of IT. With this in mind, we quickly see how impractical (and perhaps undesirable) it may be to maintain a separation between IT Governance and Information Governance. By twisting the word order into Technology and Information Governance (rather than Information and Technology Governance), King IV (knowingly or unknowingly, and despite distinguishing between technology and Information recommended practices under the principle) reinforces the idea of a new super discipline.

While this thesis will continue to maintain a large focus on the “traditional” Information Governance sub-disciplines, it will also explore the overlapping points, potential synergies, and potential conflicts between IT Governance and Information Governance. I discuss this exploration of Technology and Information Governance in my theoretical framework (in the next chapter) and the selected vignettes from the institutions under review in the chapters following thereafter.

## *Chapter Four: Theoretical Framework*

To guide my analysis of the research data drawn from my case study and interpretation and application of the relevant legislation, I employed a theoretical framework based on five key sources:

- King IV;
- The <IR> Framework;
- COBIT 5;
- The Three Lines of Defence model; and
- The vision, mission, values, and strategy documentation of University X.

### **King IV**

Though there is no formally legislated requirement stating that South African public higher education institutions must implement a response to King IV (whereas the 2014 Reporting Regulations specifically call out King III), I hold that only a very naïve institution would ignore King IV. For, as taken from King IV itself (Institute of Directors South Africa, 2016:35):

“Good governance does not exist separately from the law, and a Corporate Governance code that applies on a voluntary basis may also trigger legal consequences. A court considers all relevant circumstances in determining the appropriate standard of conduct for those charged with governance duties, including what the generally accepted practices for a particular setting and situation are. Voluntary governance codes such as King IV recommend leading practices for how governance duties should be discharged, and therefore influence and affect what practices are considered and eventually adopted and implemented by governing bodies. The more widely certain recommended practices in codes of governance are adopted, the more likely it is that a court would regard conduct that conforms to these practices as meeting the required standard of care. In this way the provisions of voluntary codes of governance find their way into jurisprudence to become part of the common law. Consequently, failure to meet an established Corporate Governance practice, albeit not legislated, may invoke liability.”

With taking the above into account, the recommended practices listed under the King IV’s Technology and Information Governance principle serve as a starting point for identifying the essential components and measurement factors required of an Information Governance programme within a South African public higher education institution. The recommended practices are listed in full in Appendix A. As an example, consider the following recommended practice (Institute of Directors South Africa, 2016:63):

“The governing body should exercise ongoing oversight of the management of Information and, in particular, oversee that it results in the following:

- a. The leveraging of Information to sustain and enhance the organisation’s intellectual capital.
- b. An Information Architecture that supports confidentiality, integrity, and availability of Information.
- c. The protection of privacy of Personal Information.
- d. The continual monitoring of security of Information.”

From the above, one can begin to identify Information Governance components and measurement factors that may form part of a larger framework. In particular, Information Security could be considered a component with confidentiality, integrity, and availability of Information as its measurement factors. Beyond Information Security, just from the above practice, we also see Information Architecture<sup>1</sup>, privacy, and Integrated Thinking (through the mention of intellectual capital). Thus, in my discussion on vignettes drawn from my case study, I shall examine how the presence and maturity (or lack thereof) of King IV’s recommended practices for Technology and Information Governance may have influenced the institutional outcomes identified within the vignettes. Similarly, in my concluding chapter, I shall also test my recommendations and proposed framework against the recommended practices. At a minimum, my recommendations and proposed framework must speak to all of the recommended practices under the Technology and Information Governance principle and, where appropriate, the overlaps between the Risk Governance and Compliance Governance principles and recommended practices.

## **The <IR> Framework**

I cannot consider King IV as part of my theoretical framework without discussing Integrated Thinking, Integrated Reporting, and the capitals view of an organisation (as discussed previously in Chapter 3). Consider the following recommended practice (Institute of Directors South Africa, 2016:62):

“The governing body should exercise ongoing oversight of Technology and Information management and, in particular, oversee that it results in the following:

- a. Integration of people, technologies, Information, and processes across the organisation...”

---

<sup>1</sup> “An Information Architecture is a high-level map of the Information requirements of an organisation. It is a personnel-, organisation-, and technology-independent profile of the major Information categories used within an enterprise. The profile shows how the Information categories relate to business processes and how the information categories must be interconnected to facilitate support for decision-makers” (Brancheau & Wetherbe, 1986:453).

From the above practice, we can see how King IV continually highlights the interrelated nature of the model capitals. In this example, we can easily infer reference to human (“people”), manufactured (“technologies”), and intellectual (“Information” and “processes”) capitals. For a more practical example, consider the below statement from the Payment Card Industry Data Security Council (PCI Security Standards, 2014:1):

“One of the biggest risks to an organisation’s Information Security is often not a weakness in the technology control environment. Rather it is the action or inaction by employees and other personnel that can lead to security incidents—for example, through disclosure of Information that could be used in a social engineering attack, not reporting observed unusual activity, accessing sensitive Information unrelated to the user’s role without following the proper procedures, and so on. It is therefore vital that organisations have a security awareness program in place to ensure employees are aware of the importance of protecting sensitive Information, what they should do to handle Information securely, and the risks of mishandling Information. Employees’ understanding of the organisational and personal consequences of mishandling sensitive Information is crucial to an organisation’s success.”

From the above, we can easily argue that a successful Information Security programme requires an integrated approach: technology, such as properly configured firewalls, needs to be in place (manufactured capital); employees need to be trained and made aware of Information Security related risks and good practices to mitigate those risks (human capital) even though training programmes are not without costs (financial capital). An Information Security breach may result in: financial loss through direct theft or administrative fines (financial capital); the loss of confidential Information such as trade secrets (intellectual capital); and/or reputational damage through the improper handling of the disclosure of the breach (social and relationship capital). On the more positive side, however, training and awareness initiatives and Information- or Cybersecurity research may improve or enhance both an organisation’s human and intellectual capital. Displaying a good level of legislative compliance and adherence to good Information Security practices may even have a positive effect on how government regulators and the general public view an organisation.

To extend this example to South African higher education, an institute’s Information Security training and awareness programme must also extend to the student body as many students may have heightened access rights, sometimes the equivalent of or greater than the access rights granted to some employees: class representatives, tutors, teaching or research assistants, and Student Representative Council members. Even students without such heightened access may expose the institution to risk through, for example, personal devices allowed to connect to the institution’s network (especially if the institution’s stance on Bring Your Own Device is unclear or immature). However, such student training and

awareness programmes could take on any number of forms, each influencing the institution's capitals differently, ranging from simple poster campaigns, blended learning courses, bug bounty initiatives, a module within an academic programme, through to bleeding edge Information- and Cybersecurity vulnerability research projects.

From the above, it is clear that an institution needs to approach Technology and Information Governance in a holistic and integrated manner. The capitals view provides an arguably intuitive approach to do so. However, the model capitals are just that: models. As mentioned in Chapter 3, King and the <IR> Framework expects each institution to define and refine their own list of applicable capitals from the broad-in-scope model capitals. Given the scope and timing of this study however, it is difficult (if not implausible and even undesirable) for one to define the capitals for University X<sup>2</sup>. Still, to guide the analysis and position in my concluding recommendations, we need some additional theoretical lens that aligns (explicitly or implicitly, knowingly or unknowingly) with the guiding principles of the <IR> Framework, but enables a more subject-relevant view of Technology and Information Governance. This is where we turn to COBIT 5.

## COBIT 5

As discussed in the previous chapter, COBIT 5 focuses on “systemic governance and management through interconnected enablers” (ISACA, 2012a:27). Through its various supplements, COBIT 5 delves deeply into each of these enablers that, when considered with the <IR> Framework in mind, provides not a proxy for an organisation's capitals, but rather a subject-relevant translation with which we can more easily assess Technology and Information Governance-related initiatives, components, and measurement factors.

Continuing the discussion from the previous chapter, COBIT 5 further expands on the concept of interconnected enablers through the introduction of a set of common dimensions shared by all enablers, which ISACA (2012a:28) believes would:

- “[Provide] a common, simple, and structured way to deal with enablers;
- [Allow] an entity to manage complex interactions; and
- [Facilitate] successful outcomes of the enablers.”

The four common dimensions for enablers are (ISACA, 2012a:28-29):

---

<sup>2</sup> Cloete (2018), proposed adopting 4 capitals for Stellenbosch University, arguing that the institution should consistently consider them in decision-making: Students, Staff, Finance, and Facilities.

1. **Stakeholders**—those “who play an active role and/or have an interest in the enabler”;
2. **Goals**—“each enabler has a number of goals, and enablers provide value by the achievement of these goals” in terms of the “expected outcomes of the enabler [and/or] the application or operation of the enabler itself”; goals can be further sub-categorised by:
  - **Intrinsic quality**—“the extent to which enablers work accurately, objectively, and provide accurate, objective, and reputable results”;
  - **Contextual quality**—“the extent to which enablers and their outcomes are fit for purpose given the context in which they operate”;
  - **Access and security**—“the extent to which enablers and their outcomes are accessible and secured”;
3. **Life cycle**—“each enabler has a life cycle, from inception through an operational/useful life until disposal”; and
4. **Good practices**—“for each of the enablers, good practices can be defined. Good practices support the achievement of the enabler goals. Good practices provide examples of suggestions on how best to implement the enabler, and what work products or inputs and outputs are required.”

On a related note, COBIT 5 also discusses enabler performance management as “enterprises expect positive outcomes from the application and use of enablers” (ISACA, 2012a:29). To manage enabler performance, COBIT 5 (ISACA, 2012a:29) suggests that “the following questions will have to be monitored and thereby subsequently answers—based on metrics—on a regular basis:

1. Are stakeholder needs addressed?
2. Are enabler goals achieved?
3. Is the enabler life cycle managed?
4. Are good practices applied?

COBIT, however, is not without its criticisms. Though the various iterations of the King Code are similarly not without their criticisms, the Reporting Regulations do still position the Code within the South African higher education sector’s legislative universe. COBIT, on the other hand, does not have the same legislative weight behind it<sup>3</sup>. Thus, given my position within ISACA (as considered previously in the discussion on researcher reflexivity in Chapter 1), this section briefly highlights some of the criticisms against COBIT, including the standard’s complicated concepts, structures, and resulting

---

<sup>3</sup> Even so, King III (2009:16) does explicitly reference COBIT (and most likely COBIT 4.1 given the publication date of King III).

complexity; its generic nature and limited practical implementation guidance; and limited evidence of proven benefits (Zhang & Fever, 2013; Bartens, De Haes, Lamoen, Schulte and Voss, 2015). In contrast, for example, King IV provides a selection of sector specific supplements “to make it more easily applicable to all organisations: public and private, large and small, for-profit and not-for-profit” (Institute of Directors South Africa, 2016:10).

Despite these criticisms, through referencing COBIT 5’s enabler dimensions and performance management during my analysis of the vignettes drawn from University X as presented in the following chapters, I was able to determine, for example, to what extent the enablers were considered as an interconnected whole, to what extent enabler goals were met (or even if there were any defined goals), and to what extent did a underperforming or non-existent enabler affect the others. However, as suggested within the list of enablers itself, one can expect a lot of variety between organisations (such as the culture, ethics, and behaviour enabler). To better understand the institution under review, so as to better ensure the relevance of my analysis, I also considered my primary case’s vision, mission, and values statements as part of the theoretical framework, as discussed later in this chapter.

### **The Three Lines of Defence**

As positioned by the Institute of Internal Auditors, the Three Lines of Defence serves as model to assist with the effective and efficient co-ordination of various risk and control functions (such as internal auditors, Enterprise Risk Management initiatives, compliance officers, and fraud investigators) to ensure that there are “neither gaps in controls nor unnecessary duplication of coverage” (The Institute of Internal Auditors, 2013:1). The Institute of Internal Auditors (2013:1-2) argues further that:

“Although Risk Management frameworks can effectively identify the types of risks that modern businesses must control, these frameworks are largely silent about how specific duties should be assigned and coordinated with the organisation.

Fortunately, best practices are emerging that can help organisations delegate and co-ordinate essential Risk Management duties with a systematic approach. The Three Lines of Defence model provides a simple and effective way to enhance communications on Risk Management and control by clarifying essential roles and duties.”

Though COBIT 5’s 2012 supplement, *Enabling Processes*, presents a recommended RACI chart for each of the processes discussed therein, many of the positions and functions listed in the RACI were not present within University X at the time of writing. As any recommendation that I make must also consider the realities of the South African higher education sector, including financial constraints, it cannot simply

recommend that the institution should create and fill new positions to match COBIT's model RACI chart and expect that the appointees would then be able to resolve all Technology and Information Governance matters.

Coupled with the legislated mandatory institutional governance structures required at each South African public higher education institution, the Three Lines of Defence provides an additional means of understanding the institution and formulating practical and realistic recommendations.

To briefly summarise, the Three Lines of Defence are:

- **Functions that own and manage risks:** “As the first line of defence, operational managers own and manage risks. They also are responsible for implementing corrective actions to address process and control deficiencies. Operational management is responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis. Operational management identifies, assesses, controls, and mitigates risks, guiding the development and implementation of internal policies and procedures and ensuring that activities are consistent with goals and objectives” (The Institute of Internal Auditors, 2013:3).
- **Functions that oversee risk:** “Management establishes various risk management and compliance functions to help build and/or monitor the first line of defence controls... Management establishes these functions to ensure the first line of defence is properly designed, in place, and operating as intended. Each of these functions has some degree of independence from the first line of defence, but they are by nature management functions. As management functions, they may intervene directly in modifying and developing the internal control and risk systems” (The Institute of Internal Auditors, 2013:4). These functions may include Risk Management, compliance, or controllership functions.
- **Functions that provide independent assurance:** “Internal auditors provide the governing body and senior management with comprehensive assurance based on the highest level of independence and objectivity within the organisation. This high level of independence is not available in the second line of defence. Internal audit provides assurance on the effectiveness of governance, Risk Management, and internal controls, including the manner in which the first and second lines of defence achieve Risk Management and control objectives” (The Institute of Internal Auditors, 2013:5).

Additionally, the Institute of Internal Auditors (2013:2) argues that before the lines of defence, an organisation's governing board and executive management (as primary stakeholders of the lines) are best

“positioned to help ensure that the Three Lines of Defence model is reflected in the organisation’s Risk Management and control processes. Finally, external stakeholders, such as external auditors and government or sector regulators also have a role to play. For example, the South African Information Regulator, through the POPIA regulations, may set and formally define minimum control standards for the processing of Personal Information.

Interestingly, Luburic, Perovic, and Sekulovic (2015) argue that the first line of defence can be further strengthened by merging risk owner responsibilities and business process owner responsibilities into one individual or team. Luburic, Perovic, and Sekulovic (2015:246), using the ISO 9004 standard as a basis, define process owner as the individual or team “with defined responsibilities and authorities to establish, maintain, control and improve the process and its interaction with other processes.” This view provides another element to consider when examining membership of the mandatory institutional governance structures required at each South African public higher education institution and the “such other structures and offices as may be determined by the institutional statute” (Republic of South Africa, 1997:22).

However, since the 2013 release of the positioning paper *The Three Lines of [Defence] in Effective Risk Management and Control* (The Institute of Internal Auditors, 2013), contributors to the professional literature have argued that blurred or blended lines of defence model can result in irrelevant, inefficient and inadequate co-ordination of assurance efforts (PricewaterhouseCoopers South Africa, 2014:3). If the lines between the second and third lines blur (i.e. those that monitor risks and controls blurring with internal audit), “the safety net for senior management and the board becomes less effective and may not enable the board to fully discharge its governance oversight responsibility” (PricewaterhouseCoopers South Africa, 2014:13). King IV thus refines and builds upon the King III principles and practices for combined assurance by introducing a five level Combined Assurance Model (Deloitte Africa, 2016:6)<sup>4</sup>. Moving from a position of defence to one of assurance is significant, allowing organisations to consider good risks, value, and opportunities too. Though King IV does not specifically prescribe a recommended structure, it does identify the organisational units that may be best suited to fill the lines:

1. Functions that provide independent assurance;
2. Functions that oversee risk;

---

<sup>4</sup> Some readers may know of the Five Lines of Assurance. In the response to the public commentary on the draft version of King IV, the King Committee argued: “The use of the Five Lines of Assurance has been discarded in favour of listing what assurance services and functions may include. It is then left to the determination of the governing body and audit committee on how these should be combined to accomplish the objectives of the combined assurance model” (Institute of Directors South Africa, 2016a:23).

3. Functions that own and manage risks;
4. Specialist functions; and
5. The governing body.

This model allows for a matrix of assurance providers across the organisation, with both horizontal and vertical relationships (Deloitte Africa, 2016:20). Of particular interest, the inclusion of the traditional Three Lines and specialist units may provide both an interesting challenge and opportunity for South African higher education institutions. As I delve into examples drawn from University X, I shall unpack my understanding of specialist units further, their interaction with the traditional Three Lines.

## **Institutional values**

As mentioned in my introductory chapter, a public higher education institution may find a means to legally trade in Personal Information. Yet, even if such trade might be legal, the institution's people (staff, students, study applicants, alumni, donors, vendors, and research participants) might find the idea unpalatable (especially if the trade involves their own Personal Information). However, what if the profits from the trade of student Personal Information, for example, was not simply absorbed into an institution's general budget, but instead went to programmes that provide direct benefits to students? Would the institution's people then be amenable to trading Personal Information? Similarly, learning and learner analytics (another form of study applicant and student Personal Information processing) may enable an institution to make better-informed decisions concerning study acceptance criteria, class sizes, the overall size and shape of the institution, or even enable the institution to identify individual students at risk of dropping out.

With the above in mind, we can quickly see that institutional values (or the institution's culture, ethics, and behaviours if referring to COBIT 5's enablers) may influence the positioning of Information Governance-related initiatives and programmes within the institution. As such, I have taken the institutional vision, mission, and value statements (of the institution under review) as the final element of my theoretical framework in my analysis and final recommendations. Below, I have briefly summarised the institution's vision, mission, and values statements (as directly quoting them would enable readers to easily identify the institution in question). At the time of writing, based on my interpretation, the institutions then-vision, mission, and values included or focused on:

- Inclusivity, transformation, social justice, and sustainability;
- Excellence, innovation, and creativity;

- Empathy, servant-leadership, and accountability;
- Student-centricity;
- Future-orientation; and
- Making a positive impact, globally and locally.

Building upon these, University X's institutional transformation plan positions three themes for organising transformation goals, namely:

- Place;
- Programmes; and
- People.

Successfully bridging the Personal Information gap will, undoubtedly, rely on some measure of change management. By considering the transformation plan, which at its heart focuses on institutional change, I can make more practical recommendations for University X. More specifically:

- Place considers both the institution's physical spaces and foundational institutional culture, which relates to COBIT's culture, ethics, and behaviour enabler; and
- Programmes (which considers both core academic programmes and other related competencies such as transformation, innovation, and communication) and People (which considers institutional stakeholders and the ease in which they can participate in the institution's governance structures) relates to COBIT's people, skills, and competencies enablers.

Further, to support its discussions on transformation, University X also refers to Bergquist's (1992:4-6) *The Four Cultures of the Academy*. These, summarised below, in the context of Place, Programmes, and People, help contextualise the final recommendations in the last chapter:

- **The collegial culture:** “a culture that finds meaning primarily in the disciplines represented by the faculty in the institution; that values faculty research and scholarship and the quasi-political governance processes of the faculty; that holds untested assumptions about the dominance of rationality in the institution; and that conceives of the institution's enterprise as the generation, interpretation, and dissemination of knowledge and as the development of specific values and qualities of character among young men and women who are future leaders of our society.”
- **The managerial culture:** “a culture that finds meaning primarily in the organisation, implementation, and evaluation of work that is directed toward specified goals and purposes; that values fiscal responsibility and effective supervisory skills; that holds untested assumptions about

the capacity of the institution to define and measure its goals and objectives clearly; and that conceives of the institution's enterprise as the inculcation of specific knowledge, skills, and attitudes in students so that they might become successful and responsible citizens.”

- **The developmental culture:** “a culture that finds meaning primarily in the creation of [programmes] and activities furthering the personal and professional growth of all members of the collegiate community; that values personal openness and service to others, as well as systematic institutional research and curricular planning; that holds untested assumptions about the inherent desire of all men and women to attain their own personal maturation, while helping others in the institution become more mature; and that conceives of the institution's enterprise as the encouragement of potential for cognitive, affective, and behavioural maturation among all students, faculty, administrators, and staff.”
- **The negotiating culture:** “a culture that finds meaning primarily in the establishment of equitable and egalitarian policies and procedures for the distribution of resources and benefits in the institution; that values confrontation and fair bargaining among constituencies (primarily management and faculty or staff) with vested interests that are inherently in opposition; that holds untested assumptions about the ultimate role of power and frequent need for outside mediation in a viable collegiate institution; and that conceives of the institution's enterprise as either the undesirable promulgation of existing (and often repressive) social attitudes and structures or the establishment of new and more liberating social attitudes and structures.”

## **Institutional understanding of governance and management**

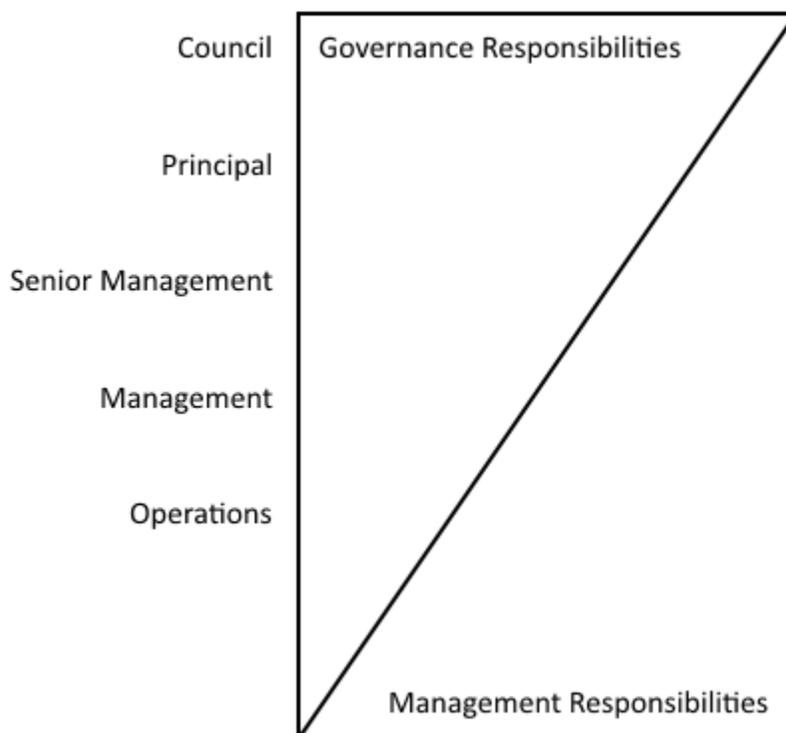
During 2017, University X, pushed by changes in its legislative universe, established a task team under the institution's Principal<sup>5</sup> and his management team to:

- establish the foundation for an ontology of Information Governance related terminology to promote a shared understanding across the institution;
- identify, interpret, and contextualise the institution's Information Governance requirements, risks and opportunities;
- disseminate this contextualisation to the Principal's management team; and
- make prioritised recommendations to address the identified risks and seize the identified opportunities.

---

<sup>5</sup> See Appendix C for a discussion on the mandatory institutional governance structures.

I have considered the task team's findings and recommendations in my own recommendations at the end of this thesis. However, as part of the task team's deliverables, the task team positioned a spectrum view of governance and management (not unlike my argument for a D-I-K spectrum) as illustrated in the figure below:



*Figure 2 Governance and Management Spectrum*

This graphic (not to scale) depicts a mix of governance- and management-related responsibilities. As one moves upwards through the institutional hierarchy (y axis), the mix of responsibilities leans towards a governance focus, but without completely abandoning management responsibilities. The Principal, for example, has both governance- and management-related responsibilities, but with a stronger management focus than Council and a stronger governance focus than the institution's senior management.

## **Conclusion**

In this chapter, the sources that informed the analysis were defined:

- King IV, which positions the minimum requirements necessary within a Technology and Information Governance framework;

- The <IR> Framework, which expands on the King's Integrated Reporting and Integrated Thinking requirements;
- COBIT 5, which presents a more subject-relevant set of 'capitals' (i.e. enablers) and dimensions to consider in the analysis on the implementation thereof;
- The institutional vision, mission, and values of the institution which serves as my unit of analysis, which provides additional necessary context for my analysis and resulting recommendations; and
- The institutional understanding of governance and management responsibilities.

## Chapter Five: Privacy

In Chapter 1, under the discussion about the role of the researcher in this study, I provided some of my personal background, including my work as a privacy professional. Within that capacity, I often (sometimes jokingly) argue that privacy-related legislative compliance simply requires an organisation to do other things, which it should be doing anyway, in a well-coordinated and mature manner. This chapter, plans to test the strength of the argument. Based on my experiences, there is no single solution to ensure privacy-related legislative compliance; it is not something that an organisation's IT, Legal, or Compliance department can address on their own. Rather it requires a co-ordinated effort, involving multiple disciplines and stakeholders from across the organisation. With this in mind, I argue that through examining efforts at privacy-related legislative compliance, we can begin working towards answering the first research question: *what are the essential components, of an Information Governance programme, required to adequately enable a privacy legislative compliance initiative?*

There is some evidence in the literature which supports this approach. The Economist Intelligence Unit (2018), for example, surveyed over 300 business executives, drawn from across the globe about the disruptive nature of compliance and regulatory requirements—"the interplay of regulatory trends and strategic priorities." Though most of the respondents positioned that the scope and pace of regulatory change hindered "the ability of business organisations to achieve their strategic objectives," the respondents also positioned that "the work towards staying in compliance is not an unmitigated loss... [instead] the benefits for many businesses are substantial" (The Economist Intelligence Unit, 2018:10). As it pertains to privacy, 99% of respondents indicated that they had at least started to develop a response to comply with the GDPR, with 25% of respondents stating that they had "entirely changed strategy or operations specifically in response to [the] GDPR" and another 25% stating that they had "entirely changed a strategic or financial goal to comply with [the GDPR]" (The Economist Intelligence Unit, 2018:8). Yet, the survey also revealed that efforts to comply with the GDPR triggered opportunities to improve business process efficiency, Information and Cyber Security programmes, and privacy-related training and awareness programmes. Interestingly, stepping back from topic of privacy, the Economist Intelligence Unit (2018:10) also argued:

“... as compliance deadlines loomed, businesses would begin searching for efficiencies that better prepared them for further change and reduced the cost burden of additional compliance. The improved quality and collection of an organisation's data, regardless

of industry or product and service, became a clear solution for both meeting and proving compliance.

This put a spotlight on Information Governance.”

All of the respondents cited at least one compliance-driven improvement to their organisational approach to Information Governance, with benefits including improved security, improved efficiency, reduced risk exposure, increased customer satisfaction, improved brand image, improved agility, and improved increased internal collaboration (Economist Intelligence Unit (2018:11).

In this chapter then, I first establish the scope of privacy legislative compliance through an examination of the applicable South African legislation. Thereafter, I discuss several vignettes drawn from University X’s initiatives to address its privacy requirements. Through this, we would be able to identify the Information Governance and Management sub-disciplines required to, at least in the context of University X, approach privacy-related legislative compliance. Through this we can take our first steps towards defining and describing a framework which a South African public higher education institution could ultimately use to develop its unique approach towards privacy legislation compliance.

## **What does the legislation say?**

The constitutional right to privacy is enshrined in the South African Bill of Rights, Constitution of the Republic of South Africa, 1996 (Republic of South Africa, 1996). As a starting point then, let us look at how POPIA (Republic of South Africa, 2013) defines Personal Information:

“... [Personal Information is] Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person<sup>6</sup>, including, but not limited to—

- a) Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- b) Information relating to the education or the medical, financial, criminal or employment history of the person;
- c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- d) the biometric information of the person;
- e) the personal opinions, views or preferences of the person;

---

<sup>6</sup> Law and Martin (2009:308) define a juristic person as “an entity, such as a corporation, that is recognised as having legal personality i.e. it is capable of enjoying and being subject to legal rights and duties.”

- f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- g) the views or opinions of another individual about the person; and
- h) the name of the person if it appears with other Personal Information relating to the person or if the disclosure of the name itself would reveal Information about the person.”

Additionally, section 26 of POPIA (Republic of South Africa, 2013) establishes a prohibition on the processing of Special Personal Information, which includes:

- a) “the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
- b) the criminal behaviour of a data subject to the extent that such information relates to—
  - i. the alleged commission by a data subject of any offence; or
  - ii. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.”

POPIA then further establishes the conditions for the lawful processing of Personal Information. To briefly summarise in plainer language, the conditions cover:

- **Accountability:** where accountability and responsibility for compliance with POPIA lies within an organisation;
- **Processing limitation:** limitations on the processing of Personal Information in terms of how, why, when, where, and from whom it is collected;
- **Purpose specification:** the purposes for collecting Personal Information—POPIA positions that Personal Information can only be collected for specific purposes;
- **Further processing limitation:** limitations on the further processing of Personal Information (i.e. beyond the specific purpose for which it was originally collected);
- **Information quality:** requirements to maintain quality (i.e. accurate) Personal Information;
- **Openness:** requirements to document all Personal Information processing and notify data subject of any processing in a transparent manner;
- **Security safeguards:** requirements to maintain the integrity and confidentiality of Personal Information (including any third party processing); and
- **Data subject participation:** providing mechanisms that allow data subjects to access their Personal Information (and request corrections or deletion of the Information).

I shall use these conditions to structure my examination of our vignettes throughout the remainder of this chapter. Before I do though, to properly establish the reach of this legislation within an organisation, we should also examine how the Act defines processing:

“...processing means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including—

- a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
- b) dissemination by means of transmission, distribution or making available in any other form; or
- c) merging, linking as well as restriction, degradation, erasure or destruction of Information.”

Considering the above, we can already establish a sense of the scope of POPIA. Before digging further though, it is worth briefly discussing one element of the GDPR. Though not explicitly mentioned in POPIA, the GDPR does also position the principles of privacy-by-design and privacy-by-default (see Recital 78 of the GDPR (2016)):

“In order to be able to demonstrate compliance with [the GDPR], the controller<sup>7</sup> should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of Personal Data, pseudonymising Personal Data as soon as possible, transparency with regard to the functions and processing of Personal Data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of Personal Data or process Personal Data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors<sup>8</sup> are able to fulfil their data protection obligations.”

Recital 78 aligns closely with the POPIA sections quoted above. Though most of my discussion in the remainder of this chapter focuses on POPIA, we cannot ignore the GDPR, especially considering that University X often engages with European-based partner institutions, donors, and students. Further, the

---

<sup>7</sup> Article 4 of the GDPR establishes that controller “means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law” (i.e. a controller, for our discussion, is similar to POPIA’s responsible party).

<sup>8</sup> Article 4 of the GDPR establishes that processor “means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller” (i.e. a processor, for our discussion, is similar to POPIA’s operator),

GDPR also introduces the Data Protection Officer<sup>9</sup> (“DPO”) role and position that, pending the POPIA regulations, may help us understand and to a certain extent predict the role requirements of POPIA’s articulation of Information Officers. As we delve further into this chapter, I shall often refer to other sections of both POPIA and the GDPR.

## Personal Information Life Cycle

By my reading, if we look back at POPIA’s understanding of processing, combined with our understanding of privacy- and secure-by-design principles, the legislation suggests or establishes a phased life cycle for Personal Information:

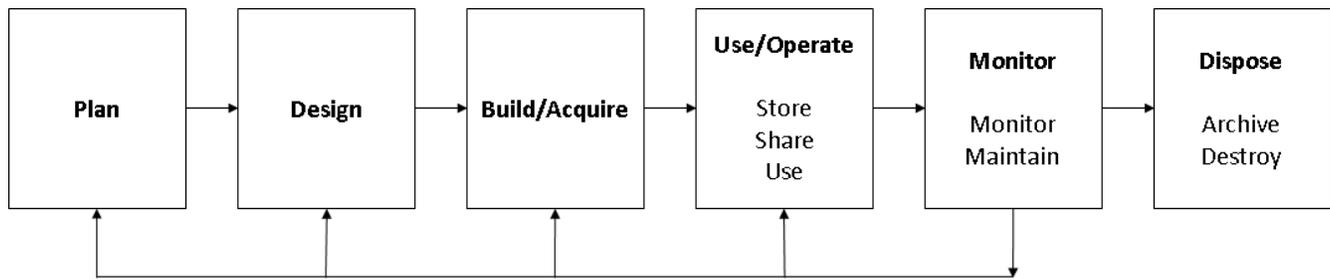
Phase	Activities (as defined in POPIA)
Preliminary	Activities that take place before actual processing of personal information, including Data Protection Impact Assessments <sup>10</sup> .
Collection and Creation	Collection, receipt, recording of personal information.
Utilisation	Organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use, dissemination, merging, linking, restriction, degradation of personal information.
Disposal	Erasure or destruction of personal information.

*Table 2 Personal Information Life Cycle*

While the above provides an interesting starting point, there is also merit in examining other life cycle models. For example, COBIT 5’s *Enabling Information* presents a more generic and process oriented view as visualised below (ISACA, 2013:33).

<sup>9</sup> “Under the GDPR, it is mandatory for certain controllers and processors to designate a DPO. This will be the case for all public authorities and bodies (irrespective of what data they process), and for other organisations that - as a core activity - monitor individuals systematically and on a large scale, or that process special categories of Personal Data on a large scale... [The] DPO is a cornerstone of accountability and that appointing a DPO can facilitate compliance and furthermore, become a competitive advantage for businesses. In addition to facilitating compliance through the implementation of accountability tools (such as facilitating or carrying out Data Protection Impact Assessments and audits), DPOs act as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation)” (Article 29 Data Protection Working Party, 2016:4).

<sup>10</sup> Data Protection Impact Assessments are a GDPR requirement (see Recital 84 of the GDPR (2016)). Specifically, an organisation should conduct such assessments when “[Personal Information] processing operations are likely to result in a high risk to the rights and freedoms of natural persons... to evaluate, in particular, the origin, nature, particularity and severity of [those risks]. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of [Personal Information] complies with [the GDPR].”



*Figure 3 COBIT 5 Information Life Cycle*

However, in earlier supplements, COBIT 5 (ISACA, 2012a:81) presents an Information life cycle wherein:

1. business processes (supported by IT processes) generate and process Information;
2. the organisation through further processing thereafter transforms Information<sup>11</sup>;
3. the organisation creates value, through the processing and transformation of Information, from Information; and
4. the creation of value drives or informs business processes and so the cycle repeats.

I am particularly fond of the COBIT model as it explicitly positions value creation. I would argue that we could strengthen the model drawn from POPIA by considering value creation in at least the Preliminary and Utilisation phases.

## Life Cycle in Practice

From a privacy perspective, using the life cycle view, we should consider a process at the point in which new Personal Information is captured (i.e. at the Collection and Creation phase of the above cycle). Quite often, organisations collect such Information through forms. At University X, we can see study (prospective student) application forms, bursary application forms, residence application forms, and work study programme application forms, to name but a few. Some of these forms ask for the applicant's national ID number and, if you recall our discussion in Chapter 2, such ID numbers actually say a lot more than be apparent at first glance.

If you were following POPIA's condition of processing limitation (specifically that of minimality<sup>12</sup>) an organisation should not over collect Personal Information. If an organisation collects South African

<sup>11</sup> COBIT explicitly refers to transforming Data into Information and thereafter Information into Knowledge; I instead still prefer my spectrum view of Information as discussed in Chapter 2.

<sup>12</sup> Section 10 of POPIA states that "Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant, and **not excessive**." Emphasis mine.

national ID numbers, then it should not need to collect date of birth or gender as separate fields, as this Information can be derived from the ID number. By reducing the number of questions/fields on a form, one can reduce the overall length and complexity of the form (which may ultimately lead to more individuals being able to complete the form and complete it accurately).

However, as also mentioned in Chapter 2, international students do not necessarily have South African national ID numbers. In such cases, an institution may need a separate form for international prospective students or, if using an electronic form, make sure that the form is dynamic enough to ask international prospective students for date of birth and gender, but not ask South African prospective students for such Information beyond requesting their ID numbers. To complicate matters though, we also have to consider institutional values. University X recognises a non-binary understanding of gender. As such, the underlying master data structures of the institution allow students to capture non-binary as their gender<sup>13</sup>. Thus, to enable this, University X's applications forms must still ask for gender.

The discussion about application forms should highlight the importance of carving out time to properly consider what Personal Information you want to collect and why. It is not only about security and impact assessments. In University X's example, the institutional values played a key role in this decision—historically, statutory reporting requirements did not ask for non-binary statistics, but still the institution chose to position the option on its application form. To complicate matters even further, such a change to the forms also has several downstream implications. As an example, consider if a student applies to study and selects male on the application form. During the student's second year of study, the student asks to change<sup>14</sup> their registered gender to non-binary. If the institution allows the change, does the change only have an impact going forward or must the change apply retroactively, back to the creation of the student's record? How then do these changes affect statutory reporting and any Institutional Research, Academic Analytics, or Learning Analytics initiatives?

---

<sup>13</sup> This, and similar decisions, forms part of the institution's transformation plan (see Chapter 4), particularly under the theme of Place. Take for example, renewing universal access to amenities such as bathrooms. Gender expression provides but one example; race, another. For example, the South African Higher Education Management Information System (HEMIS) only considers African, Coloured, Indian, and White, and a No Information option. I do not identify as any of those groups and, when faced with such a form, would provide garbage information. Well, I was born in Africa, so I must be African then. University X has, however, made the following options available to its staff and students: Asian, Black African, Coloured, Indian, White, Prefer not to Say, No Information, in line with its own institutional values and policies, while still providing a workable baseline for statutory reporting.

<sup>14</sup> Sections 23, 24, and 25 of POPIA discuss the condition of data subject participation, which positions that responsible parties must provide mechanisms that allow data subjects to access to their personal information; to change or correct their personal information; and to have their personal information deleted.

## Institutional Research and Academic & Learning Analytics

As discussed in the opening chapters, Corporate Governance has shifted from a focus on short-term thinking to long-term thinking in response to the need to create value in a sustainable manner (Institute of Directors South Africa, 2016:4). Value creation, according to the <IR> Framework, is defined as “the process that results in increases, decreases, or transformations of the capitals caused by an organisation’s business activities and outputs... Governance refers to how the organisation is directed by the governing body in exercising ethical and effective leadership. Hence, the governing body’s role in value creation is to lead the organisation ethically and effectively so as to support the value creation process in the short, medium and long term” (Integrated Reporting Committee of South Africa, 2017:3). One could argue that Information Governance then should require the governing body to lead the organisation ethically and effectively so as to support value creation with a particular focus on enhancing and sustaining the organisation’s intellectual capital. King IV (2016:62) does support this stance by, for example, recommended practice 13(f)<sup>15</sup>:

“The governing body should exercise ongoing oversight of Technology and Information Management and, in particular, oversee that it results in...[the] assessment of value delivered to the organisation through significant investments in technology and Information...”

Institutional Research and Academic & Learning Analytics are a sampling of Information Governance and Management sub-disciplines that could enable a higher education institution to derive (additional) value from its Information (i.e. intellectual capital) and/or inform investments into or management of the institution’s other capitals (from an Integrated Thinking perspective) or enablers (from a COBIT 5 perspective). Further, these sub-disciplines, by their very nature often require the processing of Personal Information. Through examining how University X positions these sub-disciplines, and reflecting on my involvement with national bodies that consider these sub-disciplines, we can tackle one more of POPIA’s conditions for the lawful processing of Personal Information, namely: further processing limitations (i.e. the processing of Personal Information for a purpose other than the purpose under which the Personal Information was originally collected). Before delving into the specifics of further processing, let us define our three sub-disciplines. Firstly, Botha, Muller, and Webber, (2016:1-2) define Institutional Research as:

“...research aimed at the understanding of universities as institutions... [it is] usually understood as applied and actionable research aimed at decision-makers in higher

---

<sup>15</sup> See Appendix A for the full listing of King IV recommended practices under Technology and Information Governance.

education institutions and at policy-makers in regional and national higher education systems. The purpose of [Institutional Research] is primarily to inform institutional planning, policy development, and decision making. The application, management, and analysis of institutional Information remains a key concern of [Institutional Research] practitioners...”

Academic Analytics and Learning Analytics are thus subsets of Institutional Research. Lemmens and Henn (2016:231) first define these sub-disciplines by both the goals/purpose behind them:

“Several South African higher education institutions have started appropriate critically the notion of “Data-driven decisions”, in the hope of using the insights from analytics to reduce potential risks. For higher education institutions, these risks are predominantly linked to student academic success. There are multiple risk factors that may cause a student to drop out or to fail, such as the absence of adequate financial and emotional support. National governing agencies, now more than ever, focus on using the data reported by higher education institutions to inform decisions on funding, academic programmes and other interventions... [Analytics] serves as an entry point towards a better understanding of the student body. The use of advanced Data Analytics gives institutions more Information about their students that ever before. With Data Analytics, institutions are able to develop metrics for the calculation of retention rates, success rates, graduation rates, throughput rates, staff-student ratios and a whole range of other indicators providing more knowledge about their institution”

Lemmens and Hen (2016:232-233) then, building upon the work of Campell, DeBlois and Oblinger (2007), Elias (2011), and Long and Siemens (2011), define Academic Analytics and Learning Analytics as:

“... Academic Analytics consists of an analysis of data by means of statistical and predictive modelling techniques in an effort to identify performance indicators. Academic Analytics is conducted with the aim of improving organisational processes, workflows, resource allocation, and institutional measurement through the use of learner, academic, and institutional Data... The metrics derived from Academic Analytics provide institutions with the input and output metrics at an institutional level, but say very little about the learning process and how it relates to the characteristics of the learner in the learning process.”

“... Academic Analytics consists of an analysis of data by means of statistical and predictive modelling techniques in an effort to identify performance indicators. Academic Analytics is conducted with the aim of improving organisational processes, workflows, resource allocation, and institutional measurement through the use of learner, academic, and institutional Data... The metrics derived from Academic Analytics provide institutions with the input and output metrics at an institutional level, but say very little about the learning process and how it relates to the characteristics of the learner in the learning process.”

“... [Learning analytics is] analytics at the level of the individual student and their learning [and can be defined as] the measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimising

learning and the environments in which it occurs. Learning analytics are largely concerned with improving learner success... In recent years, Learning Analytics has emerged as a specific focus area in Institutional Research and has evolved as a critical entry point on student Data in an effort to gain better insight into the student learning experience. What makes Learning Analytics unique is the fact that it harnesses real time Data about student performance and analyses the Data in a short return time in order to enable institutions to provide custom-made interventions for individual students before it is too late for them to benefit from such interventions.”

I have only briefly touched on the Academic & Learning Analytics conversation above (to delve deeper would be worthy of a separate study). From the above, we can see the interplay between these sub-disciplines and privacy. To make it more concrete, let us consider examples drawn from University X.

For Academic Analytics, University X maintains the pass rates of academic modules and programmes by year. Through Academic Analytics, University X may be able to analyse and consider the entry requirements for any particular module or programme (i.e. the minimum grade a potential student should achieve on her or his National Senior Certificate (or equivalent)) and monitor the impact of any changes. For example, by increasing the entry requirements and thereby admitting only academically stronger students<sup>16</sup> for a particular module, University X may see an improved pass rate for that module at the module or programme level (i.e. not necessarily at the level of a specific student).

For Learning Analytics, at the time of writing, University X had just entered the requirements gatherings phase of a multi-year project that aims to build upon existent, stand-alone student support and wellness programmes, ultimately delivering a mature, integrated Learning Analytics programme. In designing the programme, the analysts need to delve into the existing programmes and systems, planning for future programmes and systems, and the student Information available institutionally through core institutional systems, within individual support or wellness programmes, within individual smaller systems, and even other programmes at the periphery, such as sporting clubs and student societies. During the investigation, the analysts encountered several privacy-related concerns and questions, some inherent to the concept of Learning Analytics and some specific to the context of University X, that may eventually dictate the final scope, extent, and implementation of the Learning Analytics programme. The analysts had planned to take an iterative approach, which allowed them to, upon the discovery of a privacy-related concern return to areas of the institution already covered. I believe that this caution is well warranted as one does not

---

<sup>16</sup> Within the context of South Africa and goals related to transformation and redress, University X does not only consider academic performance when deciding to accept a particular student into a course of study. The other pieces of Information which inform such decisions may, of course, plug directly into University X's Learning Analytics initiatives and resulting interventions.

have to look far to find examples of organisations suffering reputational harm as a result of a Data Analytics faux pas<sup>17</sup>. And that sits at the heart of our conversation of Learning Analytics at University X. It is not only about what is (a) possible with the given technology and available Information and (b) what is legal, it is also about institutional values, culture, and context, and (for lack of a better phrase) the tolerable creepiness factor. The discussion below expands on this further.

University X offers health services to its students, including but not limited to first aiders at sporting events, general medical practitioner services, and psychological and counselling services. Some of these services are offered free of charge to students, while other services allow for claims against medical aid schemes or for cash payments (especially when students do not wish to expose their health information to the medical aid primary account holder<sup>18</sup>). Currently, University X utilises two, isolated implementations of specialised Health Information Systems—one implementation for the mental health services, and the other for the general practitioner and first aid services (i.e. there is no integration with these systems and other systems, nor between the two Health Information Systems). This is, of course, a prudent stance given the positioning of Health Information as Special Personal Information<sup>19</sup> under POPIA. However, imagine how, knowing about physical injury or the mental health of students might contribute to a Learning Analytics programme (an athlete experiences a concussion on the sports field on the weekend before a major academic examination) or an Academic Analytics programme (the percentage of students diagnosed with depression).

University X is currently asking if they should consider integrating Health Information Systems with its proposed Learning Analytics initiative. Would the University, as Target did, find merit in identifying or

---

<sup>17</sup> Consider, for example, the anecdote about Target outing a teenager's pregnancy through their customer Data Analytics (Duhigg, 2012; Hill, 2012). Though the authenticity and accuracy of this anecdote has been questioned (see, for example, (Harford (2014))), it remains a cautionary tale that is not always heeded. Consider, for example, that the UK Information Commissioner's Officer recently fined Emma's Diary, a "Data broking company, which provides advice on pregnancy and childcare, sold the information to Experian Marketing Services, a branch of the credit reference agency, specifically for use by the Labour Party. Experian then created a database which the party used to profile the new mums in the run up to the 2017 General Election." See <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/08/emma-s-diary-fined-140-000-for-selling-personal-information-for-political-campaigning/>.

<sup>18</sup> Many students with access to medical aid fall under their parent or guardian's medical aid account. Any claim sent to the medical aid includes a code which indicates at least the procedure (i.e. not necessarily a diagnosis) the student-patient underwent or plans to undergo. This allows the medical aid administrators to evaluate any claim against plan, available medical savings, and so forth, before approving or refusing the claim. The medical aid primary account holder can then of course, should they wish, identify the procedure by the code on the medical aid invoice or statement. This may of course lead to the embarrassment of the student.

<sup>19</sup> Consider the very recent breach of SingHealth, Singapore's largest group of healthcare facilities (The Straits Times, 2018a, 2018b). The attackers, allegedly, were primarily after the Health Information of Prime Minister Lee Hsien Loong (imagine the damage that could be done by revealing that the minister was, for example, gravely ill or was tackling a condition with strong negative stigma attached). However, in the process, the attackers also stole the Personal Information of 1.5 million other patients, including strong and unique personal identifiers and related Personal Information that could be used in all manner of malicious attacks.

predicting pregnancy amongst its student body? While such questions would certainly test the institutions values and ethical stance on privacy, it also leads to a host of far more practical questions. For example, if the University did intend to integrate the Health Information Systems with the greater Learning Analytics initiative:

- Would the University need to ask for student-patient consent before linking their Health Information to the greater Learning Analytics initiative?

In the next section (Funder access to student Information, below), I delve into the problems with collecting and managing consent. For the purpose of this discussion, it is worth pointing out that one does not necessarily need to obtain consent before one can process Personal Information lawfully under POPIA (see Section 11 in particular). Consider, for example, that you were applying for a new job. When doing so, the potential employer asks you for your consent to run a background check. What would happen if you refused to give your consent? Would the employer still consider you for the position? Probably not. This is an example of consent that is not really voluntary as it does not allow a genuine choice for you as job-seeker; you have to consent if you want to be considered for the position. Instead the employer should instead simply establish a privacy notice (see Section 18 of POPIA) detailing, in a clear and transparent manner, why they are collecting your Personal Information (i.e. to evaluate your qualifications and work experience against the position requirements) and what they will do with it (e.g. verify the accuracy/authenticity of the Information using a background verification service). In positioning a privacy notice, the potential employer thus does not have to take on the burden of managing consent (though they would still take on the responsibility of protecting any collected Personal Information as the remainder of POPIA still applies).

If maintaining consent for participation in Academic & Learning Analytics is impractical or unfeasible in the Health Services context, if the University were to still pursue this opportunity, it would then need to establish a privacy notice instead. However, if the University were to follow the privacy notice route (i.e. by utilising our health services, your Information will be used as part of our Academic & Learning Analytics), would potential student-patients still be comfortable using the University's health services? That I cannot answer at this stage—the University would need to engage with its people to understand their appetite for such monitoring, translate that understanding into the appropriate privacy policy, and only thereafter re-look at considering Health Information in its Academic & Learning Analytics.

- How would the University govern, manage, and operationalise access controls to student-patient Health Information when integrating Health Information Systems to the greater Learning Analytics initiative?

Currently, the Health Information Systems are isolated from other institutional applications. This contains access control risks, as only a handful of identified health practitioners, supporting administrative staff, and support IT staff need and have access to the system. Even among them, access is restricted by role (i.e. supporting administrative staff do not need and thus do not have access to patient diagnostic details at a system level<sup>20</sup>). If the University were to integrate the Health Information Systems with other applications, it becomes far more difficult to manage access, ranging from determining who should have access (i.e. what Information will be used as part of the Analytics and who will have access to that Information to run the Analytics). As more and more individuals gain access to certain Information, it becomes more and more difficult to protect that Information. Consider, for example, the Payment Card Industry Security Standards Council's (PCI Security Standards Council, 2014:1-2) position on the matter:

“One of the biggest risks to an organisation's Information Security is often not a weakness in the technology control environment. Rather it is the action or inaction by employees and other personnel that can lead to security incidents—for example, through disclosure of Information that could be used in a social engineering attack, not reporting observed unusual activity, accessing sensitive Information unrelated to the user's role without following the proper procedures, and so on. It is therefore vital that organisations have a security awareness program in place to ensure employees are aware of the importance of protecting sensitive Information, what they should do to handle Information securely, and the risks of mishandling Information. Employees' understanding of the organisational and personal consequences of mishandling sensitive Information is crucial to an organisation's success. Examples of potential consequences may include penalties levied against the organisation, reputational harm to the organization and employees, and impact to an employee's job. It is important to put potential organisational harm into perspective for personnel, detailing how such damage to the organization can affect their own roles.”

In the South African context, POPIA Sections 107, 108, and 109 explicitly list the penalties for an offense in terms of the Act, which includes imprisonment for up to 10 years, administrative fines of up to R10 million, or both. Section 99 further establishes civil remedies, such as civil action for damages, available to data subjects. I hold that training and awareness initiatives are crucial to the success of any privacy initiative. Integrating Health Information with a greater Academic & Learning Analytics programme

---

<sup>20</sup> Of course, this does not account for password sharing between different users. I discuss this element of privacy, i.e. individual behaviour, at the end of this chapter.

provides but one (more extreme) example of the need for training and awareness initiatives. Even if the University did not integrate its Health Information Systems with other applications, the current users of those Health Information Systems would themselves still require sensitising to the risks and legislative requirements surrounding Health Information.

- How would the University reconcile the technological differences between the Health Information Systems and the rest of its estate?

Now we return to our earlier conversation about the impact of allowing students and staff to identify as non-binary. Firstly, the University has maintained its two implementations of its Health Information System separately from its other systems, with no guarantee that the individual implementations stored Data in the same way (or in the same way as other institutional systems). Thus, it is wholly possible that, from a technical perspective, any integration might require significant cost and effort to realise. To complicate matters, section 16(1) of POPIA, in discussing the condition of Information quality, states that “a responsible party must take reasonably practicable steps to ensure that the Personal Information is complete, accurate, not misleading, and updated where necessary.” However, at the time of writing, University X could not, for example, identify which system would hold the most recent and accurate Information about a particular student or staff member? Would it be the Student Information System, Human Resources Information System, or the Health Information System? What happens if one of these systems allows non-binary expressions of gender and the others do not? When viewed from the context of a Personal Information life cycle, should University X have several discrete life cycles by system or institutional area? I do not necessarily have the answers to these questions. However, these questions do highlight another aspect of privacy legislative compliance that we need to consider further in our discussion.

## **Funder access to student Information**

During my time as a higher education institution’s Deputy Information Officer and during my time on the USAf POPIA sector code of conduct task team (see Chapter 1), I was and am frequently asked: “What should I [as lecturer, residence head, client services consultant, Registrar, or even as (Deputy) Vice-Chancellor] do when a parent calls and asks for Information about their child?” For example, parents may call to ask about a student’s academic performance. At first glance, this looks like a fairly simple and straightforward question to answer. Especially since, historically at University X, such Information was freely given. However, if one does just a bit of digging, we quickly uncover that this seemingly simplistic question sparks several other questions and considerations. For instance, we would need to

consider if the student in question is legally considered a child or an adult. Specifically, POPIA section 1 defines:

- a child as “a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself”; and
- a competent person as “any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child”.

The Children’s Act (38 of 2005) section 18(3)(b) establishes that “a parent or other person who acts as guardian of a child must... assist or represent the child in administrative, contractual and other legal matters.” Further, Sections 34 and 35 of POPIA establish under which conditions a responsible party can process Personal Information of children (for example, with the consent of a competent person). With these conditions and definitions in mind, in plainer language, in practice, this would allow a parent access to the Information of a child student. However, this parental access falls away when the student turns 18.

In this section, I intend to show how an institution’s stance on Information Governance and Management may influence its approach to dealing with funder requests for student Information. Or, conversely, how an institution’s approach to dealing with funder requests for student Information may influence its stance on Information Governance and Management. For the purpose of this discussion, a funder is anybody that pays a (portion of a) student’s study fees. Potential funders could thus be parents, guardians, siblings, grandparents, aunts or uncles, private donors, private organisations, bursary programmes, and even the National Student Financial Aid Scheme (“NSFAS”).

For the 2018 application cycle University X, expected potential students to sign a contract at the time of formal application to study at the institution. This contract set out the institution, the applicant, and (if applicable) the applicant’s guardian’s rights and responsibilities within the application procedure. While the standard contract template allowed a guardian to provide consent for the agreement between a child applicant and the institution<sup>21</sup>, the contract also explicitly stated that guardians had no right to a student’s information (i.e. that University X will not share an adult or child student’s Information with the student’s parents). Instead University X has positioned the following:

- proactively pushes selected de-identified, aggregated student Information to the public;

---

<sup>21</sup> Interestingly, the template also allowed guardians to agree to serve as surety and co-principal debtor for any debts of the applicant (though with no guarantee that the applicant would ever be accepted for study by or would ever formally register as a student at University X).

- provides self-service functionality that allows students and alumni to access their Personal Information on demand;
- has pre-existing agreements with third party qualification verification services that process requests, on behalf of the institution, to verify an individual's claim of holding a qualification from University X;
- directs third party requestors to engage directly with the student(s) or alumni in question (if possible<sup>22</sup>); or
- if none of the above mechanisms prove suitable, directs third party requestors to submit a formal request under PAIA which includes the mechanisms for reaching out to students and alumni for their consent.

This stance, alone, raises some interesting questions. For example, POPIA Section 11 discusses when Personal Information may be processed. Section 11(1)(f), establishes that “Personal Information may only be processed if... processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.” One could argue that a funder has a legitimate financial interest in a student's academic performance as that may determine the funder's willingness to continue funding the student's studies. Even so, students that are adult children may, for any number of personal reasons, still not want a paying parent to access their student Information (such as ongoing divorce proceedings, estrangement for whatever reason, and so forth).

Is University X's choice to simply rely on a blanket 'no' for any third party request to identified student Information the best choice though? In answering, we should consider what University X might require to enable a different approach that is not already covered by PAIA. PAIA has the mechanism for collecting consent from data subjects per request (i.e. the students in this extended example) and verifying any requestors' identity. However, PAIA can be slow (it allows organisations up to 30 days to respond to a request under the Act) and may in itself not be the most user-friendly (if one considers the design and nature of the prescribed request forms and the rules baked into the Act that govern when an institution can, cannot, or may not release any or all requested Information—an ill-phrased request may result in an organisation refusing the request). But, as mentioned above, University X already makes use of PAIA as essentially the last option for Information-seekers (barring warrants and subpoenas).

---

<sup>22</sup> University X does not, or at least should not as per the contract with students, share contact details of students or alumni with third parties; thus third party requestors that do not have a student's contact details, must instead make use of the institution's PAIA request process.

If we start from the position that University X will not simply share student Information with anybody, but also does not want to push requestors towards its PAIA processes, realistically then University X would have to maintain a white list, by student, of individuals with pre-approved access to a student's Information (i.e. a record of a student's consent permitting a specific individual access to that student's University-held Information). Consent is, however, problematic as, once you begin collecting consent, you then need to maintain it. A student should be able to, at any time, alter their white list. University X would then need to establish the technology to a) collect and maintain consent and b) provide accurate and up-to-date records to those who handle the requests for student Information. Coupled with this consent engine, those handling the requests would also need mechanisms to verify the identity of any requestor.

Within my institution, I have witnessed cases when a student loses control of their university account through, for example, a phishing attack. Those compromised accounts are then used to launch further phishing or spam activities. Using a compromised e-mail account to spam others is just one example of what might go wrong if sensitive Information falls into the hands of a malicious actor. Identity theft, fraud, doxxing<sup>23</sup>, and revenge porn<sup>24</sup> are just a small sampling of possible attacks. This highlights the importance of verifying requestors, but does not explain how one would identify and establish the mechanisms—should funders get their own user accounts and access to University X's self-service functionality; should University X's call centres invest in voice-based biometric identification systems? If University X was to do this, it would immediately increase its POPIA-related risks simply because it would need to process far more Personal Information (i.e. the additional Personal Information of funders) than it already does.

To summarise, University X would need to implement several technological, procedural, and policy changes to enable funder access to student Information, while establishing a minimum level of access control over that Information. In the context of the sector's funding crunch, this sort of investment may simply not be financially viable. I would thus argue that the only reasonable stance (pending the POPIA regulations and sector code of conduct) would be to apply a blanket no, to not act as an intermediary between adult children and their parents, and to rely on PAIA for those few instances when the parent and adult child cannot reach an agreement between themselves.

---

<sup>23</sup> "To publicly identify or publish private information about (someone) especially as a form of punishment or revenge" (Merriam-Webster, 2018a).

<sup>24</sup> Posting sexually explicit images of a person "online without that person's consent especially as a form of revenge or harassment" (Merriam-Webster, 2018b).

This section, has shown that both the institution's stance on Personal Information has influenced its technological and operational procedural investments and that the institution's stance on Information Governance and Management (even if it was just a question about financial viability) has influenced its approach to Personal Information. In other words:

- University X will not share student Information with funders by default because it does not have the mechanisms to still meet its institutional privacy goals and enable this sharing lawfully according to POPIA; and
- University X will not invest in the mechanisms to enable sharing of student Information with funders by default because such mechanisms would expose the institution to additional POPIA-related risks (if only from an increase in the volume of Personal Information to protect) and are otherwise not seen as strategic or value-driving investments.

Before I close this section, within University X, I discovered that potential donors and external bursary fund managers often request identified student Information directly from the institution. These donors use this Information to identify needy and/or deserving students that they would like to approach in order to offer bursaries. These donors further explicitly request identified, rather than de-identified or aggregate, Information for a number of reasons ranging from establishing a personal connection with potential beneficiaries or requiring access to more qualitative Information as part of their decision-making processes. To complicate matters, these donors often require the Information almost immediately after they make the request for Information as these offers are often positioned with multiple institutions simultaneously and beneficiaries are considered on a first-come-first-serve basis.

Thus, those University staff members tasked with managing the relationship with these donors are faced with a conundrum: either slow down the process to first seek out student consent or, to some extent, ignore elements of POPIA's conditions of lawful processing to give students the best chance of securing the funding. There is no easy answer here, but I believe that higher education institutions (taking their institutional values into account<sup>25</sup>) should take the opportunity to lead, to educate, and sensitise donors to the constitutional right to privacy and privacy-related legislation. I understand that this may not be an easy path to walk, but if we can't expect our Universities to do so, then who should?

---

<sup>25</sup> And thereby their stance on privacy. For example, refer to my earlier discussion in Chapters 1 and 4 on the trade of Personal Information, the lawfulness of such trade, and the interplay with institutional culture and values.

## Conclusion

In this chapter, I discussed elements of privacy-related legislation as it pertains to the South African higher education sector. I further unpacked examples, drawn from University X, to highlight how upcoming and existent privacy-related legislation may impact upon or disrupt Personal Information processing within the institution. Though my examples may have tended towards the more burdensome elements of compliance, we cannot forget the potential benefits.

In particular, I stressed the importance of privacy and privacy-related (i.e. security) training. Humans can both strengthen an institution's security (especially in areas where technology cannot (yet)<sup>26</sup>) and weaken an institution's security (through their behaviour (e.g. clean desks or lack thereof) and vulnerability to social engineering). As mentioned earlier in the chapter, attacks are directed at both staff and students. Institutions may benefit, at least from a security and operational perspective, by training both staff and students. Such student-focused training could in itself be seen as a differentiator, better preparing students for work in industries which deal with high volumes and/or high value Information, Personal or otherwise, such as the Health, Finance, and even Retail industries (think of the loyalty cards that may be in your wallet at this moment).

In addition to the importance of training, I also set out to establish if a privacy programme could inform an institution's overall Information Governance and/or Management framework. In the examples drawn from University X (in this chapter, in the footnotes, and throughout this thesis) I specifically highlighted the interplay between privacy and the following Information Governance sub-disciplines: Academic & Learning Analytics (which also implies Big Data, Predictive Analytics, and from our earlier discussion, Identity and Access Management, Architecture (Enterprise, Information, etc.), Continuity and Disaster Recovery, Information- and/or Cyber Security, Data- and/or Information Classification, and Risk Management (including Third Party Risk Management). At the heart of it though, privacy-legislative compliance forces an institution to relook at its Information processing. Consider again the discussion on Academic & Learning Analytics at University X. Privacy informed the discussion regarding the integration of Health Information Systems with the greater Analytics initiative. These earlier discussions highlight how privacy compliance may shape institutional processes or, more specifically, the Information life cycle within these processes.

---

<sup>26</sup> Such as reducing the inherent risks or value of Information through minimising what Information is collected in, for example, a research project (i.e. research surveys that do not collect any personal identifiers). This forms part of a researcher's research methodology which is, at least to date, still requires humans to actively consider and plan out.

At the start of this chapter, I set out to test the strength of my argument that privacy-related legislative compliance simply requires an organisation to do other things, which it should be doing anyway, in a co-ordinated and mature manner. Through my examination of vignettes drawn from University X, I have demonstrated that, for example, a proper definition of roles and responsibilities (i.e. Identity and Access Management) is a core consideration in the institution's Academic & Learning Analytics implementation. One could expand this further, arguing that University X also requires the proper classification of Information (i.e. a Data and/or Information Classification framework) to define Health Information and the staff responsibilities attached to access to such Information, which in turn will inform the Identity and Access Management requirements.

In Chapter 1, in positioning my research questions, I aimed to identify the essential components, of an Information Governance programme, required to adequately enable a privacy legislative compliance initiative within a South African public higher education institution. However, in delving into the specifics of University X and through my work on the USAf national task team, I discovered that this is easier said than done, given the uniqueness of each institution. Consider, institutions that may or may not recognise non-binary understanding of gender within their master data structures, but statutory reporting requirements only require reporting on percentages of female and male staff and students. Here, institutional values even go so far as to affect how University X reports to the Department of Higher Education and Training (which may in turn influence the institution's funding).

Instead, I discovered that privacy legislative compliance instead presents a tool or mechanism through which an institution could identify its particular Information Governance and Management framework requirements. Privacy compliance forces institution's to ask questions about their business processes (and document and maintain evidence of any resulting decisions to both satisfy potential audits and Information Regulator investigations, and give effect to POPIA's condition of openness and transparency). As many privacy initiatives across the South African higher education sector are, at the time of writing, in their infancy, the institutions are well-positioned to relook at their Information Governance and Management policies and frameworks, using privacy as the impetus, within the context of the (again, at the time of writing) forthcoming sector POPIA code of conduct and national POPIA regulations. That said, the professional literature does make recommendations of a starting point or the minimum requirements for enabling privacy compliance. I explore these recommendations in the next chapter.

## Chapter Six: Recommendations

Within the discussion on the vignettes presented in the previous chapters, within the context of privacy, I have highlighted when:

- The lack of and/or immaturity of Information Governance-related sub-disciplines within the institution exposed the institution, its people, or its partners to unnecessary risk and/or actual harm (such as immaturity in the procurement processes to identify the risks involved in Internet of Things procurements);
- The presence of and/or maturity of Information Governance-related sub-disciplines within the institution prevented or mitigated unnecessary risk and/or actual harm to the institution, its people, or its partners (such as the institutional Cybersecurity function's consideration of Internet of Things technology) ; and
- The presence of and/or maturity of Information Governance-related sub-disciplines within the institution delivered or could deliver additional value to the institution, its people, or its partners (such as Academic & Learning Analytics).

With these discussions in mind, coupled with my theoretical framework, we can tackle my research questions. In particular, when answering my first research question (*What are the essential components, of an Information Governance programme, required to adequately enable a privacy legislative compliance initiative?*):

- Using King IV as a starting point (see Appendix A), we can identify the components that would serve as the basis for an Information Governance framework; and
- Using the <IR> Framework and COBIT 5, we can identify additional required and recommended components and measurement factors.

In particular, COBIT 5 (ISACA, 2013:70) presents an illustrative set of enablers for privacy compliance. For example, COBIT 5 positions the following privacy-relevant policies under the principles, policies, and frameworks enabler: Records Management, Information Security, Data Governance and/or Data Management (see Appendix B for further examples). Though we can refer to these frameworks to establish a recommended minimum standard, institutional values can have a drastic effect on the institutional view or understanding of Information Governance and Management. As such, it may be impossible to recommend a sector-specific Information Governance framework that adds more value

than the existing professional standards and frameworks. Rather, documents such as the draft POPIA sector code of conduct which plans to clarify the application of POPIA within higher education sector may be more appropriate.

That said, using the institutional values and analysis of vignettes drawn from University X, we can argue that an institution can use its privacy-related initiatives as a starting point to review and prioritise individual Information Governance framework components and identify additional required and recommended measurement factors. This of course would then require the proper positioning of privacy within the institution. For example, placing privacy within an existing institutional silo may flavour privacy programmes (a privacy officer in IT may put a stronger focus on the technological requirements, whereas a privacy officer in Legal may put a stronger focus on compliance). Further, placement within a silo may limit the privacy officer to that silo or subject domain.

But what about my other research questions:

2. What is the difference between Information Governance and Information Management (as it pertains to the South African public higher education sector)?
3. Do Information Governance accountabilities and responsibilities adequately address the statutory institutional governance structures required by the Higher Education Act?

To address these questions, we should consider what is next for University X. In their book, De Stadler and Esselaar (2015:92-94) present “practical strategies for becoming and remaining [POPIA] compliant” across two broad phases, Phase 1: Getting Started and Phase 2: Sustained Compliance. By plotting where University X lies within these phases, we can discuss the institution’s short- to medium-term approach to POPIA compliance. Briefly, the phases entail:

### **Getting started:**

1. What questions should responsible parties be asking (a checklist):
  - a. “What Personal Information do we have?
  - b. What do we use it for? Do we really need the Personal Information?
  - c. Do the data subjects know what Personal Information we have and understand what we use it for?
  - d. Do we have a clear and comprehensive privacy policy?
  - e. Can we de-identify the Personal Information?
  - f. Are we satisfied that the Personal Information is held securely whether records are on paper or online?
  - g. Do only the people who need access have access to the Personal Information?

- h. Is the Personal Information accurate and up to date?
  - i. Do we delete or destroy the Personal Information when we no longer need it?
  - j. Who is the Information Officer currently? Who will it be? Does someone have to be hired?
  - k. Do we keep a record of the processing activities?"
2. Planning a POPIA project:
- a. Conduct an initial risk assessment to determine the size and scope of Personal Information processing activities at a high level;
  - b. Conduct a detailed risk assessment, to investigate “specific instances of non-compliance” and identify “other risks and inefficiencies in the business” (i.e. consider not only compliance, but also risk and value too);
  - c. Develop solutions;
  - d. Implement solutions; and
  - e. Establish an audit and/or compliance function to ensure continued sustained compliance.

### **Sustained compliance:**

1. Appoint a competent Information Officer;
2. Develop effective and efficient privacy-related audit and monitoring processes;
3. Capture the protection of Personal Information within employee job descriptions and key performance indicators;
4. Establish Information Governance structures to ensure that privacy features on the business’ agenda and strategies;
5. Develop a tool “with which the privacy impact of new projects can be measured”; and
6. Conduct regular training and awareness initiatives.

At the time of writing, University X completed several high-level and detailed risk assessments, and now focuses on developing and implementing solutions and establishing the supporting Information Governance structures. In particular, University X is looking to develop a privacy policy, establish an institution-wide Incident Management programme (which considers Information breaches and leaks as a type of incident), an Information Classification framework, and supporting governance structures through subcommittees of the mandatory institutional governance structures (see Appendix C).

If we look back at De Stadler and Esselaar’s (2015) checklist of questions, we can argue that University X has a (at least partial) view and understanding of the Personal Information processed within the institution (questions *a*, *b*, and *c*) through their risk assessments (COBIT’s governance process of

evaluation). If we were to follow the questions, question *d* positions the privacy policy. I would argue that University X focus their short-term attention here, as such a document would set the scene (COBIT's governance process of direction) for several other initiatives (COBIT's governance process for monitoring and management processes of plan, build, run, and monitoring).

### **The privacy policy—a recommendation**

Based on my understanding of the University X context, and review of the literature, I would recommend that University X consider a policy based on:

- a principle-based approach, to accommodate and clarify the varying understandings of Information within the institution;
- the King IV stance of 'apply and explain' (learning from failings in the 'comply or else' rules-based approach to Corporate Governance);
- both POPIA and international legislation;
- a life cycle view of Personal Information;
- a process view, with a strong focus on the responsibilities of process owners; and
- with a strong focus on the institution's Principal's accountability (as statutory Information Officer).

With the above in mind, the privacy policy should, through clarifying foundational principles that give effect to the right to privacy, establish and enable an institutional framework for the processing of Personal Information that positions respect for data subjects, transparency, accountability, and auditability at its core.

### **The privacy policy—principles**

POPIA is an example of a principles-based piece of legislation "that is designed to be applied intelligently to many unique situations, rather than to provide a fixed set of rules that must be applied universally" (De Stadler and Esselaar, 2015:1). From this position, we can argue that there is merit in clarifying those principles for a particular organisation and, in our case, in the context of University X. Though, of course, responsible parties should apply the principles throughout the entire Personal Information life cycle, I believe there is merit in displaying the principles by life cycle phase when the application of (or the articulation of the application of) a principle is most pertinent. Thus, with the phases defined in Chapter 5 (Preliminary, Collection and Creation, Utilisation, and Disposal), I believe that the University should consider the following policy scope and 10 principles. I derived these principles from the literature

reviewed and an understanding of University X's POPIA compliance gaps and initiatives. Table 3 summarises the mapping of these principles to the POPIA conditions for the lawful processing of Personal Information and the COBIT 5 enablers.

## **Policy Scope**

### *Overarching theme: Accountability and responsibilities*

Though one could argue that an organisation should consider accountability and responsibility as an eleventh principle, I instead argue that, in defining the policy scope, purpose, and implementation, one defines the accountability and responsibility structures. Ultimately, the institution's Principal (as statutory Information Officer) should own and be accountable for the existence of, maintenance of, and monitoring of compliance against the policy. Process owners should thereafter be responsible for the implementation of the policy. Thereafter, assurance, audit, and specialist units<sup>27</sup> should be made available to support the implementation of and monitoring of compliance with the policy. Positioning the scope as such, links back to King IV's discussion on combined assurance (see Chapter 4).

This further aligns with the institutional understanding of a governance and management spectrum (see Chapter 4). By placing responsibility with process owners, the institution enables the subject matter experts (i.e. the process owners) to establish more realistic or subject-relevant evaluation, direction, and monitoring processes (i.e. governance processes as defined within COBIT, see Chapter 3), while also allowing these specialists scope to also consider risk and value too (i.e. not just compliance with the policy, even though, admittedly, this recommended policy is heavily weighted towards compliance).

Further, the policy should not be written in such a way that, at the time of promulgation, the bulk of the institution immediately becomes non-compliant with the policy. Instead, the policy should position a moratorium and comply-by date at a reasonable point in the future (aligned with the POPIA regulations, pending their finalisation, if possible). Finally, the policy should apply to all Personal Information

---

<sup>27</sup> Based on COBIT 5's illustrative list and the European Union's Guidelines on Data Protection Officers, and my understanding of University X's context, I would recommend that the institution consider the position and enablement of the following specialist units:

- Compliance Office(r);
- Freedom of Information Office(r);
- Information Security Manager and/or Management System (such as that as discussed in ISO 27000 (The British Standards Institution, 2013).
- Privacy Office(r) (potentially modelled after the GDPR's DPO); and
- Research Integrity Office(r).

processing, including administrative, teaching and learning, and research processes. This includes any third party processing done for or on the behalf of the institution.

## **Preliminary Phase**

### *Principle 1: Privacy by design and by default*

Process owners must give effect to the right to privacy by default within their processes. Process owners must thus consider privacy and the protection of Personal Information during the analysis and design of their processes. Specifically, process owners must, during the design of a new process or review and analysis of an existent process:

- conduct a Privacy Impact Assessment<sup>28</sup> to determine the lawfulness of and to identify and evaluate risks associated with the proposed processing of Personal Information;
- use the outcomes of the assessment to identify and design appropriate and reasonable safeguards and other measures within their processes to mitigate identified risks (which may include halting a process determined as unlawful); and
- document the outcomes of the assessment and how it informed the design of the process.

The Privacy Impact Assessment should also do more than compare a proposed process against legislation. The institution should develop a Privacy Impact Assessment methodology and supporting tools that enables or nudges process owners and assessors towards an Integrated Thinking approach during the assessment. For example, when assessing an existent process, the process owner and assessors should also be able to articulate training requirements for all process stakeholders. The institution should also establish an Information Classification Framework to help process owners identify instances of Personal Information processing and understand the sensitivity or value of the Personal Information involved. Specialist units (e.g. a privacy office or officer) must develop the tools (and supporting training) that would enable process owners to conduct a Privacy Impact Assessment. Specialist units should also make themselves available to assist with the assessment of complex, high risk, and/or high value processing of Personal Information.

### *Principle 2: Secure by design and by default*

Process owners must, in utilising the outcomes of the Privacy Impact Assessment, identify, design, and implement reasonable technical, organisational, and procedural information security and cyber security

---

<sup>28</sup> Note that I do not recommend calling it a Data Protection Impact Assessment. Privacy, rather than Data Protection, allows for a wider spectrum of understandings of Data and Information.

measures within their processes to ensure the confidentiality, integrity, and availability of Personal Information.

### **Collection and Creation Phase**

#### *Principle 3: Minimality*

Process owners must ensure that their processes do not collect more Personal Information than is necessary or relevant to the process.

#### *Principle 4: Accuracy*

Process owners must take reasonable measures to ensure the accuracy and completeness of any collected Personal Information. Where reasonably possible, process owners must ensure that their processes collect Personal Information directly from data subjects.

#### *Principle 5: Notification*

Process owners must take reasonably practicable steps to notify data subjects of any Personal Information processing.

#### *Principle 6: Consent*

Any consent to the processing of personal information, according to POPIA, must be “voluntary, specific, and an informed expression of will in terms of which permission is given for the processing of personal information.” However, consent is not always necessary, practical, or desirable for every potential process.

Process owners must thus determine the need for consent during the design of their process (i.e. as part of the Privacy Impact Assessment). If process owners identify a need to capture consent, such consent processes must align with the provisions of POPIA.

### **Utilisation Phase**

#### *Principle 7: For specific purposes*

Process owners must ensure that any processing of Personal Information must align with the original specified purpose for collecting the Personal Information as specified in the privacy notice or consent procedures (see principles 5 and 6).

Some further processing of Personal Information may be allowable under law when such processing aligns with the original specified purpose for collecting the personal information. Within the context of

the University, such further processing may still be subject to research ethics approval and/or institutional- and gatekeeper permission.

#### *Principle 8: Access*

Process owners must ensure that their processes give effect to all data subject rights. This includes giving data subjects access to mechanisms that allow them:

1. access to their Personal Information;
2. to change or correct their Personal Information; and
3. to have their Personal Information deleted.

#### *Principle 9: Breach notification*

The University must establish procedures to detect, report, investigate, and contain Personal Information breaches. Where reasonably possible, process owners must ensure that their processes align with the institutional Incident Management and breach procedures.

Where process owners cannot reasonably align their processes with the institutional procedures (such as in specific research projects), they must still establish breach procedures aligned with the outcomes of their Privacy Impact Assessment (see principle 1). For research projects, process owners should address this requirement through the research ethics approval and/or institutional- and gatekeeper permission processes (see principle 7).

### **Disposal Phase**

#### *Principle 10: Defensible disposal*

Process owners should not keep Personal Information for longer than is required. POPIA considers the storage and retention of personal information as processing of personal information (see definitions). Long-term storage may also expose the institution, the process owner, and the data subjects to unnecessary risk. Process owners must ensure the proper disposal of a record or Personal Information as soon as reasonably practicable after achieving the purpose for which the information was originally collected (see principle 7) through:

- archiving records with vital or historical value as per the University's Records Management Policy; or
- destruction, deletion, or de-identification of a record or Personal Information as per the University's Records Management Policy.

## The privacy policy—mapping principles

As mentioned above, I map the proposed policy principles to both COBIT 5’s enablers and POPIA’s conditions for the lawful processing of Personal Information. Keen-eyed readers may notice that I have not positioned all 7 of COBIT’s enablers below (most notably missing services, infrastructure, and applications). I simply selected those that are most relevant at the policy level, but that does not exclude the consideration or application of the other enablers at the implementation of the principles.

<b>POPIA Condition</b>	<b>Principle(s)</b>	<b>COBIT Enabler(s)</b>
Accountability	See Policy Scope	Principles, policies, and frameworks
Processing Limitation	1. Privacy by Design and Default 3. Minimality 4. Accuracy 5. Notification 6. Consent	Culture, ethics, and behaviour
Purpose Specification	1. Privacy by Design and Default 3. Minimality 7. For Specific Purposes 10. Defensible Disposal	Organisational Structures
Further Processing Limitation	1. Privacy by Design and Default 7. For Specific Purposes 10. Defensible Disposal	People, skills, and competencies
Information Quality	1. Privacy by Design and Default 4. Accuracy 8. Access	Principles, policies, and frameworks
Openness	1. Privacy by Design and Default 5. Notification	Processes
Security Safeguards	2. Secure by Design and Default 9. Breach Notification	Information
Data Subject Participation	8. Access	Processes

*Table 3 POPIA Conditions to Policy Principles Mapping*

## The privacy policy—Privacy Impact Assessments

As I position the Privacy Impact Assessment as a key element of the first principle, it is worth a closer examination. At the time of writing, University X had develop a spreadsheet-based prototype of a Privacy Impact Assessment. A mapping of the prototype’s requirements against the 10 principles, illustrates both the importance of such as assessment and the overlap between the 10 principles.

<b>The prototype directs assessors and process owners to articulate, for each assessed process:</b>	<b>Principle(s)</b>
all the types of Personal Information (as defined in POPIA) that they plan to process;	3. Minimality
how they intend to collect the Personal Information;	4. Accuracy
from whom they intend to collect the Personal Information (and the geographic location of such data subjects);	4. Accuracy
how they will notify data subjects about the intended purposes for processing the Personal Information;	5. Notification
how they will obtain data subject consent (if necessary);	6. Consent
why they are processing the Personal Information;	7. For Specific Purposes
where and how they will store the Personal Information;	2. Secure by Design and Default
how they will secure the Personal Information;	2. Secure by Design and Default
if and with whom they plan to share the Personal Information (and the geographic location of such third party recipients)	See Policy Scope
if they will provide mechanisms that would allow data subjects to access and update their Personal Information;	8. Access
how long they will store the Personal Information;	7. For Specific Purposes 10. Defensible Disposal
any foreseeable processing of the Personal Information for any other purpose beyond the original purpose; and	7. For Specific Purposes
their acceptance of their responsibility to protect the Personal Information.	See Policy Scope

*Table 4 Privacy Impact Assessment to Policy Principles Mapping*

The first principle (Privacy by Design and Default) applies to the entirety of the assessment (remember, this first principle calls for the assessment). After articulating the above, the prototype suggests an overall risk rating (low, medium, or high) for each assessed item and recommends safeguards and other measures

to address those risks. The rating is not completely automated and a competent assessor may still make or recommend adjustments to the risk ratings or recommended safeguards and other measures. Principle 9 (Breach Notification) is missing from the above, as the assessment focuses on preventative controls; i.e. any breach should trigger the institution's existent breach handling procedures.

The prototype, as described above, pushes assessors and process owners towards considering a host of Information Governance-related sub-disciplines, including Research Data Management, Records Management (as part of Defensible Disposal), Information- and Cybersecurity, (Third Party) Risk Management, and even 'Business' Continuity (consider the question on how and where to store Personal Information) and IT Disaster Recovery. The prototype also, to some extent, functions as a teaching tool through, for example, clarifying or defining types of Personal Information. There is, however, still room for improvement, which provides an opportunity for further research (in addition to those discussed later in this chapter).

### **The privacy policy—potential weaknesses**

Bergquist (1992) (see Chapter 3 and the discussion on Bergquist's *The Four Cultures of the Academy*) extensively discusses the change (or perhaps the difficulties associate with change) within universities. By my reading, the proposed policy above smacks of the managerial culture, which may face heavy resistance within pockets of the university where other cultures may dominate. For example, I explicitly stated that the policy should:

- apply to both research and teaching and learning processes; and
- thereby empowers assurance, audit, and specialist units to 'get involved' with the more academically-focused processes within the University.

Institutional autonomy and academic freedom are unique considerations for universities and some may perceive the proposed policy as a threat to that autonomy and freedom. At University X, we may then see a potential struggle between the culture, ethics, and behaviour enablers and the other six (i.e. in order to pursue their mandate, to what extent must the audit, assurance, or privacy professional operate counter to the expected institutional etiquette?), which we could easily link into a discussion on institutional autonomy and academic freedom:

“At the outset, it is important to identify to whom we are referring when the debate on institutional autonomy and academic freedom is engaged. Who are the alleged violators of academic freedom?”

... But there is a second set of perpetrators of this crime, namely institutional bureaucrats within the walls of the universities. We include Councils in this category, as well as those in administrative hierarchies up to and including Vice-Chancellors. Scholars such as Roger Southall and Julian Cobbing (2005), and André du Toit (2004, 2005), speak of these alleged violators of academic freedom. They refer to the corporatisation of the university, and note how the new managerialism undermines the collegiate governance and atmosphere of the academy” (Habib, Morrow & Bentley, 2006:2).

While, throughout this thesis, I have argued for and recommended that a privacy legislative compliance project can serve as the foundation for an Information Governance framework, the success of such a project relies on addressing institutional autonomy and academic freedom. Consider, to what extent would a privacy impact assessment be (seen as) nothing more than a bureaucratic hurdle rather than a value-adding process? Thus, to borrow from Habib, Morrow and Bentley:

“The recommendation advanced in this report is very different from that which seems to emerge implicitly in the existing literature. In this literature, there is either a hope for some distant institutional revolution to create the macroeconomic fundamentals for a better resourced or even free higher education system; or there is incessant hand-wringing, and continuous complaints about the neo-liberal character of our world. Our recommendation is that institutional autonomy and academic freedom need to be constructed through the contestation of empowered stakeholders, which itself is a product of the messy process of higher education reform and entrepreneurial academic practice” (Habib, Morrow and Bentley, 2006:30).

From a privacy perspective, such conversations (or “contestations”) have just begun within University X. I would not be surprised if these conversations, as suggested by Habib *et al.* above, turn messy. But from that mess, I believe University X may find what is necessary to bridge its Personal Information Governance gap as I discuss further below.

## **Further research opportunities**

Through this study, I have:

- detailed the international and local history of Information Governance as a super-discipline;
- unpacked the more recent legislative requirements for Information Governance and privacy, in particular, at South African public higher education institutions;
- developed and recommended a policy stance driven by a principles-based approach to privacy.

To conclude this thesis, I have identified several opportunities for further research. Firstly, as mentioned throughout this thesis, at the time of writing, the Information Regulator had not yet published the actual regulations under POPIA. Despite my involvement on the USAf task team and the development of a

higher education sector code of conduct for POPIA, I could not account for all possible permutations of and interactions between the final POPIA regulations, the higher education sector code, and any other related sector's code of conduct (if any). Similarly, I could not fully consider the South African Cybercrimes and Cybersecurity Bill given its uncertain progress through the South African Parliament. In addition to legislative changes, the professions further continue to develop and refine standards and frameworks; the Compliance Institute of South Africa, for example, plans to release an updated version of their Generally Accepted Compliance Practice framework and principles in early November 2018 (Compliance Institute of Southern Africa, 2018), which (based on my informal conversations with members of the Institute) may expand upon King IV's discussion on combined assurance. The formal launch of the POPIA regulations and/or the enactment of the Cybercrimes and Cybersecurity Bill, or other related standards and frameworks, would undoubtedly trigger opportunities for further research.

Further, on 24 October 2018, Tim Cook tweeted out Apple's privacy principles (Cook, 2018). They are:

“First, companies should challenge themselves to de-identify customer Data or not collect that Data in the first place.

Second, users should always know what Data is being collected from them and what it's being collected for. This is the only way to empower users to decide what collection is legitimate and what isn't. Anything less is a sham.

Third, companies should recognize that Data belongs to users and we should make it easy for people to get a copy of their Personal Data, as well as correct and delete it.

And fourth, everyone has a right to the security of their Data. Security is at the heart of all data privacy and privacy rights.

Technology is capable of doing great things. But it doesn't want to do great things. It doesn't want anything. That part takes all of us. We are optimistic about technology's awesome potential for good — but we know that it won't happen on its own.”

I find Cook's first principle particularly intriguing. True, a Privacy Impact Assessment could be used to determine if de-identification is plausible and desirable within a process. That said, de-identification by design and default is a far stronger statement than privacy by design and default. It would be interesting to monitor how the world, University X, and, yes, even Apple, considers Cook's statement.

As I briefly mentioned in Chapter 4, the COBIT framework is not without its criticisms—in particular, the limited practical guidance covering the adaptation and implementation of the framework, and limited evidence of proven benefits of following the framework. These criticisms immediately highlight potential paths for future research. For example, Mello and Neto (2016) investigated whether it was possible to, using COBIT 5, develop a governance and management framework for shared services centres in the

public sector. Similarly, Omari, Barnes, and Pitman (2012) conducted a study that attempted to determine if it would be possible to use or adapt a subset of COBIT 5 processes to develop a framework for IT audit in the Australian public sector. Within the context of my study, COBIT-related opportunities include:

- research into the applicability of COBIT within the South African higher education sector;
- research on the actual implementation of COBIT within the South African context or specifically the South African higher education sector; and
- the development of a sector-specific COBIT supplement covering higher education.

To add to the above list, ISACA recently announced the launch of COBIT 2019 (ISACA, 2018). At the time of writing, I do not have a full picture of the differences (if any) between COBIT 5 and the expected 2019 edition. It is worth noting that ISACA argues that COBIT 2019 will offer “more implementation resources, practical guidance and insights”, which, if well executed, will address some of the criticisms made against the standard. At a minimum, I imagine a review of the differences between COBIT 5 and 2019, may further inform University X’s approach to both privacy and, Technology and Information Governance.

On a related note, King IV specifically introduced sector supplements to “broaden the acceptance of Corporate Governance by making it accessible and fit for application across a variety of sectors and organisational types” (Institute of Directors South Africa, 2016:35). More specifically, the supplements “provide high-level guidance and direction on how the King IV Code should be interpreted and applied by a variety of sectors and organisational types” (Institute of Directors South Africa, 2016:75). This provides an interesting contrast when considering the criticisms levelled at COBIT. To date, there are five sector supplements for King IV: municipalities, non-profit organisations, retirement funds, small and medium enterprises, and state-owned entities. Within the context of my study, the development of a sector supplement for higher education (or rather a clarification of the Code for higher education) may be suitable for further research. However, King IV itself warns against the development of too many supplements, because:

- King IV could/should be interpreted and applied in a wide variety of contexts, it would not be possible to cover all of these contexts through supplements; and
- “... an attempt to do so would be contrary to the normative rather than prescriptive approach of King IV” (Institute of Directors South Africa, 2016:75).

That said, USAf did find it worthwhile to explore the development of a higher education sector code for POPIA and one could argue that the DHET 2014 Reporting Regulations serve, at least partially, as a

King III sector supplement. Thus, even though King IV warns against too many supplements, a higher education sector-specific clarification or supplement may still be of value.

Finally, this study only followed University X's journey up to mid-2018. There is undoubtedly merit in further study, following University X into the future and/or deeper investigation across multiple South African higher education institutions. In particular, following the University's transformation journey, as it pertains to Bergquist's *The Four Cultures of the Academy*, may allow a researcher to explore change management within the institution. Bergquist (1992:188), building upon the work of Watson and Johnson (1972), for example, articulates three domains of change: structure, process, and attitude<sup>29</sup>. My proposed privacy policy leans heavily towards process change (as it puts a strong focus on process owner responsibilities). Bergquist (1992:191-193) argues:

“The major strengths of the process domain relate to the empowerment that accompanies skill building... an effort that emphasises alterations in process begins with the assumption that people can change (individually or as a group) and that through training and education people can become more accomplished...[The] early practitioners of this strategy emphasised the need for men and women in organisations to take responsibility for their individual actions by reflecting on their own behaviour, learning new skills, and acquiring new, practical Knowledge. This model of education based on experience empowers men and women. It suggests to them that they need not become victims of oppressive structures or attitudes.

...The major weakness in this approach to organisational change is its emphasis on individualistic solutions to complex, group-centred problems and the ephemeral nature of this seemingly pragmatic approach to training and education. Individual, process-oriented change is usually sabotage by the group. This lesson has been learned many times over in the painful re-entry of men and women into the ‘real’ world who have just experienced an enriching and transforming training [programme]. They return to [an] unsupportive, unforgiving, and misinformed group of colleagues. Because process-oriented change comes about slowly and at considerable cost (in training, education, and time away from work), it is also difficult to sustain, especially when money is tight and dreams of personal transformation seem at best optimistic.”

Given University X's transformation plan and its inextricable ties with privacy, compliance, risk, and value, I quote Bergquist's closing remarks (1992:229-230):

“...we can look forward to working and finding meaning in colleges and universities that embrace all four cultures. One of the best ways that we can begin to prepare for this task and to cope with challenges posed by these new organisational types and

---

<sup>29</sup> Not unlike COBIT's enablers and, as mentioned above, should be considered as part of a Privacy Impact Assessment. Change management will certainly be crucial to establishing a culture (for lack of a better word) of Privacy Impact Assessments and may also be crucial to privacy-related changes to an existent process.

frames is to examine our own institutions in order to appreciate and engage the diverse and often conflicting cultures that reside in them.”

With the ever-evolving Personal Information breaches and leaks, referenced throughout this thesis and reported upon in the media, I would argue that a working understanding of privacy might one day soon be considered a valuable life skill (if not already). As a higher education institution, University X should not be dissuaded from pursuing privacy-driven change, just because process domain-related change is difficult or costly. As previously mentioned, privacy-related training programmes could be seen as an important differentiator—positioning University X as not only bridging the Personal Information gap, but actively building the bridge for and leading others.

# References

- Badia, A. (2014) 'Data, Information, Knowledge: An Information Science Analysis', *Journal of the Association for Information Science and Technology*, 65(6), pp. 1279–1287.
- Barrenechea, M. (2013) *Information Governance is Good Business*. Available at: <https://www.opentext.com/campaigns/ceo-white-paper-series-information-governance-is-good-business/> (Accessed: 6 September 2016).
- Bartens, Y., De Haes, S. Lamoen, Y., Schulte, F. and Voss, S. (2015) 'On the way to a minimum baseline in IT governance: Using expert views for selective implementation of COBIT 5', *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2015–March, pp. 4554–4563.
- Bergquist, W. H. (1992) *The Four Cultures of the Academy*. 1st edn. San Francisco: Jossey-Bass Inc.
- Botha, J., Muller, N. J. and Webber, K. (2016) 'Institutional Research in South African Higher Education: Framing the Contexts and Practices', in Botha, J. and Muller, N. J. (eds) *Institutional Research in South African Higher Education*. 1st edn. Stellenbosch: SUN MeDIA Stellenbosch, pp. 1–22.
- Brancheau, J. C. and Wetherbe, J. C. (1986) 'Information architectures: Methods and practice', *Information Processing and Management*, 22(6), pp. 453–463.
- Bryman, A. (2012) *Social Research Methods*. 4th edn. New York, United States of America: Oxford University Press.
- Buckland, M. (1991) 'Information As Thing', *Journal of the American Society for Information Science*, 42(5), pp. 351–360.
- Burawoy, M. (1998) 'The Extended Case Method', *Sociological Theory*, 16(1), pp. 4–33.
- Caldicott Committee (1997) *Report on the review of patient-identifiable information*, United Kingdom Department of Health.
- Capurro, R. and Hjørland, B. (2003) 'The concept of information', *Annual review of information science and technology*, 37(1), pp. 343–411.
- Cayton, H. (2006) *Information governance in the Department of Health and the NHS*.
- Cloete, I. (2018) *Stellenbosch University: Business Intelligence*.

- Commission on Federal Paperwork (1977) *Report of Commission on Federal Paperwork*. Available at: <https://babel.hathitrust.org/cgi/pt?id=umn.31951d00818930g;view=1up;seq=4> (Accessed: 24 March 2017).
- Compliance Institute of Southern Africa (2018) *Compliance Institute of Southern Africa: Resources*. Available at: <https://www.compliancesa.com/Resources> (Accessed: 1 October 2018).
- Cook, T. (2018) *Apple's Privacy Principles*. Available at: [https://twitter.com/tim\\_cook/status/1055035539915718656](https://twitter.com/tim_cook/status/1055035539915718656) (Accessed: 24 October 2018).
- Cousin, G. (2009) *Researching Learning in Higher Education*. 1st edn. New York, United States of America: Routledge.
- De Stadler, E. and Esselaar, P. (2015) *A Guide to the Protection of Personal Information Act*. 1st edn. Cape Town: Juta and Company Ltd.
- Deloitte Africa (2016) 'King IV Bolder Than Ever'. Available at: [https://www2.deloitte.com/content/dam/Deloitte/za/Documents/governance-risk-compliance/ZA\\_King\\_IV.pdf](https://www2.deloitte.com/content/dam/Deloitte/za/Documents/governance-risk-compliance/ZA_King_IV.pdf). (Accessed: 1 October 2018)
- Dinneen, J. D. and Brauner, C. (2015) 'Practical and philosophical considerations for defining information as well-formed, meaningful data in the information sciences', *Library Trends*, 63(3), pp. 378–400.
- Donaldson, A. and Walker, P. (2004) 'Information governance - A view from the NHS', *International Journal of Medical Informatics*, 73(3), pp. 281–284.
- Duhigg, C. (2012) *How Companies Learn Your Secrets - The New York Times, The New York Times Magazine*. Available at: <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&r=1&hp> (Accessed: 10 August 2018).
- Dyn (2016) *Dyn Statement on 10/21/2016 DDoS Attack | Dyn Blog*. Available at: <https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/> (Accessed: 11 December 2017).
- Gartner (2017) *IT (information technology) - Gartner IT Glossary*. Available at: <https://www.gartner.com/it-glossary/it-information-technology> (Accessed: 11 December 2017).
- Habib, A. (2016) *Op-Ed: The Politics of Spectacle – reflections on the 2016 student protests | Daily Maverick*. Available at: <https://www.dailymaverick.co.za/article/2016-12-05-op-ed-the-politics-of-spectacle-reflections-on-the-2016-student-protests/> (Accessed: 5 July 2017).

Habib, A., Morrow, S. and Bentley, K. (2006) *Academic freedom, institutional autonomy and the corporatised university in contemporary South Africa*. Pretoria, South Africa: The Council of Higher Education.

Hagmann, J. (2013) 'Information governance – beyond the buzz', *Records Management Journal*, 23(3), pp. 228–240.

Hill, K. (2012) *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, *Forbes*. Available at: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#69cab4cd6668> (Accessed: 10 August 2018).

Institute of Directors South Africa (2009) 'King Code of Governance for South Africa 2009', *King Report on Governance for South Africa 2009*, p. 66.

Institute of Directors South Africa (2016a) 'Draft King IV Report: Responses to the summarised public comments'. Available at: [https://cdn.ymaws.com/www.iodsa.co.za/resource/collection/3BCAB4D5-6804-4A8D-A26C-D169F767BE36/King\\_IV\\_Report\\_-\\_Responses\\_to\\_summarised\\_comment.pdf](https://cdn.ymaws.com/www.iodsa.co.za/resource/collection/3BCAB4D5-6804-4A8D-A26C-D169F767BE36/King_IV_Report_-_Responses_to_summarised_comment.pdf). (Accessed: 1 October 2018).

Institute of Directors South Africa (2016b) 'King IV Report on Corporate Governance for South Africa 2016'.

Integrated Reporting Committee of South Africa (2017) 'Disclosure of Governance Information in the Integrated Report an Information'.

ISACA (2012a) *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT*. 1st edn. Rolling Meadows, Illinois: ISACA.

ISACA (2012b) *COBIT 5 Implementation*. 1st edn. Rolling Meadows, Illinois: ISACA.

ISACA (2012c) *Comparing COBIT 4.1 and COBIT 5*. Available at: <https://www.isaca.org/COBIT/Documents/Compare-with-4.1.pdf> (Accessed: 13 March 2017).

ISACA (2013) *COBIT 5 Enabling Information*. 1st edn. Rolling Meadows, Illinois: ISACA.

ISACA (2018) *Get a "Sneak Peek" at the New COBIT 2019*. Available at: <https://www.isaca.org/COBIT/Pages/Get-a-Sneak-Peek-at-the-New-COBIT-2019.aspx> (Accessed: 23 October 2018).

ISACA (no date) *ISACA ® Glossary of Terms*. Available at: <https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf> (Accessed: 11 December 2017).

- IT Governance Institute (2007) *COBIT 4.1*. Rolling Meadows, Illinois: IT Governance Institute.
- Kahn, R. A. and Blair, B. T. (2004) *Information Nation: Seven Keys to Information Management Compliance*. 1st edn. Silver Spring, Maryland, United States of America: AIIM Publications.
- King, M. and Roberts, L. (2013) *Integrate: Doing Business the 21st Century*. 1st edn. Cape Town: Juta and Company Ltd.
- Kooper, M. N., Maes, R. and Lindgreen, E. E. O. R. (2011) ‘On the governance of information: Introducing a new concept of governance to support the management of information’, *International Journal of Information Management.*, 31(3), pp. 195–200.
- Law, J. and Martin, E. A. (2009) *A Dictionary of Law*. 7th edn. Oxford.
- Lemmens, J.-C. and Henn, M. (2016) ‘Learning Analytics: A south African Higher Education Perspective’, in Botha, J. and Muller, N. J. (eds) *Institutional Research in South African Higher Education*. 1st edn. Stellenbosch: SUN MeDIA Stellenbosch, pp. 231–253.
- Logan, D. (2010) *What is Information Governance? And Why is it So Hard? - Debra Logan*. Available at: [http://blogs.gartner.com/debra\\_logan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard/](http://blogs.gartner.com/debra_logan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard/) (Accessed: 4 July 2017).
- Luburic, R., Perovic, M. and Sekulovic, R. (2015) ‘Quality Management in Terms of Strengthening the “ Three Lines Of Defence ” in Risk Management’, *International Journal for Quality Research*, 9(2), pp. 243–250.
- Maylor, H. and Blackmon, K. (2005) *Researching Business and Management*. 1st edn. Hampshire, Great Britain: Palgrave Macmillan.
- Meadow, C. T. and Yuan, W. (1997) ‘Measuring the impact of information: Defining the concepts’, *Information Processing & Management*, 33(6), pp. 697–714. doi: 10.1016/S0306-4573(97)00042-3.
- Mello, E. C. J. and Neto, J. S. (2016) *A Governance and Management Model for the Public Sector Shared Services Center Based on COBIT 5*. Available at: <https://www.isaca.org/COBIT/focus/Pages/a-governance-and-management-model-for-the-public-sector-shared-services-center-based-on-cobit-5.aspx> (Accessed: 1 August 2018).
- Merriam-Webster (2017) *Technology | Definition of Technology by Merriam-Webster*. Available at: <https://www.merriam-webster.com/dictionary/technology> (Accessed: 11 December 2017).
- Merriam-Webster (2018a) *Dox | Definition of Dox by Merriam-Webster*. Available at:

<https://www.merriam-webster.com/dictionary/dox> (Accessed: 4 August 2018).

Merriam-Webster (2018b) *Revenge Porn / Definition of Revenge Porn by Merriam-Webster*. Available at: [https://www.merriam-webster.com/dictionary/revenge porn](https://www.merriam-webster.com/dictionary/revenge%20porn) (Accessed: 4 August 2018).

Nguyen, C. Sargent, J. and Stockdale, R. (2014) 'Towards a unified framework for governance and management of information', *25th Australasian Conference on Information Systems, 8th -10th Dec 2014, Auckland, New Zealand*, p. 13. Available at: [https://aut.researchgateway.ac.nz/bitstream/handle/10292/8024/acis20140\\_submission\\_223.pdf?sequence=1](https://aut.researchgateway.ac.nz/bitstream/handle/10292/8024/acis20140_submission_223.pdf?sequence=1) (Accessed: 4 July 2017)

Nitecki, J. Z. (1985) 'The Concept of Information-Knowledge Continuum: Implications for Librarianship Continuum: of Information-Knowledge for Librarianship Implications', *The Journal of Library History (1974-1987)*, 20(4), pp. 387–407.

Noy, D. (2011) 'Thailand's Sufficiency Economy: Origins and Comparisons with Other Systems of Religious Economics', *Social Compass*, 58(4), pp. 593–610.

Omari, L., Barnes, P. H. and Pitman, G. (2012) 'Optimising COBIT 5 for IT Governance: Examples from the Public Sector', in *2nd International Conference on Applied and Theoretical Information Systems Research*, pp. 2–14. Available at: [https://eprints.qut.edu.au/55561/1/LoaiAlOmari\\_Optimising\\_COBIT\\_5\\_for\\_IT\\_Governance.pdf](https://eprints.qut.edu.au/55561/1/LoaiAlOmari_Optimising_COBIT_5_for_IT_Governance.pdf) (Accessed: 4 August 2018).

PCI Security Standards Council (2014) *Best Practices for Implementing a Security Awareness Program, PCI Data Security Standard (PCI DSS)*. Available at: [https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_V1.0\\_Best\\_Practices\\_for\\_Implementing\\_Security\\_Awareness\\_Program.pdf](https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf). (Accessed: 26 April 2018).

PricewaterhouseCoopers South Africa (2014) 'Covering Your Bases: Implementing Appropriate Levels of Combined Assurance'. Available at: <https://www.pwc.co.za/en/assets/pdf/combined-assurance-brochure-jan-2015.pdf>. (Accessed: 1 October 2018).

Ragan, C. R. (2013) 'Information Governance: It's a Duty and it's Smart Business', *Richmond Journal of Law & Technology*, 19(12), pp. 1–32. Available at: <http://jolt.richmond.edu/v19i4/article12.pdf>. (Accessed: 4 July 2017).

Republic of South Africa (1996) *Constitution of the Republic of South Africa, Government Gazette*.

- Republic of South Africa (1997) *Higher Education Act 101 of 1997, Government Gazette.*
- Republic of South Africa (2005) *Children’s Act 38 of 2005, Government Gazette.*
- Republic of South Africa (2013) *Protection of Personal Information Act 4 of 2013, Government Gazette.*
- Rowley, J. (2007) ‘The wisdom hierarchy: representations of the DIKW hierarchy’, *Journal of Information Science*, 33(2), pp. 163–180.
- Sloan, P. (2014) ‘The Compliance Case for Information Governance’, *Richmond Journal of Law & Technology*, 20(2), pp. 1–46. Available at: <http://jolt.richmond.edu/v20i2/article4.pdf>. (Accessed 4 July 2017).
- Smallwood, R. F. (2014) *Information Governance: Concepts, Strategies, and Best Practices*. 1st edn. Hoboken, New Jersey: John Wiley & Sons, Inc.
- The Economist Intelligence Unit (2018) ‘Compliance and Regulatory Disruption’, pp. 1–16. Available at: [http://www.priorityworldwide.com/services/compliance\\_and\\_education.aspx](http://www.priorityworldwide.com/services/compliance_and_education.aspx). (Accessed: 20 July 2018).
- The European Parliament and The European Council (2016). ‘Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)’, Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN>. (Accessed: 31 October 2016)
- The Institute of Internal Auditors (2013) ‘IIA Position Paper : The Three Lines of Defense in Effective Risk Management and Control’, January, pp. 1–7.
- The International Integrated Reporting Council (2013) *The International Integrated Reporting Framework, The international <IR> framework.*
- The South African Institute of Chartered Accountants (2015) *Integrated thinking: an exploratory survey.*
- The Straits Times (2018a) *Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore’s worst cyber attack, Singapore News & Top Stories - The Straits Times.* Available at: <https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most> (Accessed: 12 August 2018).
- The Straits Times (2018b) *SingHealth cyber attack: Method of attack showed high level of sophistication, Singapore News & Top Stories - The Straits Times.* Available at:

<https://www.straitstimes.com/singapore/method-of-attack-showed-high-level-of-sophistication>  
(Accessed: 12 August 2018).

Tim Harford (2014) *Big data: are we making a big mistake?*, *Financial Times*. Available at: <https://www.ft.com/content/21a6e7d8-b479-11e3-a09a-00144feabdc0> (Accessed: 18 October 2018).

U.S. Department of Homeland Security (2016) 'Strategic Principles for Securing the Internet of Things (IOT) Introduction and Overview', pp. 1–17.

UNISA (2017) *Outcome: National Review of LLB Programmes*. Available at: <http://www.unisa.ac.za/sites/myunisa/default/Announcements/Outcome:-National-Review-of-LLB-Programmes> (Accessed: 5 July 2017).

United Kingdom National Health Service (2008) *Health and social care staff members: what you should know about information governance*.

Western Cape Government (2016) *Decoding your South African ID number | Western Cape Government*. Available at: <https://www.westerncape.gov.za/general-publication/decoding-your-south-african-id-number-0> (Accessed: 12 June 2017).

Wilson, T. (2005) 'Evolution in Information Behavior Modeling Wilson's Model', in Fisher, K., Erdelez, S., and McKechnie, L. (eds) *Theories of Information Behavior*. 1st Edition. Medford, New Jersey, pp. 31–36.

Wilson, T. D. (1981) 'On user studies and information needs', *Journal of Documentation*, 37(1), pp. 3–15.

Wortmann, F. and Flüchter, K. (2015) 'Internet of Things: Technology and Value Added', *Business and Information Systems Engineering*, 57(3), pp. 221–224.

Xia, F., Yang, L., Wang, L. and Vinel, A. (2012) 'Internet of things', *International Journal of Communication Systems*, 25(9), pp. 1101–1102

Zhang, S. and Fever, H. Le (2013) 'An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model', *Journal of Economics, Business and Management*, 1(4), pp. 391–395.

Zins, C. (2007) 'Conceptual Approaches for Defining Data, Information, and Knowledge', *Journal of the Association for Information Science and Technology*, 58(4), pp. 479–493.

# Appendices

## Appendix A: King IV recommended practices for Technology and Information Governance

As drawn from King IV (Institute of Directors South Africa, 2016:62):

10. “The governing body should assume responsibility for the governance of Technology and Information by setting the direction for how technology and information should be approached and addressed in the organisation.
11. The governing body should approve policy that articulates and gives effect to its set direction on the employment of Technology and Information.
12. The governing body should delegate to management the responsibility to implement and execute effective Technology and Information Management.
13. The governing body should exercise ongoing oversight of Technology and Information Management and in particular, oversee that it results in the following:
  - a. Integration of people, technologies, Information and processes across the organisation.
  - b. Integration of Technology and Information risks into organisation-wide Risk Management.
  - c. Arrangement to provide for business resilience.
  - d. Proactive monitoring of intelligence to identify and respond to incidents, including [cyber-attacks] and adverse social media events.
  - e. Management of the performance of, and the risks pertaining to, third-party and outsourced service providers.
  - f. The assessment of value delivered to the organisation through significant investments in Technology and Information, including the evaluation of projects throughout their life cycles and of significant operation expenditure.
  - g. The responsible disposal of obsolete Technology and Information in a way that has regard to environmental impact and Information Security.
  - h. Ethical and responsible use of Technology and Information.
  - i. Compliance with relevant laws.

14. The governing body should exercise ongoing oversight of the management of Information and, in particular, oversee that it results in the following:
  - a. The leveraging of Information to sustain and enhance the organisation's intellectual capital.
  - b. An Information architecture that supports confidentiality, integrity, and availability of Information.
  - c. The protection of privacy of Personal Information.
  - d. The continual monitoring of security of Information.
15. The governing body should exercise ongoing oversight of the management of technology and, in particular, oversee that it results in the following:
  - a. A technology architecture that enables the achievement of strategic and operational objectives.
  - b. The management of risks pertaining to the sourcing of technology.
  - c. Monitoring and appropriate responses to developments in technology, including the capturing of potential opportunities and the management of disruptive effects on the organisation and its business model.
16. The governing body should consider the need to receive periodic independent assurance on the effectiveness of the organisation's Technology and Information arrangements, including outsourced services.
17. The following should be disclosed in relation to Technology and Information:
  - a. An overview of the arrangements for governing and managing Technology and Information.
  - b. Key areas of focus during the reporting period, including objectives, significant changes in policy, significant acquisitions and remedial actions taken as a result of major incidents.
  - c. Actions taken to monitor the effectiveness of Technology and Information management and how the outcomes were addressed.
  - d. Planned areas of future focus.”

## Appendix B: COBIT 5 illustrative set of enablers for privacy compliance

As drawn from COBIT 5 (ISACA, 2013:70):

Enabler	How Can This Enabler Help to Address the Issue?
Principles, Policies and Frameworks	<p>“In terms of policies, a number of policies can be relevant:</p> <ul style="list-style-type: none"> <li>• Relevant board-level policies may include Records Management and Information Security management policies;</li> <li>• Specific Data Governance or Data Management policies may also exist or be in consideration; [and]</li> <li>• A dedicated privacy policy can be developed outlining the rights of the individuals involved and how privacy will/needs to be protected.”</li> </ul>
Processes	<p>Governance-related processes, including:</p> <ul style="list-style-type: none"> <li>• “Ensure risk optimisation; [and]</li> <li>• Ensure stakeholder transparency.”</li> </ul> <p>And management-related processes including:</p> <ul style="list-style-type: none"> <li>• “Manage the IT management framework (specifically Data classification guidelines);</li> <li>• Manage Enterprise Architecture;</li> <li>• Manage risk;</li> <li>• Manage security;</li> <li>• Manage requirements definition;</li> <li>• Manage security services;</li> <li>• Monitor, evaluate and assess the system of internal control; [and]</li> <li>• Monitor, evaluate and assess compliance with external requirements.”</li> </ul>
Organisational structures	<p>“Key responsibility to overcome this issue belongs to:</p> <ul style="list-style-type: none"> <li>• Privacy officer—An individual who is responsible for monitoring the risk and business impacts of privacy laws and for guiding and</li> </ul>

Enabler	How Can This Enabler Help to Address the Issue?
	<p>coordinating the implementation of policies and activities that will ensure that the privacy directives are met;</p> <ul style="list-style-type: none"> <li>• Information security manager</li> </ul> <p>Other related functions can include:</p> <ul style="list-style-type: none"> <li>• Records Management;</li> <li>• Document Management;</li> <li>• Enterprise architecture;</li> <li>• Data/Information Architecture;</li> <li>• Business process owners;</li> <li>• Business executives; [and]</li> <li>• Audit.”</li> </ul>
Culture, Ethics and Behaviour	<p>“The following behaviours are important for maintaining control over privacy issues:</p> <ul style="list-style-type: none"> <li>• Ethical behaviour;</li> <li>• Learning culture;</li> <li>• Risk awareness; [and]</li> <li>• Sense of ownership.”</li> </ul>
Information	<p>“A number of information items are essential for managing privacy issues:</p> <ul style="list-style-type: none"> <li>• Data security and control guidelines;</li> <li>• Data classification guidelines;</li> <li>• Approved user access rights; [and]</li> <li>• Classification of information sources.”</li> </ul>
Services, Infrastructure, and Applications	<p>“A number of services (usually to be provided by the IT function) are relevant in a privacy context:</p> <ul style="list-style-type: none"> <li>• Metadata repository/data dictionary;</li> <li>• Security Management Systems;</li> <li>• Enterprise/Data Architecture system;</li> </ul>

<b>Enabler</b>	<b>How Can This Enabler Help to Address the Issue?</b>
	<ul style="list-style-type: none"><li>• Data profiling tools;</li><li>• Database Management Systems; [and]</li><li>• Document Management Systems.”</li></ul>
People, Skills, and Competencies	“Some skills and competencies requirements for privacy include: <ul style="list-style-type: none"><li>• Business process analysts;</li><li>• Data analysts;</li><li>• Security analysts; [and]</li><li>• Records managers.”</li></ul>

## Appendix C: Mandatory institutional governance structures

As mentioned in Chapter 1, the Higher Education Act (101 of 1997), as amended to date at the time of writing, positions several mandatory structures for South African public higher education institutions. I have briefly summarised them in the table below:

Structure	Detail
Council	“The Council of a public higher education institution must govern the public higher education institution, subject to this Act and the institutional statute” (Republic of South Africa, 1997:23)
Senate	“The Senate of a public higher education institution is accountable to the Council for the academic and research functions of the public higher education institution and must perform such other functions as may be delegated or assigned to it by the Council” (Republic of South Africa, 1997:25).
Committees of Council and Senate	<p>“The Council and the Senate of a public higher education institution may each establish committees to perform any of their functions and may appoint persons, who are not members of the Council or the Senate, as the case may be, as members of such committees” (Republic of South Africa, 1997:26).</p> <p>The Council and the Senate are not divested of responsibility for the performance of any function delegated or assigned to a committee under this section [of the Act]” (Republic of South Africa, 1997:26).</p>
Principal	<p>“The Principal of a public higher education institution is responsible for the management and administration of the public higher education institution” (Republic of South Africa, 1997:26).</p> <p>The Principal is “the chief executive and accounting officer of a public higher education institution, and includes a Vice-Chancellor and a Rector” (Republic of South Africa, 1997:7).</p>
Institutional Forum	<p>“The institutional forum of a public higher education institution must:</p> <ol style="list-style-type: none"> <li>a. advise the council on issues affecting the institution, including the: <ol style="list-style-type: none"> <li>i. the implementation of the Higher Education Act (101 of 1997), and the national policy on higher education;</li> </ol> </li> </ol>

Structure	Detail
	<ul style="list-style-type: none"> <li>ii. race and gender equity policies;</li> <li>iii. the selection of candidates for senior management positions;</li> <li>iv. codes of conduct, mediation and dispute resolution procedures; and</li> <li>v. the fostering of an institutional culture which promotes tolerance and respect for fundamental human rights and creates an appropriate environment for teaching, research and learning; and</li> </ul> <p>b. perform such functions as determined by the Council” (Republic of South Africa, 1997:26).</p>
Students’ Representative Council	<p>“The establishment and composition, manner of election, term of office, functions and privileges of the students’ representative council of a public higher education institution must be determined by the institutional statute and the institutional rules” (Republic of South Africa, 1997:29).</p>