

**FACETS OF INFORMATION GOVERNANCE SYSTEM AT THE SOUTH AFRICAN
COUNCIL FOR SOCIAL SERVICE PROFESSIONS**

by

Tshepo Chauke

Student number: 38569043

Submitted in accordance with the requirements for the degree of

DOCTOR OF PHILOSOPHY AND LITERATURE

in the subject

INFORMATION SCIENCE

at the

UNIVERSITY OF SOUTH AFRICA, PRETORIA

PROMOTER: PROF. M NGOEPE

DECLARATION OF ORIGINALITY

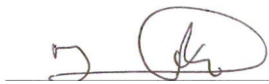
Name: TSHEPO ARNOLD CHAUKE

Student number: 38569043

Degree: DOCTOR OF PHILOSOPHY AND LITERATURE

Title: FACETS OF INFORMATION GOVERNANCE SYSTEM AT THE SOUTH AFRICAN COUNCIL FOR SOCIAL SERVICE PROFESSIONS

I, **Tshepo Arnold Chauke** declare that the above thesis is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references. I further declare that I submitted the thesis to originality checking software and that it falls within the accepted requirements of originality. I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or any other higher education institution.

Signature: 

Date: 29 January 2022

ABSTRACT

In many organisations, information governance (IG) is implemented in fragmented silos and does not add value. After realising this, South African Council for Social Service Professions (SACSSP), embarked on digital transformation process to modernise the organisation by implementing an information governance system. The SACSSP was experiencing challenges due to the lack of a cogent information technology (IT) system design and the disparaged registration, finance and external verification systems inherited that are not compatible with new system innovations to ensure effective and efficient operations. This study utilised the Control Objective for Information and Related Technology (COBIT) to develop an information governance system at SACSSP, with a view for entrenching a culture of good corporate governance.

This critical emancipatory study used qualitative data collected through interviews, focus groups, observation, system and document analysis in response to research questions. The study was a participatory action research project that involved collaboration between the researcher and study participants in defining and solving the problem through needs assessment exercise. In order to address bias, the research findings were reviewed by peers to identify things that might have been missed or gaps that were not addressed. All three phases of participatory action research were followed, namely the 'look phase': getting to know stakeholders so that the problem is defined on their terms and the problem definition is reflective of the community context; the 'think phase': interpretation and analysis of what was learned in the 'look phase'; and the 'act phase': planning, implementing, and evaluating, based on information collected and interpreted in the first two phases. Data was analysed thematically with the use of Atlas Ti 9 and presented in text, figures, pictures and diagrams. The key findings report on the processes taken by the SACSSP in identifying and implementing the IG system implementation, that is, records management, information technology, content management, data governance, information security, data privacy, risk management, litigation readiness, regulatory compliance, long-term digital preservation, and even business intelligence.

The results of the analysis suggest that integrated online system implementation, including system architecture can be used to address issues associated with information integrity in the present and near term, with proper IG policy and information & communication technology (ICT) infrastructure in place. It does not, however, guarantee reliability of information in the first place, and would have several limitations as a long-term solution for maintaining digital records.

The study established that there were no underlying technologies for the implementation of innovation technologies such as, artificial intelligence (AI). Core services of the organisation for social service professionals is dealing with registration related services such: as requirements for registrations; Foreign applications; Registrations fees; Restoration, Banking details. However, the SACSSP was on the right track towards digital transformation of the organisation.

The study suggests a framework for information governance to assist professional organisations and board members to adopt a tailored governance system that would be designed according to their needs. It can be concluded that a successful IG system can be attained through adoption of principles and related accountabilities with a clear strategic direction that is supported by organisational business units. The study recommends that organisations need to make an emphasis of a holistic approach to IG in order to empower a board to coordinate and integrate decision making across the organisation.

Key terms: Information governance; Control Objectives for Information and Related Technologies; South African Council for Social Service Professions; Corporate governance; Participatory Action Research

DEDICATION

This thesis is dedicated to the giants, namely: my mother, Mantshe “N’wa Chauke” Tshabalala and both the Late Bulelani Didiza and Lukishi Mamaile, who took interest in my studies and periodically checking on my progress.

ACKNOWLEDGEMENTS

My sincere gratitude goes to my supervisor, Prof. M Ngoepe, for his faith in this research and his constant encouragement and quick feedback over the years of this project. I remember all your emails, Messenger messages or SMSs would start like this “*Ntate, when are you submitting...*” His guidance has helped me to shape my research, revise the measurement instrument and enhance my writing skills. Working under him has been a stimulating and rewarding experience. I feel very fortunate to have been standing among the giants due to the insightful comments and valuable suggestions.

My deepest sense of gratitude to all the guinea pigs of the in-depth interview instrument used for data collection in this study at the SACSSP: Ms Langi Malamba, Ms Lorraine Masipa, Ms Elaine Harrison, Mr Libe Molapo, Ms Glory Modjadji, Ms Albertinah Thabethe, Mr Leepo Seele, and Mr Ben Kopotja. Your constructive responses and inputs assisted in improving to collect reliable data based on follow-up questions posed. I must express my deep appreciation and gratitude to my wife, Tebogo, for the patience and love all these years, as well as my son, Nyiko, who, upon hearing that I am doing a doctoral study, asked: “*What kind of a doctor are you going to be because you are using a laptop? I know doctors are in hospitals?*”

I would also like to thank the South African Council for Social Service Professions, the Council (Board) and the Registrar, Ms Malamba who assisted with granting me access and trusting me in the implementation of an information governance system to support corporate governance. It would be the greatest sin to forget Dr Victor Paledi for the reviews all my chapters and valuable inputs on the whole product.

Most importantly, I appreciate all the participants in the focus group gatherings and access to hardware, systems and documents analysis for the. Without their help and support, this research could not have been possible. Finally, I would like to thank Unisa for sponsoring my PhD studies.

Habakkuk 2: 2 - 3

Write down the revelation and make it plain on tablets so that whoever reads it may run with it. For the revelation awaits an appointed time...

Table of Contents

DECLARATION OF ORIGINALITY.....	
ABSTRACT.....	i
DEDICATION	iii
ACKNOWLEDGEMENTS	iv
Table of Figures	xiii
List of Tables	xvi
List of Abbreviations	xvii
CHAPTER ONE	1
INTRODUCTION: PUTTING THINGS INTO PERSPECTIVE.....	1
1.1 Introduction and background	1
1.1.1 Conceptualisation.....	4
1.1.2 Contextual setting.....	5
1.2 Statement of the problem.....	6
1.3 Purpose of the study	8
1.3.1 Research questions	8
1.4 Scope and delimitations	9
1.5 Justification of study.....	9
1.6 Originality.....	10
1.7 Theoretical foundation	11
1.7.1 Brief background of COBIT framework.....	13
1.8 Preliminary literature review	15
1.8.1 Evaluate, direct and monitor.....	15
1.8.2 Align, plan and organise.....	16
1.8.3 Build, acquire and implement	16
1.8.4 Deliver service and support	17
1.8.5 Monitor, evaluate and assess.....	17
1.9 Research methodology.....	17
1.10 Definition of terms	18
1.11 Ethical considerations.....	19
1.12 Citation management and referencing method	19
1.13 Chapter outline	19
1.14 Summary.....	21

CHAPTER TWO	22
LITERATURE REVIEW: AN INFORMATION GOVERNANCE SYSTEM IN SUPPORT OF CORPORATE GOVERNANCE.....	22
2.1 Introduction.....	22
2.2 Evaluate, direct and monitor	23
2.2.1 Governance framework setting and maintenance.....	25
2.2.2 Benefits delivery	26
2.2.3 Risk optimisation	26
2.2.4 Resource optimisation	27
2.2.5 Stakeholder engagement.....	29
2.3 Align, plan and organise.....	30
2.3.1 Information and technology management framework	31
2.3.2 Strategic management	32
2.3.3 Enterprise architecture	32
2.3.4 Innovation	34
2.3.5 Portfolio management.....	40
2.3.6 Budgeting and costing	42
2.3.7 Human resources management.....	43
2.3.8 Relationship management	45
2.3.9 Service level agreements.....	45
2.3.10 Vendors management.....	46
2.3.11 Quality management.....	46
2.3.12 Risk management	48
2.3.13 Security management.....	50
2.3.14 Data management.....	52
2.4 Build, acquire and implement	54
2.4.1 Programme management	55
2.4.2 Requirements definition.....	55
2.4.3 Solutions identification and build.....	56
2.4.4 Availability and capacity management.....	57
2.4.5 Organisational change management	58
2.4.6 IT change management	60
2.4.7 IT change acceptance and transitioning management.....	61

2.4.8	Knowledge management	61
2.4.9	Asset management	64
2.4.10	Configuration management	65
2.4.11	Project management.....	66
2.5	Deliver, service and support	66
2.5.1	Operations management.....	67
2.5.2	Service request and incident management.....	70
2.5.3	Problem management	71
2.5.4	Continuity management	72
2.5.4.1	Continual improvement	73
2.5.5	Security services management.....	74
2.5.6	Business process controls management.....	75
2.6	Monitor, evaluate and assess.....	76
2.6.1	Performance and conformance monitoring	77
2.6.2	Internal control system	77
2.6.3	External requirements compliance	78
2.6.4	Assurance management	78
2.7	Summary.....	79
CHAPTER THREE		80
RESEARCH METHODOLOGY		80
3.1	Introduction.....	80
3.2	Research paradigm.....	81
3.3	Research approaches.....	83
3.3.1	Quantitative research.....	83
3.3.2	Qualitative research	84
3.3.3	Mixed methods research.....	85
3.3.4	Justification for using a qualitative approach	86
3.4	Research methods	86
3.5	Population and sampling.....	92
3.5.1	Purposive sampling.....	93
3.5.2	Theoretical sampling.....	94
3.5.3	Generic sampling.....	94
3.5.4	Snowball sampling	94

3.5.5	Justification for sampling technique used.....	95
3.6	Data collection instruments.....	95
3.6.1	Interviews.....	96
3.6.2	Focus groups	97
3.6.3	Observations.....	99
3.6.4	Document analysis.....	99
3.6.5	System (applications) analysis.....	100
3.7	Trustworthy of data	100
3.7.1	Trustworthiness	101
3.7.2	Authenticity.....	101
3.7.2.1	Democratic validity.....	101
3.7.2.2	Outcome validity.....	102
3.7.2.3	Process validity	102
3.7.2.4	Dialogue validity	102
3.7.2.5	Catalytic validity.....	102
3.8	Data analysis and presentation.....	104
3.9	Ethical considerations.....	104
3.10	Evaluation of research methodology.....	106
3.11	Summary	107
CHAPTER FOUR		108
ANALYSIS AND PRESENTATION OF RESULTS.....		108
4.1	Introduction.....	108
4.2	Participants' profile.....	108
4.3	Data analysis presentation.....	109
4.4	Presentation and discussion of results	111
4.5	Theme one: Evaluation, direction and monitor	111
4.5.1	Governance framework setting and maintenance.....	112
4.5.2	Benefits delivery	113
4.5.3	Risk optimisation	114
4.5.4	Resource optimisation	115
4.5.5	Stakeholder engagement.....	117
4.6	Theme two: Align, plan and organise.....	120
4.6.1	Information and technology management framework	120

4.6.2	Strategic management	122
4.6.3	Enterprise architecture	123
4.6.4	Innovation	123
4.6.5	Portfolio management.....	129
4.6.6	Budgeting and costing	132
4.6.7	Human resources management.....	135
4.6.8	Relationships management	136
4.6.9	Service level agreements.....	138
4.6.10	Vendors management	139
4.6.11	Quality management.....	141
4.6.12	Risk management	142
4.6.13	Security management.....	144
4.6.14	Managed data.....	146
4.7	Theme three: Build, acquire and implement	147
4.7.1	Programme management	148
4.7.2	Requirements definition.....	149
4.7.3	Solutions identification and build.....	158
4.7.4	Availability and capacity management.....	159
4.7.5	Organisational change management	161
4.7.6	IT changes management	164
4.7.7	IT change acceptance and transitioning management.....	166
4.7.8	Knowledge management	167
4.7.9	Asset management	168
4.7.10	Configuration management	169
4.7.11	Project management.....	172
4.8	Theme four: Deliver, service and support.....	174
4.8.1	Operations management.....	174
4.8.2	Service request and incident management.....	179
4.8.3	Problem management	180
4.8.4	Continuity management	180
4.8.5	Security services management.....	183
4.8.6	Business process control management.....	187

4.9	Theme five: Monitor, evaluate and assess.....	191
4.9.1	Performance and conformance monitoring	191
4.9.2	Internal control system	193
4.9.3	External requirements compliance	194
4.9.4	Assurance management	196
4.10	Summary	198
CHAPTER FIVE.....		199
INTERPRETATION AND DISCUSSION OF RESEARCH FINDINGS.....		199
5.1	Introduction.....	199
5.2	Evaluate, direct and monitor	199
5.2.1	Governance framework setting and maintenance.....	201
5.2.2	Benefits delivery	202
5.2.3	Risk optimisation	203
5.2.4	Resource optimisation	203
5.2.5	Stakeholder engagement	204
5.3	Align, plan and organise.....	204
5.3.1	I&T management framework	205
5.3.2	Strategic management	205
5.3.3	Enterprise architecture	206
5.3.4	Innovation	208
5.3.5	Portfolio management.....	211
5.3.6	Budgeting and costing	211
5.3.7	Human resources management.....	212
5.3.8	Relationships management	214
5.3.9	Service level agreements.....	214
5.3.10	Vendors management	215
5.3.11	Quality management.....	216
5.3.12	Risk management	217
5.3.13	Security management.....	218
5.3.14	Managed data.....	220
5.4	Build acquire and implement	222
5.4.1	Programme management	222
5.4.2	Requirements definition.....	223

5.4.3	Solutions identification and build.....	224
5.4.4	Availability and capacity management.....	224
5.4.5	Organisational change management	225
5.4.6	IT changes management	225
5.4.7	IT change acceptance and transitioning management.....	226
5.4.8	Knowledge management	226
5.4.9	Asset management	227
5.4.10	Configuration management	228
5.4.11	Project management.....	228
5.5	Deliver, service and support.....	229
5.5.1	Operations management.....	229
5.5.2	Service request and incident management.....	233
5.5.3	Problem management	233
5.5.4	Continuity management	234
5.5.5	Security service management.....	235
5.5.6	Business process control management.....	235
5.6	Monitor, evaluate and assess.....	236
5.6.1	Performance and conformance monitoring	236
5.6.2	Internal control system	236
5.6.3	External requirements compliance	237
5.6.4	Assurance management	237
5.7	Summary.....	238
CHAPTER SIX		239
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS		239
6.1	Introduction.....	239
6.2	Summary of findings	240
6.2.1	Evaluation, direction and monitor	240
6.2.2	Align, plan and organise.....	242
6.2.3	Build, acquire and implement	243
6.2.4	Deliver, service and support	244
6.2.5	Monitor, evaluate and assess.....	244
6.3	Recommendations	245
6.3.1	Evaluation, direction and monitor	246

6.3.2 Align, plan and organise.....	246
6.3.3 Build, acquire and implement.....	247
6.3.4 Deliver, service and support.....	247
6.3.5 Monitor, evaluate and assess.....	248
6.4 Proposed information governance system framework at THE SACSSP.....	248
6.4.1 Description of the information governance system framework	251
6.4.2 Application of the information governance system	253
6.5 Recommendations for future research.....	254
6.6 Implications on theory and practice	255
6.7 Final conclusion	255
References	257
Annexure A: Questionnaire.....	284
Annexure B: Documents analysed	291
Annexure C: Ethical clearance.....	294
Annexure D: Letter of permission	298
Annexure E: Informed consent.....	299
Annexure F: Proof of qualitative analysis activities.....	305
Annexure G: Data source verification	306

TABLE OF FIGURES

Figure 1-1: One of the Archives room at SACSSP	6
Figure 1-2: Governance and management key areas	12
Figure 1-3: COBIT release timeline	14
Figure 1-4: COBIT core model	15
Figure 2-1: Role of the board and responsibilities	24
Figure 2-2: Evaluate, direct and monitor domain processes	24
Figure 2-3: Scope of I&T-related risk relative to other major risks.....	27
Figure 2-4: Resource optimisation	28
Figure 2-5: Resource levelling.....	29
Figure 2-6: Plan domain processes.....	30
Figure 2-7: Goals cascade	31
Figure 2-8: Blockchain transaction	37
Figure 2-9: Activists camouflaged against mass surveillance	39
Figure 2-10: John Hopkins coronavirus interactive map.....	40
Figure 2-11: Service identification process.....	41
Figure 2-12: Service portfolio	41
Figure 2-13: South African public sector budget cycle key milestones.....	43
Figure 2-14: Skills management cycle.....	44
Figure 2-15: Risk response plan	49
Figure 2-16: Ransomware screenshot	51
Figure 2-17: Data linkage possibilities.....	53
Figure 2-18: Build, acquire and implement domain processes.....	55
Figure 2-19: Capacity management process.....	58
Figure 2-20: SECI Model.....	63
Figure 2-21: Configuration Items contribution to IT service	65
Figure 2-22: Run domain processes	67
Figure 2-23: Service desk activities.....	71
Figure 2-24: Continual improvement model	73
Figure 2-25: Monitor domain processes.....	77
Figure 2-26: Planning, monitoring and reporting	79
Figure 3-1: Research methodology roadmap	81
Figure 3-2: Action Research Interacting Spiral.....	90
Figure 3-3: SACSSP organisational structure	93
Figure 4-1: Participants profile	109
Figure 4-2: Data groupings.....	110
Figure 4-3: Quotations generated	110
Figure 4-4: Innovation discussion items	124
Figure 4-5: Focus group meeting - Digital certificates	125

Figure 4-6: Search a register.....	129
Figure 4-7: Complaints management	129
Figure 4-8: Professional conduct process	131
Figure 4-9: Registration services.....	131
Figure 4-10: SACSSP budget 2018 – 2021.....	132
Figure 4-11: Employee compensation.....	133
Figure 4-12: Bid evaluation – networking	137
Figure 4-13: Fiber requirements meeting	137
Figure 4-14: Hardware and software tender advertisement	139
Figure 4-15: System development tender	140
Figure 4-16: Files, cabinets with returned certificates	141
Figure 4-17: Ransom malware message sent.....	144
Figure 4-18: Initial briefing notes	150
Figure 4-19: Scoping requirements	150
Figure 4-20: Benchmarking exercise - Similar sized organisation.....	151
Figure 4-21: Benchmarking notes (similar sized council one)	152
Figure 4-22: Benchmarking – similar sized council two.....	153
Figure 4-23: Solutions evaluation	154
Figure 4-24: Digital certificate meeting.....	155
Figure 4-25: Networking requirements meeting	155
Figure 4-26: Backup requirement.....	156
Figure 4-27: Proposed server hardware solution	158
Figure 4-28: Backup and replication systems.....	160
Figure 4-29: How to connect document on MS Teams invite	165
Figure 4-30: Meeting login instruction	168
Figure 4-31: Computing hardware analysis results	169
Figure 4-32: Dry wall in server room	170
Figure 4-33: Portion of building plan	170
Figure 4-34: Procedure to log into MS Teams.....	174
Figure 4-35: Networking and cooling assets	176
Figure 4-36: Old server room	176
Figure 4-37: Fire extinguisher outside old server room	177
Figure 4-38: Server room notice.....	178
Figure 4-39: Fire extinguishers in archives room	181
Figure 4-40: IT and Business Re-engineering Committee MS Teams invitation	181
Figure 4-41: Surveillance camera	183
Figure 4-42: Access control receipt.....	184
Figure 4-43: Fire extinguisher	185
Figure 4-44: New server room door	186
Figure 4-45: Business process document	188

Figure 4-46: Consolidated processes.....	190
Figure 4-47: SACSSP annual reports.....	194
Figure 4-48: DSD Presentation on budget vote.....	195
Figure 5-1: SACSSP internet of things connection nodes.....	209
Figure 5-2: Proposed artificial intelligence framework.....	210
Table 5-1: Transition options for roles in the office, administrative job families.....	213
Figure 5-3: Sample of proposed phone USSD-based contacts.....	221
Figure 5-5: Contract management process.....	231
Figure 6-1: SACSSP Alignment of business and ICT.....	242
Figure 6-2: Information governance system framework.....	250

LIST OF TABLES

Table 2-1: COBIT 2019 framework and literature linkage	23
Table 2-2: Operability requirements	33
Table 2-3: Ten types of innovation	35
Table 2-4: Data quality implications	47
Table 2-5: Data quality components	48
Table 2-6: Solution sourcing model.....	56
Table 2-7: Pressures for organisation change	59
Table 2-8: I&T asset classification.....	64
Table 2-9: Service and Incident management differences	71
Table 3-1: Paradigm differences.....	82
Table 3-2: Common research designs / approaches	87
Table 3-3: Action research work plan and timelines.....	91
Table 3-9: Overall population classification	95
Table 3-4: Interviews sources	96
Table 3-5: Focus committee meetings activities	97
Table 3-6: Composition of focus committee meeting groups	98
Table 3-7: Applications analysis	100
Table 3-10: Catalytic authenticity process	103
Table 4-1: Key stakeholders for the SACSSP	117
Table 4-2: I&T management components.....	120
Table 4-3: SACSSP data sources	127
Table 4-4: Positions affected by digital disruption	135
Table 4-5: Organisational change management.....	161
Table 4-6: IT change transition activities.....	166
Table 4-7: Configuration documents required	171
Table 4-8: Projects identification.....	172
Table 5-2: Risk matrix.....	218
Table 5-3: Proposed pipeline services.....	222
Table 6-1: Governance system accountability, principles and practices	241

LIST OF ABBREVIATIONS

ADSL:	Asymmetric Digital Subscriber Line
API:	Application Programming Interface
APO:	Align, Plan and Organise
BAI:	Build, Acquire and Implement
BYOD:	Bring Your Own Device
CBPR:	Community-Based Participatory Research
CCTA:	Central Computer and Telecommunications Agency
CER:	Critical Emancipatory Research
CI:	Configuration Item
CMMI:	Capability Maturity Model Integration
COBIT:	Control Objectives for Information and Related Technologies
COP:	Community of Practice
CPD:	Continuing professional development
CPI:	Committee for Preliminary Inquiry
CSI:	Continual Service Improvement
CSIRT:	Computer Security Incident Response Team
CSD:	Central Supplier database
CSV:	Comma-separated values
DHA:	Department of Home Affairs
DSD:	Department of Social Development
DSS:	Deliver, Service and Support
DRP:	Disaster recovery plan
EDM:	Evaluate, Direct and Monitor
EDMS:	Electronic Document Management System
EGIT:	Enterprise Governance of Information and Technology

ETD:	Education Training Development
EU:	European Union
FMPPI:	Framework for Managing Programme Performance Information
FMPPL:	Financial Management of Parliament and Provincial Legislatures
FOIA:	Freedom of Information Act
GDPR:	General Data Protection Regulation
GEIT:	Governance of Enterprise Information Technology
GWEA:	Government Wide Enterprise Architecture Framework
HA:	High Availability
ID:	Identity Document
IG:	Information Governance
I&T:	Information and Technology
IODSA:	Institute of Directors South Africa
IoT:	Internet of Things
IP:	Intellectual Property
IS:	Information Systems
ISACA:	Information Systems Audit and Control Association
IT:	Information Technology
ITG:	Information Technology Governance
ITCM:	Information Technology Changes Management
ITSM:	Information Technology Service Management
LIS:	Library Information Systems
MEA:	Monitor, Evaluate and Assess
MMR:	Mixed Methods Research
NARA:	National Archives and Records Administration
NCPF:	National Cybersecurity Policy Framework
NGO:	Non-Governmental Organisation

NPO:	Non-profit organisation
OCM:	Organisational Change Management
O-DF:	Open Data Format
OEM:	Original Equipment Manufacturer
PAR:	Participatory Action Research
PBSW:	Professional Board for Social Work
PDCA:	Plan-Do-Check-Act
PMBOK	Project Management Body of Knowledge
PMG:	Parliamentary Monitoring Group
PMI:	Project Management Institute
PMRF:	Performance Management and Reporting Framework
PRINCE2:	Projects IN Controlled Environment Version 2
PoE:	Power over Ethernet
POPI:	Protection of Personal Information
RACI:	Responsible, Accountable, Consulted, and Informed
RCPC:	Registrar Committee for Professional Conduct
RFC:	Requests for Change
RM:	Records Management
RSA:	Republic of South Africa
SaaS:	Software as a Service
SACSSP:	South African Council for Social Service Professions
SAQA:	South African Qualification Authority
SD:	Service Design
SLA:	Service Level Agreement
SLM:	Service Level Management
SME:	Small and Medium Enterprise
SS:	Service Strategy

SO:	Service Operation
SOX:	Sarbanes-Oxley Act
SQL:	Structured Query Language
SSP:	Social Service Professional
ST:	Service Transition
TOGAF:	The Open Group Architecture Framework
TOR:	Terms of Reference
UM:	Unified Messaging
Unisa:	University of South Africa
VoIP:	Voice over Internet Protocol
VPN:	Virtual Private Network
WEF:	World Economic Forum

CHAPTER ONE

INTRODUCTION: PUTTING THINGS INTO PERSPECTIVE

1.1 INTRODUCTION AND BACKGROUND

Information governance (IG) is a concept that refers to the governing of information in the digital era where information assumes a central role (Brown & Toze 2017: 582). IG is a “subset of corporate governance, and includes key concepts from records management, content management, Information Technology (IT) and data governance, information security, data privacy, risk management, litigation readiness, regulatory compliance, long-term digital preservation, and even business intelligence” (Smallwood 2014: 5). The success of IG is key in ensuring timely, adequate, compliant information throughout business activities in order to make decisions for gaining competitiveness and improvement of organisational efficiency (Nguyen, Sargent, Stockdale & Scheepers 2014: 1). The main concern of organisations in managing business risk and service disruption while trying to improve and develop positive relationships with their external stakeholders by delivering efficient services that meet their needs (Motii & Semma 2017: 51). Iles (2013: 1) proposes IG as a fuller and richer way that has a more holistic view of organisational information than of records management. Mullon and Ngoepe (2019) indicate that IG has not been defined properly, since different domains or aspects of IG, such as records management and IT governance, to mention just two, are regulated by different government entities nationally in South Africa. This problem is further cascaded to organisational level where IG elements are managed by different business units. This brought about a gap in the governance of information which, if corrected, can bring surety to how the information is obtained, recorded, held and shared by the organisation (Warwickshire County Council 2018).

Hou (2013: 23) indicates that the availability of reliable information sources is regarded as a key component of executive decision-making. A study by Mojapelo (2017: 53) showed that the placement of records management function in public organisations in South Africa has not been clearly defined to achieve the integration of information. This was also the case with access to information, which is also a domain of IG (Mullon

& Ngoepe 2019). While it is acknowledged that information is a valuable organisational asset, many companies fail to realise its full business value. This has been attributed to poor information governance (Newman & Logan 2006; Panian 2010: 940). An effective IG initiative enables the development of formal policies and standards and ensures oversight over information so that decision makers receive accurate and timely information to respond to challenges and opportunities identified.

Kooper, Maes and Lindgreen (2011: 196) highlight the difficulty of evaluating and governing information, especially information stored in the cloud. As a result, information technology (IT) has been wrongly regarded as an umbrella term for IG (Ngoepe & Ngulube 2014). Information is stored across national boundaries, which can make the accessibility of such online records unclear in the event of malicious attacks or cloud companies closing down (Jansen & Duranti 2013: 63).

A good example of the repercussions of poor IG is the report that it had caused reputational damage to the Royal Bank of Scotland and also affected customers of other banks due to data breaches (Samiotakis 2013: 8; Smallwood 2014: 10). Recently, Huygh and De Haes (2018: 4887) and the Information System Audit and Control Association (ISACA 2018: 18) proposed a dynamic end-to-end governance system that focuses on all technology and information processing that the enterprise puts in place to achieve its goals. According to Caravaca (2016: 47), data are stored in organisations without any clear concept due to the following aspects: use of standardised formats, resolution, integrity of the image and metadata. Information is disorganised due to a lack of fixed form and stable content, and technology obsolescence that makes digital records inaccessible (Duranti 2016: 6).

Gartner, Pezzini, Natis, Malinverno, Iijima, Thompson, Thoo and Guttridge (2017) propose that the adoption of hybrid integration strategies involving a combination of cloud-resident and on-premises endpoints which can be achieved by developing, deploying, executing, managing and monitoring integration processes and flows that connect multiple endpoints, which are not currently evident. According to DataDesign Technology Partners (2019: 7), nobody knows if virtual file sharing platforms such as

Dropbox, Google Docs and others can be used in organisations. According to Smallwood (2014: 1), finding the necessary information takes time and costs money since information generated is growing at a compounding rate. According to Nicho (2013: 156), organisations are dealing with missing data, which is further compounded by information being stored in remote sites.

While institutions are faced with challenges of poor IG, there has been a need for processing or treatment of physical records through digitisation and integrating them with business information systems (IS) (Commonwealth of Australia 2013). The county councils of Nottinghamshire and Warwickshire realised that information assets are vital to their organisations for service provision as well as the effective management of their council's operations (Agnew 2019: 2; Warwickshire County Council 2018: 3).

In the United States, the National Archives and Records Administration (NARA) developed the Obama Presidential digital library, which houses 95% of all the records consisting of word-processing documents, spreadsheets, portable document files (PDFs), photographic and video records, which can be equated to about 1,5 billion "pages" (Cohen 2019). It is on that note that the Freedom of Information Act (FOIA) guideline states that the digitised archived records are considered to have permanent value and guidelines were created for their online access (United States of America 2016). Recently, the archives data of the Holocaust victims in Germany were digitised and posted online, thus making it easily accessible to be viewed by interested parties (Arolsen Archives 2019).

In the South African context, Mullon and Ngoepe (2019: 12) conclude that there was no over-arching structure responsible for overall IG since there were fragmented elements that led to duplication. The Republic of South Africa (RSA) (2019: 45) emphasises that multiple and disparaged information is hosted in silo-based systems, which are not easily integrated into a customer-focused, service-driven environment.

A study by Nguyen et al. (2014: 1) indicated that poor IG and information management practices have led to the retention of information of very little value, difficulty in finding and accessing information, the impossibility of information exchange, risks involving

data leakage, breach of information, loss of personally identifiable content, and the high cost of keeping information. The main challenge of IG is to reconcile the elements of the new information environment that has a legacy of information-related legislation, policies, institutions and practices (Brown & Toze 2017: 586).

There are regulations in place for the use of information in the cloud (Guercio 2015: 37). While efforts were made towards cooperation between the European Union (EU) and member states on regulations regarding cloud policies, the regulations on records management and digital preservation are fragmented and insufficient (Guercio 2015: 11). The General Data Protection Regulation (GDPR) outlines the sharing of data between organisations and third countries, which is enforceable by the courts (Hoofnagle, Sloot & Borgesius 2019: 71). In South Africa, the Protection of Personal Information (POPI) Act was enacted to make concessions between the right to privacy and the for free flow of, and access to information and to regulate how personal information is processed (RSA 2013: 14). This study utilised Control Objectives for Information and Related Technology (COBIT) as a lens to explore an information governance system framework to assist professional organisations and board members to adopt a tailored governance system that would be designed according to their needs.

1.1.1 Conceptualisation

Neuman (2014: 209) defines conceptualisation as a process of specifying exactly what is meant and not as the terms that are used in day-to-day life by linking those ideas to a conceptual or theoretical definition. Merkus, Helms and Kusters (2019: 151) define IG as “an establishing management of information in an organisation assuring quality and access during its life-cycle to be accountable for information assets” found in records and information management; security management; risk management, data storage and archiving; knowledge management; auditing; enterprise architecture, big data and finance.

Soma, MacDonald, Termeer and Opdam (2016: 132) conceptualise IG as an institutional framework for governing information with the purpose of providing guidance or managing across an organisation.

1.1.2 Contextual setting

This section discusses the background of the study. This study was conducted at the South African Council for Social Service Professions (SACSSP). The SACSSP is a statutory body established in terms of section 2 of the Social Service Professions Act, No. 100 of 1978 (RSA 1978: 4) as amended by Act No. 102 of 1998 (RSA 1998: 4). The council guides and regulates the professions of social work and child youth care work in aspects pertaining to registration, education and training, professional conduct and ethical behaviour, ensuring continuing professional development, and fostering compliance with professional standards (SACSSP 2018a). The council's office is situated in Pretoria, South Africa (RSA 1998: 4). The SACSSP has been operating on a manual filing system and disparaged IT systems that made it difficult to have an integrated view in support of IG. The organisation used an obsolete Silverlight-based application (SACSSP 2018b). All IT services are outsourced and it becomes difficult for the organisation to access reports since all access to the databases is controlled by the service provider (SACSSP 2018b; SACSSP 2019). The members' qualifications are sent for verification to the South African Qualifications Authority (SAQA) on an annual basis and the verification process is delayed due to inconsistent data. The researcher was part of the exploratory meeting where challenges to information access were raised and permission was given for system overhaul to take place with a view to maximise information efficiency and integration within the organisation (SACSSP 2018b: 1).

With regard to IG, the SACSSP still runs silo-based systems that are not integrated with other functions. The organisation is currently experiencing delays with paper-based processes, including the challenges with the provision of document tracking. There is dependence on the postal services where a letter sent to customers has to be registered, and this creates more costs for postage to the council. Organisational risks are not formally recorded and mitigated according to international best practices.

The challenge experienced at the SACSSP is that the archives division is full to capacity and it becomes difficult to preserve historic documents due to unsustainable long-term records storage (Figure 1-1).



Figure 1-1: One of the Archives room at SACSSP
(Photographer: Researcher: 2019)

1.2 STATEMENT OF THE PROBLEM

The problem for this study was defined by the SACSSP when the council realised that there was a need to move away from manual data processing towards more integrated and technologically supported data systems, which can be used to support the integration of data across organisations such as communication with clients, which is fraught with challenges (Brown & Toze 2017: 586). Furthermore, as depicted in Figure 1-1, the SACSSP faced challenges with physical records at the SACSSP. This was the case because the IG facets were implemented in a fragmented manner with no single business unit responsible. As a result, managers were unable to receive information timeously for decision-making or reporting to the organisation's board and the stakeholders as per their responsibilities (Guetat & Dakhli 2015: 1090).

Furthermore, Amadi-Echendu (2016: 2) points out that the disparaged legacy IT systems were not compatible with technological systems used at the SACSSP. The lack of compatibility resulted in physical files and digital records being difficult to find, making such data being unavailable for provisioning of improved service delivery to clients (Shibambu & Ngoepe 2020: 2).

The SACSSP acknowledges that its greatest asset is information and part of attaining a harmonious integration of solutions is to transition from manual processes to automated solutions. As a result, just as the researcher, the SACSSP was involved in a holistic implementation of IG within the organisation by using COBIT. ISACA (2018b: 13) confirms the updated COBIT framework that the governance and management of enterprise information and technology (I&T) should be aimed at the whole enterprise and not be limited to the IT department of an organisation. According to Moeller (2013: 126), organisations put effort into mitigating enterprise-wide risks, while the same cannot be said about risk management processes at the SACSSP due to the fact that they are not formalised. Two strategic IT risks were identified, namely a lack of a disaster recovery plan (DRP) and secure intellectual property (IP) of SACSSP data, which would lead to the loss of critical information and IP of the SACSSP (SACSSP 2019: 1).

Currently, the SACSSP Act is the only formal document prescribing the keeping of registers and any document purporting to be an extract thereof, signed by the registrar and the procedures of removal, rectification and restoration on the SACSSP's register (RSA 1998: 23). This is evident since the audit conducted in 2015/16 brought a finding that Microsoft's Structured Query Language (SQL) database was not integrated with the finance system, Pastel Accounting, and this creates reconciliation challenges due to duplicated transactional and incomplete data receipts of the membership fees (SACSSP 2016: 20). This study intended to propose an integrated framework that would offer a seamless flow of information across all business units within the organisation.

1.3 PURPOSE OF THE STUDY

The purpose of this study was to explore an IG system, with a view to entrenching a culture of supporting corporate governance at the SACSSP. In view of the purpose, the study sought to:

- determine how information governance can be used for evaluation, direction and monitoring of the SACSSP's strategy by the board
- review how the information governance planning can assist in business alignment at the SACSSP
- determine how the SACSSP can build, acquire and implement programmes and projects that support business processes
- review the outcomes of information governance and related technologies as per the planning
- establish how information governance can provide transparency in the monitoring of performance and conformance to drive the achievement of goals by management
- suggest an information governance framework for the SACSSP.

The next section addresses primary and secondary research questions

1.3.1 Research questions

Primary research question: *“How can Information Governance be implemented to support corporate governance at the South African Council for Social Service Professions?”*

The study sought to answer the following questions:

- How can information governance be used for the evaluation, direction and monitoring of the SACSSP's strategy by the board members?
- How can information governance planning assist in business alignment?
- What programmes and projects can be implemented by the SACSSP to support business processes?

- How can the outcomes of information governance and related technologies be reviewed?
- What monitoring can be provided to bring transparency of performance and conformance to drive the achievement of goals by management?

The next section discusses scope and delimitations for the study.

1.4 SCOPE AND DELIMITATIONS

This study aimed to develop an information governance system at SACSSP, with a view for entrenching a culture of good corporate governance. The study was limited to the SACSSP and the final decision on the implementation as per the recommendations presented by the researcher was done through democratisation with persons who have delegated responsibilities. The study did an assessment of the status quo and the future needs; developed the scope of work for the suitable system design, including the policies and procedures; and designed the automation and digitisation processes and physical files. The facets of IG that were covered consisted of records and information management, security management, risk management, data storage and archiving, knowledge management, auditing, enterprise architecture, big data and finance. Corporate governance consisted of risk, auditing, IT and stakeholders, among the other facets and are included as part of the scope.

1.5 JUSTIFICATION OF STUDY

Creswell (2014: 138) explains the significance of a study as conveying the importance for different audiences that may profit from reading and using the study. The importance of the study would be to enhance the use of I&T as an asset for small and medium-sized businesses' competitiveness, since most of the frameworks are designed for large organisations. The benefit for the SACSSP would be the optimisation of the processes of the core business so that it can achieve its business goals through the adoption of the framework. This is further supported by ISACA (2018b: 12) postulating that strategic alignment is of paramount importance to be

applied to overall activities in the organisation to ensure that I&T-related objectives are aligned with enterprise goals.

The research advanced how the structures can be put in place for the holistic alignment of information governance to ensure that the SACSSP stays on track to achieve their business and I&T goals, and at the same time, the measurement of IT performance of information technology governance (ITG) through the use of capability maturity model integration (CMMI). The research contributed to the body of knowledge in the application of holistic information governance processes using the convergence of the COBIT framework which would provide an integrated, top-to-bottom approach to IT governance. The processes-capability maturity scheme ranges from zero (0) to five (5) measuring how well a process is implemented and performing.

1.6 ORIGINALITY

According to Gill and Dolan (2015: 12), the key definitions of originality in a doctoral study are the following:

- Continuing a previously original piece of work.
- Carrying out original work designed by the supervisor.
- Providing a single original technique, observation or result in an otherwise unoriginal but competent piece of research.
- Having many original ideas, methods and interpretations all performed by others under direction of the postgraduate.
- Showing originality in testing somebody else's idea/theory.
- Carrying out empirical work that has not been done before.
- Making a synthesis of things that have not been put together before.
- Using already known material but with a new interpretation.
- Trying out something in this country that has previously been done only elsewhere.
- Taking a particular technique and applying it in a new area.
- Bringing new evidence to bear on an old issue.
- Being cross-disciplinary and using different methodologies.

- Looking at areas not previously explored in a particular discipline.

A high level of originality and contribution to knowledge in a way that has not been done before, is demonstrated through this study (Ngulube 2020: 520). According to Lantsoght (2018: 5), the study has brought a major piece of new information through the utilisation of COBIT framework in a professional council.

In order to meet the originality requirement for a doctoral study, the researcher collected original data for the study through the participatory action research (PAR) approach that is unique to the setting. Furthermore, for the production of new knowledge using IG to support corporate governance system in information science. The problem of the study was formulated by the participants, together with the researcher, and they were also part of proposing the solution over a period of four years. The researcher attended several meetings, provided advice, helped writing documents and interviewed participants. Furthermore, the study is original in terms of the context, as well as the methodology used to solve the problem.

1.7 THEORETICAL FOUNDATION

The research adopted an inductive reasoning approach where it commenced with the use of the Control Objectives for Information and Related Technology (COBIT) theoretical framework (Bryman 2016: 21). Leedy, Ormrod and Johnson (2019: 21) explain that the process involves the collection and inference of conclusions from data. The COBIT framework provides an integrated, top-to-bottom approach to I&T governance and better alignment from a business perspective (Samiotakis 2013: 15). The framework as described by Mourad, Malik, Anong and Mustappa (2017: 41) is that COBIT is providing the 'why' in solving business problems and supporting business goals achievement. Mourad et al. (2017: 45) opine that COBIT may be perceived as theoretical since it does not deal with daily operational issues, rather it looks at the organisation as a whole. Motii & Semma (2017: 49) state that COBIT provides a set of rules for the effective management of I&T governance. The main constructs of the study on COBIT included the five domains, one of which was known

as: Evaluate, Direct and Monitor (EDM). This domain is the responsibility of the organisational structure governance. ISACA (2012: 14) states that governance:

... ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

The domains that management is responsible for are: second construct: Align, Plan and Organise (APO); third construct: Build, Acquire and Implement (BAI); fourth construct: Deliver, Service and Support (DSS); and fifth construct: Monitor, Evaluate and Assess (MEA), as depicted in the governance and management key areas that were used in the objectives and informed literature review and data collection of the study (Figure 1-2). ISACA (2012: 14) describes management's role as planning, building, running and monitoring of activities in alignment with the direction set by the governance body to achieve the enterprise's objectives.

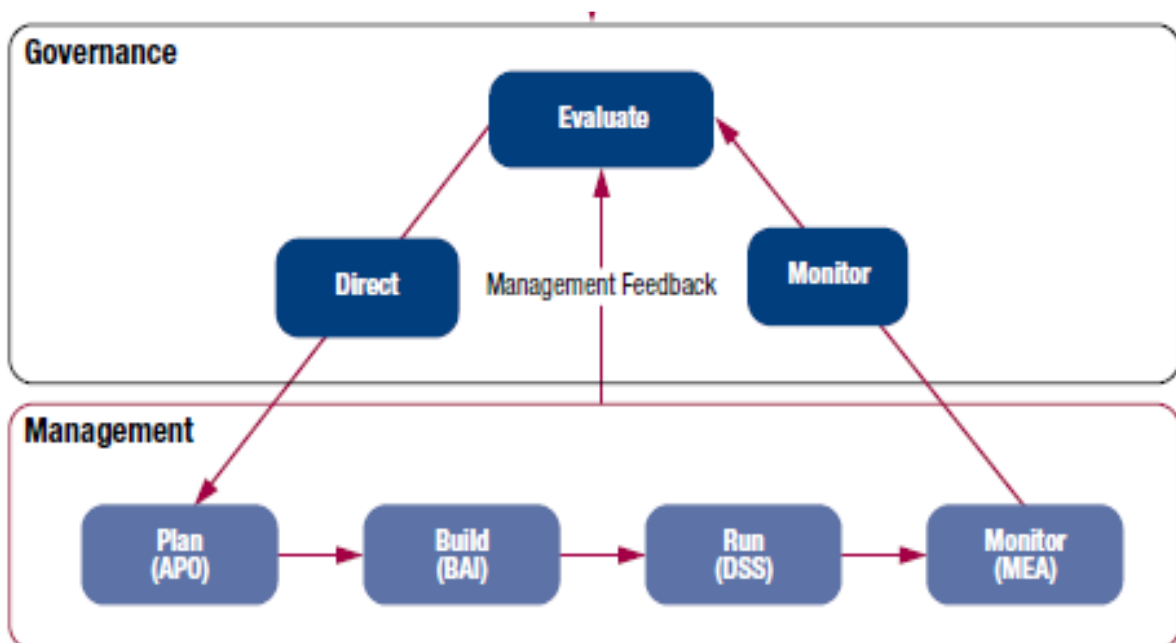


Figure 1-2: Governance and management key areas (Source: ISACA 2011: 32)

According to De Haes, Steven Vand an Grembergen (2013: 317) and ISACA (2011: 31), the EDM domain is the responsibility of the board of directors who ensures enterprise objectives by evaluating stakeholders' needs. The remaining four management domains focus on delivering the technological capabilities, services, assets and other resources that the business functions need to implement and sustain business change with the direction set by the governance body (ISACA 2012: 31). While there are no quick fixes for Enterprise Governance of Information and Technology (EGIT), the governing board and senior management have to oversee and tailor their EGIT measure and the implementation in their context and have to bring value to the organisation from digital transformation.

1.7.1 Brief background of COBIT framework

The COBIT framework's first version was released in 1996 to address an auditing outcome (Mourad et al. 2017: 41). COBIT 2 was released in 1998 to address control of processes. Management scope was included in COBIT version 3, which was released in the year 2000 (De Haes et al. 2013: 308). In 2005, COBIT version 4.0 was released to cover IT governance. Subsequent to that, COBIT 4.1 was released as an update to address Value of IT (Val IT) and IT risks (Risk IT) in 2008 and 2009, respectively. COBIT version 5 was released in 2012 to address the Governance of Enterprise IT (ISACA 2012). At the time of the study, the framework was in the 6th release, with COBIT 2019 as the latest edition, which integrates more than 25 years of development in the field, not only incorporating new insights from science, but also operationalising these insights as practice (ISACA 2018a: 9) (Figure 1-3).

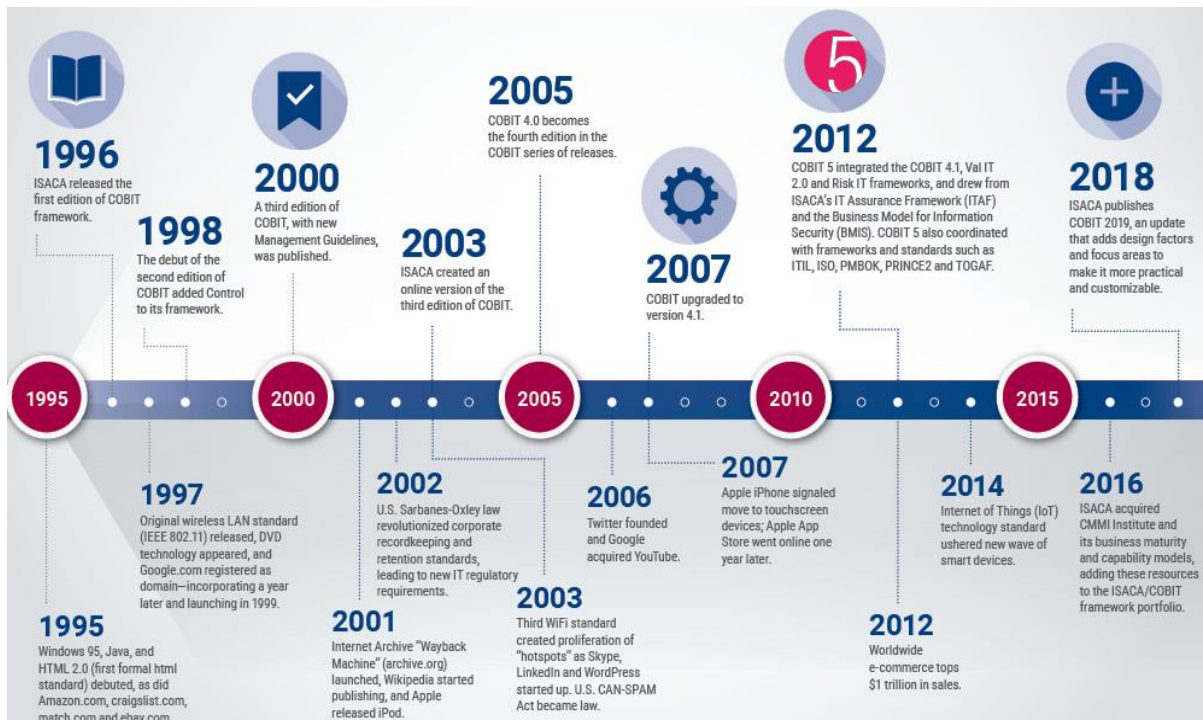


Figure 1-3: COBIT release timeline
 Source: ISACA (2018c)

The process mapping of COBIT 2019 that involves 40 processes, functions and activities as indicated in Figure 1-4. The COBIT core model guided the review of literature.

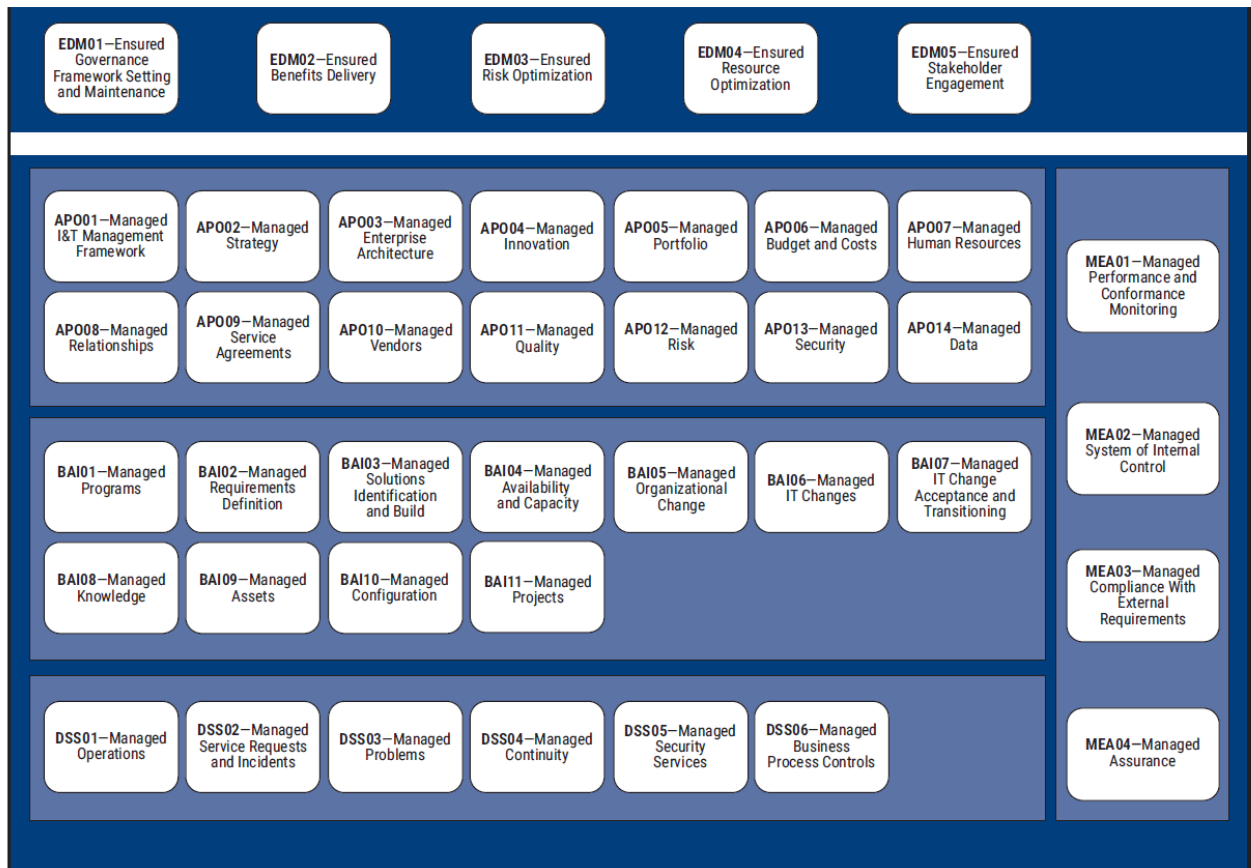


Figure 1-4: COBIT core model
(Source: (ISACA 2018a: 12)

The next section introduces the preliminary literature that was undertaken.

1.8 PRELIMINARY LITERATURE REVIEW

According to Creswell (2014: 28), a literature review provides a framework for establishing the importance of the study as well as a benchmark for comparing the results with other findings. Literature was reviewed as per the themes from objectives of the study. The themes were informed by the constructs from the theoretical framework.

1.8.1 Evaluate, direct and monitor

Ngoepe and Ngulube (2014: 3) state that information should form an integral part of organisational governance since it is regarded as an enabler of such business. A study

conducted by Chauke (2018b) at the Department of Transport in South Africa focused on the use of the COBIT framework where the strategies, processes, technological infrastructure and people were investigated. Mullon and Ngoepe (2019: 5) went a step further to outline that a holistic governance framework covers policy and legislation, technological infrastructure and people. The other benefit, as opined by Fitroh, Siregar and Rustamaji (2017: 2), is that the adoption of the COBIT framework would ensure efficient operations, decreased costs and the improvement of IT infrastructure control.

ISACA (2018a: 29) considers the EDM domain for the following:

- The provision of a consistent approach integrated and aligned with the enterprise governance approach.
- I&T-related decisions are made in line with the enterprise's strategies, objectives and desired value are realised.
- The I&T processes are overseen effectively and transparently.
- Legal, contractual and regulatory requirements are confirmed and the governance requirements for board members are met.

The next section addresses the overall organisation, strategy and supporting activities for I&T.

1.8.2 Align, plan and organise

The APO domain's role is to implement a consistent management approach for enterprise governance requirements to be met, covering governance components such as management processes; organisational structures; roles and responsibilities; reliable and repeatable activities; information items; policies and procedures; skills and competencies; culture and behaviour; and services, infrastructure and applications (ISACA 2018a: 55). Prior authors such as Mourad et al. (2017: 4) state the APO is a representation of the field of strategic dimension of I&T governance.

1.8.3 Build, acquire and implement

Mourad et al. (2017: 4) project the BAI domain as the identifier, developer and acquirer of IT solutions, their implementation and integration with business processes, and the updating and maintaining of existing systems. ISACA (2018a: 153) states that the realisation of desired business value and reduction of the risk of unexpected delays, costs and value erosion are important aspects. It further advises that improvement in communications to and involvement of business and end users would ensure the value and quality of programme deliverables and follow up of projects within the programmes, and maximise programme contribution to the investment portfolio.

1.8.4 Deliver service and support

The DSS domain is regarded as the description of the complete conditions of IT services supply (Mourad et al. 2017: 5). The purpose of the DSS, as indicated by ISACA (2018a: 231), is the delivery of I&T operational and service outcomes as per the plan.

1.8.5 Monitor, evaluate and assess

According to Mourad et al. (2017: 5), MEA looks at current deployed solutions throughout all domains and lifecycles with a view to improving them. The MEA domain provides transparency of performance and conformance, and drives the achievement of goals (ISACA 2018a: 273).

1.9 RESEARCH METHODOLOGY

The research methodology used in this study was PAR, as the project involved collaboration between the researcher and study participants in defining and solving the problem. In this study, all three the phases of PAR were followed, that is, the Look phase: getting to know stakeholders so that the problem is defined on their terms and the problem definition is reflective of the community context; the Think phase: interpretation and analysis of what was learned in the look phase; and the Act phase: planning, implementing, and evaluating, based on information collected and interpreted in the other phases (Stringer 2014).

The current study adopted a qualitative research approach which involved the collection of data through focus groups, observations, systems and document analysis in response to research questions (Creswell 2014: 139). The researcher was part of the exploratory meeting where challenges to information access were raised and permission was given for a system overhaul to take place with a view to maximising information efficiency and integration within the organisation (SACSSP 2018b). The study was conducted as per the research methodology roadmap highlighted in Figure 3-1 and the comprehensive discussion of the components of the methodology is provided in chapter three.

1.10 DEFINITION OF TERMS

Creswell and Creswell (2018: 40) explain that definition of terms ensures the removing of ambiguity and adding precision to words used, and it enables communication of the findings and ideas accurately. The key terms used in the study are information governance, corporate governance and IT governance.

Information governance

IG is defined as “the activities and technologies that people employ to maximize the value of their information while minimising associated risks and costs” (Information Governance Initiative 2018: 16). Mikalef, Boura, Lekakos and Krogstie (2020: 3) define information governance as “A collection of competences or practices for the creation, capture, valuation, storage, usage, control, archival, and the deletion of information and related resources over its life cycle.”

IT governance is “a set of policies and best practices that serves as strategic enabling force to improve enterprise business operations” (Moeller 2013: 4).

Corporate governance

According to the Institute of Directors in Southern Africa (IODSA 2016: 20), corporate governance is:

... 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.

1.11 ETHICAL CONSIDERATIONS

This study involved the gathering of information directly from human subjects by means of interviews about the development of a holistic information governance process framework at the South African Council for Social Service Professions (SACSSP). Participants were informed that they participated voluntarily and can withdraw from the interview process at any time. Data used in the study were sourced from the organisational reports and public domain. For the ethical issues that arose during the study, ethical clearance was requested as prescribed by the policy of the University of South Africa (Unisa). Further discussion of this is found in section 3.6.

1.12 CITATION MANAGEMENT AND REFERENCING METHOD

The study made use of Mendeley citation solution to manage the references. The electronic citation manager, Mendeley offer different citation styles. From the variation of 7000 citation style, a style chosen for the study is: University of South Africa – Harvard. For consistency, the Harvard method of referencing (Harvard format author(s) date: page) was used throughout this thesis where possible.

1.13 CHAPTER OUTLINE

This study is structured as follows:

Chapter one – Introduction and relevance of study

The chapter formed the basis by defining problems encountered by the study case, the SACSSP, due to the lack of a cogent IT system design and the disparaged IT systems inherited that are not compatible with new system innovations to ensure effective and efficient council operations. This chapter includes an introduction to the theoretical lens, COBIT 2019 and provides a preliminary discussion on the facts on the usage of it. It further presents the methodology that was used when conducting the study and addressing ethical considerations.

Chapter two – Literature review: An information governance system in support of corporate governance

This chapter presents a review of literature relating to information governance. It gives a better understanding of literature review on information governance processes frameworks and the theoretical frameworks in alignment of five domains and forty processes. This chapter applies COBIT framework to conduct literature that is relevant to the study.

Chapter three – Research methodology

The chapter discusses the detailed approach and design of tools that were employed for this study with specific reference to the selected population, sample and the measuring instrument to be developed. The chapter presents the procedures and methods undertaken by the researcher in conducting the study. The study discusses participatory action research project that involved collaboration between researchers and study participants in defining and solving the problem through needs assessment exercise that is alignment with the research methodology roadmap.

Chapter four – Presentation of results

The chapter presents the study case, the SACSSP, in the form of thematic analysis. The results of data collected from participants are presented in the form of themes, charts, tables and graphics to assess whether the research questions were adequately addressed and responded to as per the objectives of the study.

Chapter five – Discussions

The chapter contains the discussions of the findings, together with the interpretation and analysis of the responses. The study findings set a foundation for the information governance framework for the SACSSP and research's recommendations.

Chapter six – Conclusions and recommendations

The chapter gives the conclusions and the recommendations based on the research conducted. The study presents information governance system and proposes an IG system framework for SACSSP. The study evaluates the implications on theory and practice. The chapter provides a compass for future research.

1.14 SUMMARY

The purpose of this chapter introduced the reader to the broader research area of this study. This was achieved as introduction of the study and presented the reader with the background of the study. Next, problem statement was narrowed down. The purpose and objectives of the study for the title, *Facets of information governance system at the South African Council for Social Service Professions* was discussed, including the main objective and sub-objectives of this research.

The research questions and secondary questions that guided the study were indicated. The preliminary literature review and theoretical framework were also outlined. The author provided the justification and the scope of the study. Furthermore, the definition of terms used was given. The methodology selected was mentioned and the ethics that guide the research were explained.

The chapters of the study were decided on and, in the next chapter, the groundwork is expanded by reporting on the literature study conducted about the different aspects such information governance. The following chapter discusses the review literature in relation to the Information Governance and COBIT Framework, among other things.

CHAPTER TWO

LITERATURE REVIEW: AN INFORMATION GOVERNANCE SYSTEM IN SUPPORT OF CORPORATE GOVERNANCE

2.1 INTRODUCTION

The previous chapter laid the foundation by providing the background to the study, contextual and conceptual setting, theoretical framework, problem statement, research objectives and questions, originality of study, justification of the study, research methodology and the definition of key terms used in the study. The purpose of chapter two is to obtain a better understanding of the current research in a particular study area, including theories, phenomena and methods; and present it in a report format (Randolph 2009: 2). Having presented the background and purpose of the study in the previous chapter, it is appropriate to bring the reader up to date with the previous research that brought a focal point to the architectural facet of information governance, which includes the five domains of the COBIT 2019 framework known as: evaluate, direct and monitor (EDM); plan (APO); build (BAI); run (DSS), and monitor (MEA) which informed the objectives of the study and the literature review. This chapter presents the application of COBIT 2019. The discussion of the framework includes its relevance to IS research as well as to the study as well as literature review.

-

Table 2-1 indicates the linkage between the COBIT 2019 constructs and how they informed literature. The identified theoretical framework was discussed including their advantages and disadvantages, and thereafter applied to the study.

Table 2-1: COBIT 2019 framework and literature linkage

COBIT 2019 framework enablers	Literature themes
Evaluate, direct and monitor	2.2 Evaluate, direct and monitor
Plan (APO)	2.3 Align, plan and organise
Build (BAI)	2.4 Build, acquire and implement
Run (DSS)	2.5 Deliver, service and support
Monitor (MEA)	2.6 Monitor, evaluate and assess

2.2 EVALUATE, DIRECT AND MONITOR

The primary purpose of the board is to “steer the organisation and set its strategic direction, on the basis of which management will develop the strategy which is to be approved by the governing body” (Institute of Directors in Southern Africa (IODSA) 2016: 21).

Furthermore, the board must consider the following (ISACA 2018a: 29):

- The provision of a consistent approach integrated and aligned with the enterprise governance approach.
- I&T-related decisions are made in line with the enterprise’s strategies, objectives and desired value are realised.
- The I&T processes are overseen effectively and transparently.
- Legal, contractual and regulatory requirements are confirmed and the governance requirements for board members are met.

It is on that note that the King IV report is an important tool to be used by South African organisations to implement corporate governance principles and internal controls (Matsiliza 2017: 38). The role and responsibility of the board is depicted in Figure 2-1.

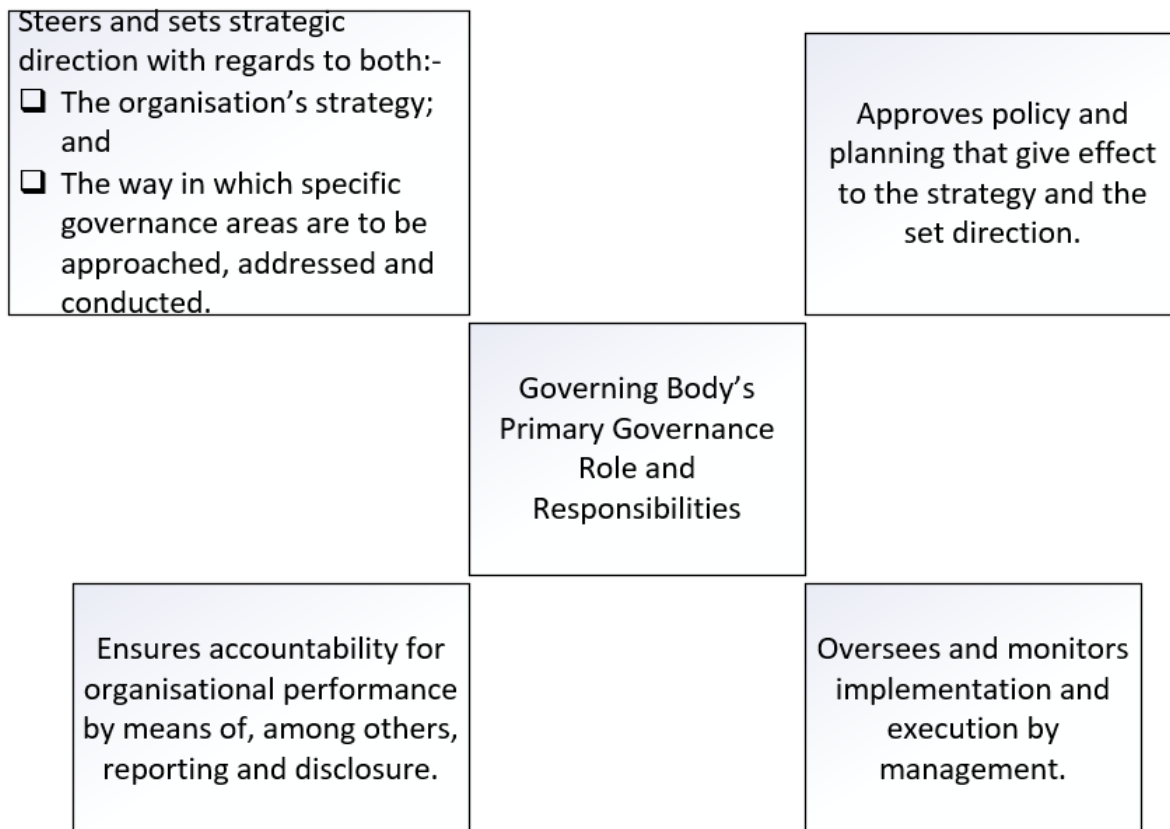


Figure 2-1: Role of the board and responsibilities
Source: (IODSA 2016: 21)

Organisations are not spared from the failures of oversight of corporate governance, where, in public sector organisations, this led to exacerbated shareholder interference, state bailouts, overall organisation under-performance, and board and CEO resignations, among other issues (Thabane & Snyman-Van Deventer 2018: 14). The results of a dysfunctional board at the South African Broadcasting Corporation (SABC) led to five governance transgressions having been committed, including bribery, fraud, corruption, tender rigging, environmental transgressions, and conflicts of interest (Thomas 2012: 463).

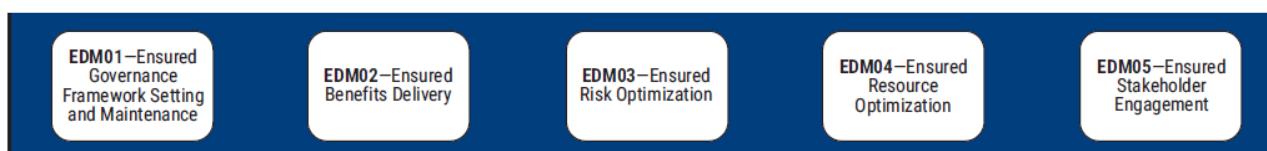


Figure 2-2: Evaluate, direct and monitor domain processes
(Source: ISACA 2018a: 12)

2.2.1 Governance framework setting and maintenance

According to Griffin, Phillips and Gully (2016: 72), the corporate governance framework is meant to provide, analyse and articulate the governance requirements of an organisation in an integrated and aligned manner by clarifying the authority and responsibility in order to achieve its mission, goals and objectives. Organisations are required to adopt corporate governance measures in order to restore confidence after a number of scandals caused a loss in confidence in markets (Stevens 2010: 1). Other pieces of legislation prescribe the principles of good governance through section three of the Co-operative Act of 2005 (RSA 2005: 14).

It is on that note a recommendation that the Department of Small Business Development in South Africa that closes a gap create by King Code of Good Governance, which is voluntary (RSA 2019b: 4). Zikopoulos, DeRoos, Parasuraman, Deutsch, Corrigan and Giles (2013: 216) outline that the purpose of the establishment of governance framework is to deliver trusted information. Merkus, Helms and Kusters (2019: 152) concluded that having a set of data definitions would assist those dealing with information governance to be able to remove chaos that may emerge from the amounts of data and information that are generated by an organisation.

One of the factors that assists in compiling an IG framework can be achieved if IT strategic matters are elevated to executive management level and can be supported by internationally accepted good practice and standards such as the King IV code of good governance, ISO 38500 standards for the corporate good governance and COBIT 2019, which is a governance I&T process framework (RSA 2012: 5; IODISA 2016). A study conducted by Chauke (2018: 262) concluded that organisations need to adopt key good corporate governance characteristics as set out in the Code of Corporate Practices and Conduct in the King IV report, supported by regulatory bodies that would ensure compliance.

2.2.2 Benefits delivery

The purpose of benefits delivery is that one can obtain desirable value from I&T capabilities, services and assets; secure affordable delivery of solutions and services, and obtain a constant and precise picture of overall costs and related benefits in order to support the needs of an organisation (Project Management Institute (PMI) 2017: 33). The executive authority must make sure that public organisations achieve its strategic mandate through the initiation of I&T-enabled investment programmes (RSA 2012: 16). The benefits that should be attained through strategy alignment are not only about automation, but also looks into strategic and competitive advantage from such a system (Valacich & Schneider 2018: 84). The adoption of an architecture alignment framework should guide the organisation-wide information solutions planning as discussed in section 2.4.3 (Kotusev 2019). Solutions identification should outline the benefits that are aligned to the organisation's strategic objectives because IT investments were found to not contribute significantly to transformation or service delivery of the South African government (RSA 2007: 3). There should be a governance mechanism that should balance the risks and benefits brought by I&T investments by optimising the core business so that it achieves its goals (Zhang & Zhou 2014: 8).

2.2.3 Risk optimisation

Risk optimisation ensures that I&T-related enterprise risk is managed so that it does not pass the threshold set in line with the risk to enterprise value arising from the use of I&T (ISACA 2018a: 41). RSA (2012: 16) advises that the executive management must ensure that ICT risks are managed and audited as per the organisational audit plan. The risk planning process involves conducting risk management planning, identification, analysis, response planning, response implementation and monitoring risk on a project (PMI 2017: 395). The organisation's board of directors, management and staff need to implement an enterprise risk management that would ensure the application in a strategy setting and throughout the organisation, designed to identify potential events that may affect the organisation and manage risk to be within its acceptable appetite and the provision of reasonable assurance in achieving an

organisation’s objectives (Aerts & Walton 2018: 448). A legal mandate set out in section 38 of the PFMA states that heads of institutions must ensure the establishment and maintenance of effective, efficient and transparent systems of risk management (RSA 1999: 36). All the risks evaluated and aggregated in section 2.3.12 are monitored by the audit committee for progress to enhance the management of risk. According to ISACA 2020 (14), enterprise risk, depicted in Figure 2-3, must be set and monitored at enterprise level to include strategic risk, environmental risk, market risk, operational risk and compliance risk in order not to lead to poor judgement or misrecognition of any risk.

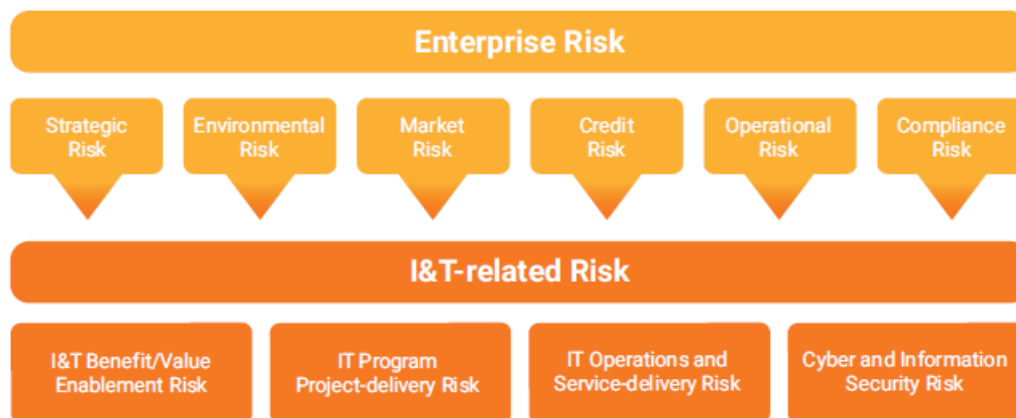


Figure 2-3: Scope of I&T-related risk relative to other major risks
Source: (ISACA 2020: 14)

2.2.4 Resource optimisation

Organisations are looking for sufficient resource optimisation with the main objective of completing the approved projects on time, within the allocated budget and not compromising the quality (Reddy, Nagaraju & Salman 2015: 240) (Figure 2-4). ISACA (2018a: 45) states that organisations should have sufficient and adequate organisation and I&T resources at their disposal to support the objectives of the enterprise.



Figure 2-4: Resource optimisation
Source: (PMI 2017)

In order to achieve the right balance in Figure 2-5, a resource optimisation technique such as resource levelling or resource smoothing is employed “to adjust the start and finish dates of activities to adjust planned resource use to be equal to or less than resource availability” (PMI 2017: 221). The main purpose of resource optimisation as highlighted in Figure 2-5 is the reduction of wastage of over-/under-allocation of resources (Reddy et al. 2015: 240).

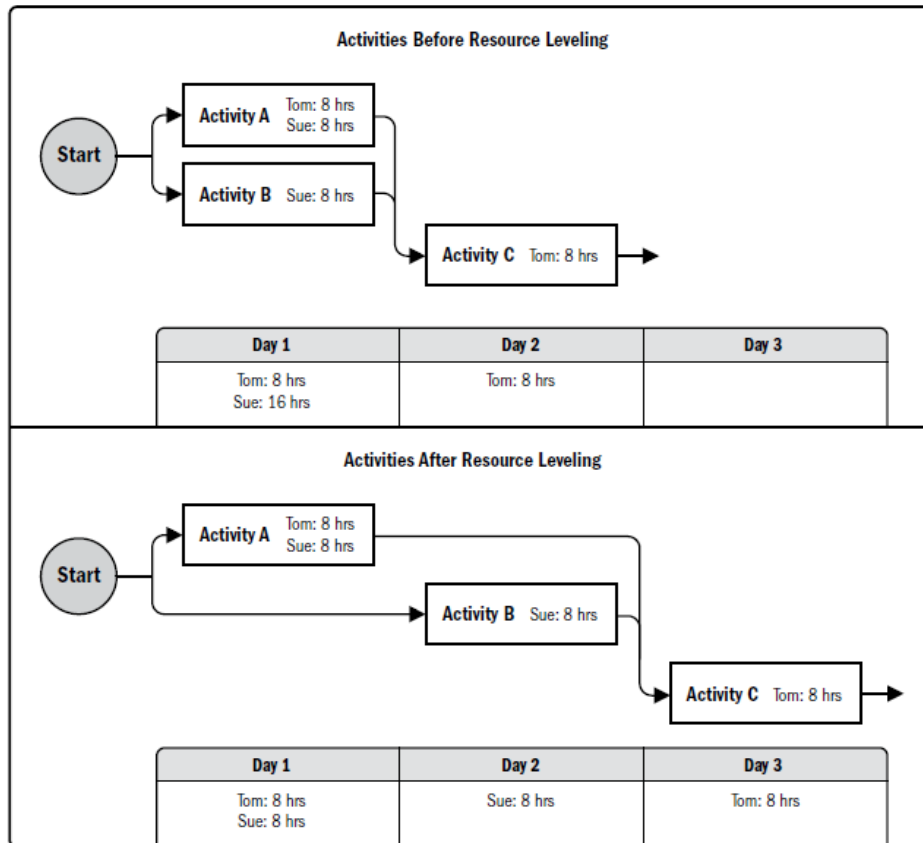


Figure 2-5: Resource levelling
Source: (PMI 2017: 212)

2.2.5 Stakeholder engagement

ISACA (2018a: 49) states that the purpose of stakeholder engagement is to ensure that all affected stakeholders are identified and consulted in the I&T governance system and that all the activities, such as I&T conformance measure and performance, are aligned to the set objectives and strategies, and transparently reported to the stakeholders. PMI 2017 (359) states that communication and reporting requirements include processes necessary to ensure that the information needs of the project and its stakeholders are met through the development or artefacts and implementation of activities designed to achieve effective information exchange.

The availability of communication technology systems such as email, audio conferencing, social media, web-based meetings and video-conferencing can greatly assist in ensuring that people who are not in the same geographical area or who have

mobility limitations or disabilities, are catered for (PMI 2017: 311). To ensure that the stakeholders have an established effective involvement in communication and reporting, the board should assess the effectiveness accuracy and reliability of mandatory reporting, while making sure that stakeholders’ requirements are met (ISACA 2018a: 50). Carrol and Buchholtz (2015: 73) point out that it is the organisation’s primary stakeholders’ objectives and profitability that must be met and ensured. IODSA (2016: 71) outlines the adoption of 16 stakeholder-inclusive approach principles that can be used as recommended practice for balancing the needs, interests and expectations of stakeholders for the benefit of an organisation over a period of time. In a study conducted by Huzzard (2021: 386), the following challenges were encountered due to a lack of / minimal stakeholder engagement: physical distance that led to stakeholder redundancy and incoherent updates on project activities.

2.3 ALIGN, PLAN AND ORGANISE

Mourad et al. (2017: 4) state that planning is a representation of the field of strategic dimension of I&T governance. The plan domain’s role is to implement a consistent management approach for enterprise governance requirements to be met, covering governance components such as management processes, organisational structures, roles and responsibilities, reliable and repeatable activities, information items, policies and procedures, skills and competencies, culture and behaviour, and services, infrastructure and applications (ISACA 2018a: 55). The planning domain has 14 processes that are discussed as depicted in Figure 2-6.

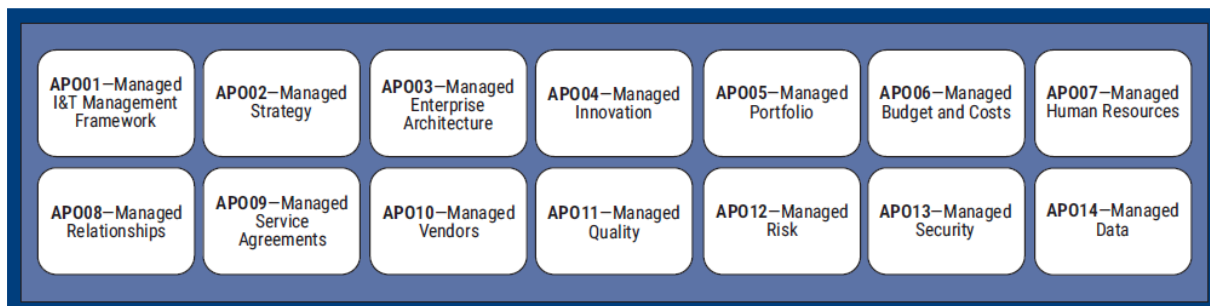


Figure 2-6: Plan domain processes
(Source: ISACA 2018a: 12)

2.3.1 Information and technology management framework

The I&T management ensures that there is a consistent management approach for the implementation of governance components such as roles and responsibilities; organisational structure; processes, policies and procedures; skills and competencies; culture and behaviour; and services, infrastructure and applications (ISACA 2018a: 55). The framework uses a demand management process to anticipate, plan for and manage the demand for I&T services while ensuring that capacity management meets the required demand of an organisation (Cabinet Office 2011a: 246). The I&T management framework process must be aligned with any applicable national and international governance and management standards and codes of practice and evaluate available good practices that are monitored in section 2.6 on pages 75 - 78.

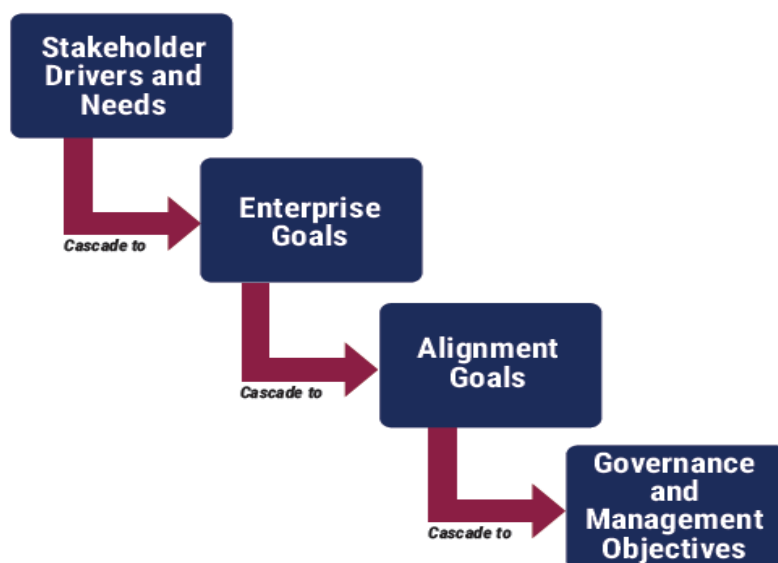


Figure 2-7: Goals cascade
Source: ISACA (2018b: 28)

The goal cascade discussed in the I&T management framework in the section have a bearing to the next section that discusses strategic management.

2.3.2 Strategic management

The Cabinet Office (2011: 134) defines strategy management as a way of prescribing and sustaining an organisation's perspective, position, plans and patterns with regard to its services and the management of those services. All the strategic requirements are packaged into a business case for a new system or hardware that is needed to execute the improved business process (Valacich & Schneider 2018: 374).

According to Ansoff, Kipley, Lewis, Helm-Stevens and Ansoff (2019: 12), strategic management is the holistic view of the current business environment, the proposed goals and steps required to reach the desired future. Gamble, Peteraf and Thompson (2017: 2) state that a company uses a strategy to explain why it matters in the marketplace by defining its application to generating utility and warranty for customers, and how competency and resources can be used to deliver value to customers. The South African government adopted a medium-term strategic planning framework (MTSF) to guide the state entities to identify important outcomes-oriented goals and objectives that are results based and can be measured and evaluated by oversight bodies (RSA 2010: 1). The strategy of the organisation is operationalised and budgeted for in sections 2.3.5 and 2.3.6, respectively.

2.3.3 Enterprise architecture

The enterprise architecture's purpose is to establish a common architecture that would create a glue that binds: business processes, information, data, application and technology architecture layers, and the development of re-usable building blocks components (Buckl & Schweda 2013: 239). The importance of enterprise architecture (EA) ensures that it manages innovation because it is critical for the survival of and success in an enterprise. The Open Group Architecture Framework (TOGAF) is chosen because it provides a detailed method and a set of supporting tools for developing an enterprise architecture (Sarno & Herdiyanti 2010: 145). According to The Open Group (2009: 6), it helps to optimise the fragmented legacy of manual and automated processes into an integrated environment that is responsive for the ever-changing business strategy.

TOGAF is a framework that advocates for placing data first in an organisation and that assists with a boundaryless information flow vision where systems can easily exchange information and use that information to improve the operations of the enterprise (The Open Group 2019: 2). The process was earlier defined as interoperability which leverages on the ability of information and software solutions to effortlessly create the capability to share, interact with and exchange information (Telesca, Rana & Ion 2007: 1; The Open Group 2018: 245).

According to Sarno and Herdiyanti (2010: 146), TOGAF consists of four architectural domains that are commonly accepted as subsets of an overall enterprise architecture, namely: business architecture – it defines the business strategy, governance, organisation, and key business processes; data architecture – the structure of the organisation’s logical data requirements that describe the existing state, definition of data requirements, and guide to data integration. According to Sarno and Herdiyanti (2010) and The Open Group (2018), there are interoperability requirements that identify integration requirements as multiple levels and information flows that are classified to indicate the extent of operability that would be needed between organisations and systems, as outlined in Table 2.2.

Table 2-2: Operability requirements

Source: The Open Group (2019)

Phase	Determination of interoperability
Architecture vision	The business scenarios capture the nature and security considerations of the information and services.
Business architecture	The information and service exchanges are further defined in business terms.
Data architecture	The organisation’s data and/or information exchange model details the content of the information exchanges.
Application architecture	It specifies the way the various applications must share the information exchanges.
Technology architecture	It specifies the appropriate technical mechanisms to permit the information and service exchanges.

Phase	Determination of interoperability
Opportunities phase	The selection of actual software solutions.
Migration planning	The logical implementation of the interoperability.

To give guidance to government entities in South Africa, the Government Wide Enterprise Architecture Framework (GWEA) which is based on TOGAF that was adopted to serve as a minimum standard which ICT plans, can be aligned with the business objectives and processes of such government entity (RSA 2009: 9).

2.3.4 Innovation

Innovative solutions are found when organisations adopt open innovation where many customer-generated ideas were requested and submitted to companies to be adopted and implemented (Valacich & Schneider 2018: 101). In a study conducted by Mhlungu, Chen and Alkema (2019: 7), the conclusion was that customers favour enterprises that provide digital offerings, which clearly shows that an organisation has the capability to respond the market. These initiatives brought a huge improvement in bringing innovative solutions to the market. Previously, universities and companies had research programmes that were complex and that involved bureaucratic processes that resulted the actual innovations becoming outdated and failing to reach the intended market (Valacich & Schneider 2018: 30). The world is littered with stories of organisations such as Kodak and Blackberry who lost out because they failed to innovate (Valacich & Schneider 2018: 553; Mui 2012). Ansoff et al. (2019: 30) highlight Nokia’s failures to compete due to a lack of innovation in products offering. In order to achieve innovative advantage, Keely, Walters, Pikkell and Quinn (2014) propose 10 types of innovation as indicated in Table 2-3.

Table 2-3: Ten types of innovation

(Source: Valacich & Schneider 2018: 99)

Innovation type	Description	Example
Profit model	Finding an unusual way of bringing about revenue from offerings.	Microsoft strategy of offering customers to adopt Office 365 on a subscription basis.
Network	Making use of competence and strength of others.	Discovery vitality using innovation for product offerings such as banking, gym, life cover and partnering with hotels and airlines.
Structure	Using the organisation's human resources and assets in innovative ways.	Google giving its employees 20% of their time to focus on their own projects.
Process	Changing of primary processes utilised to make a product of service.	The use of lean process by Toyota.
Product performance	Making of products or enhance existing through distinctness.	Coca-Cola's customisation of Coke's bottles.
Product system	Creation of the collection supporting offering.	Microsoft bundling of individual office programs into MS Office suite.
Service	Supporting and improving value of offering.	A philosophy of delivering excellent customer service.
Channel	Using of innovative ways to link offerings with customers.	Nespresso partnering with hotels and airlines.
Brand	Placement of the brand innovatively.	Virgin family of brands (airliner, fitness gyms and insurance services)
Customer engagement	Development of relevant relations with customers.	Apple tying customers to its ecosystem. Customers receiving a new phone every year.

2.3.4.1 Drivers of open innovation

Organisations that innovate are able to do things faster, better and cheaper than its competitors and, in the process, become more competitive (Valacich & Schneider 2018: 102). Email, audio and video-conferencing assisted in speeding up the flow of information and easing the task of coordinating and controlling business activities (Wild & Wild 2016: 42). Investing in intellectual capital would work in a shared-effort strategy through open source systems to produce large scale efficiencies (Maney, Hamm & O'Brien 2011: 192).

2.3.4.2 Blockchain technology

Blockchain technology was invented in 2008 as a measure to close a gap in the weaknesses identified in the financial system trust-based model (Nakamoto 2008: 1). A blockchain is a form of digital ledger consisting of 'blocks' of information, where each block contains a record of the transactions that occur within a distributed network (White & Brown 2016: 1). A blockchain network is an inexpungable and decentralised public ledger where transactions are added in blocks, serving as a proof of all transactions ever done (Valacich & Schneider 2018: 194). Any new block that is included as part of a blockchain mining process should satisfy specific rules that would make it suitable for storing in an unchangeable, yet tamper-proof manner (Fill & Haerer 2018: 4046). Nakamoto (2008: 2) proposes a digital time stamping of the transactions that are publicly announced, and the system participants agreed on a single history of the order in which they were received. In order to be achieved, Figure 2-7 details how the digital assets are transferred in the blockchain technology.

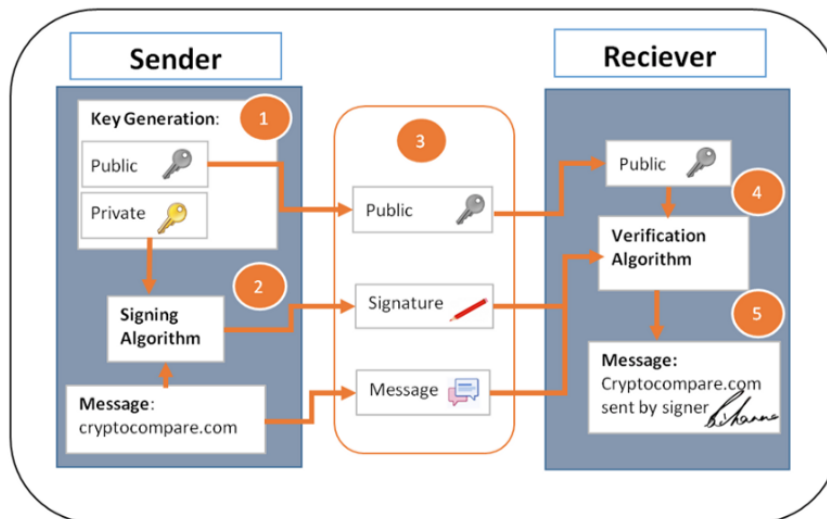


Figure 2-8: Blockchain transaction
(Source: CryptoCompare 2015)

White and Brown (2016: 2) opine that significant application of blockchain technology has been on cryptocurrency management, such as bitcoin. Blockchain technology has other areas of application such as secure registration of land rights, scans of signed contracts, digital photos, maps and similar objects (Taylor 2017: 5). Blockchain has been encoded in business processes that were adopted by Estonia and Sweden for the e-Estonia identity register and land registry systems, respectively. The United Nations (UN) has formed a blockchain coalition on climate change, while World Food Programme (WFP) and Australia Securities Exchange have not been left out for using blockchain to record shareholdings and management of transactions (Bauchere 2018).

Galiev, Prokopyev, Ishmukhametov, Stolov, Latypov and Vlasov (2019: 4) suggest the implementation of blockchain to archiving systems to consist of the following:

- Transaction timestamp
- Document creation timestamp
- Signature of the participant who created the document
- Document examination timestamp
- Signature of the participant who examined the document
- Signature of the participant who added the document to the archive

- Transaction data imprint

The following section, Internet of Things, describes physical objects with sensors, processing ability, data exchange with other technologies.

2.3.4.3 Internet of things

The Internet of Things (IoT) is the application of sensors and physical devices that are connected to automatically share data over the internet (Valacich & Schneider 2018: 41). After having been enabled by blockchain technology, IoT devices can participate in trust-free transactions, and contracts can be captured in computing codes to automatically perform the obligations that parties have committed to in an agreement (Sun, Yan & Zhang 2016: 3). Interoperability standards such as open data format (ODF) for IoT devices, machines, and web-based systems, ensure that information about things can be understood and exchanged in a standardised way among information systems (The Open Group 2019: 11). One of the implementations of IoT by the metropolitan police in the city of London added the live facial recognition system to their sensor collection to assist in spotting wanted persons walking through targeted areas (Gallagher 2020). Once the devices (sensors) have been connected, it becomes imperative to pay attention to the distribution of information collected among different organisational divisions and levels because it is the user who uses insights to perform functions to create value (Polzonetti & Sagratella 2018: 1481).

One of the sensors, the facial recognition system, is based on accessing human faces from several databases and shows variability in facial expression, resolution, pose, gender, age, lighting, background, and make-up among other facial attributes (Kak, Mustafa & Valente 2018: 164). However, there has been a growing resistance to the implemented facial recognition systems, which led to San Francisco public agencies banning the use of these systems due to tracking and monitoring that led to compromised civil rights (Andrejevic & Selwyn 2020: 3). As reflected in Figure 2-9 on page 39, activists in the United Kingdom painted their faces as a form of protest against mass surveillance (Tapper 2020).



Figure 2-9: Activists camouflaged against mass surveillance (Laney 2020)

2.3.4.4 Artificial intelligence

According to Muro, Whiton and Maxim (2019: 5), artificial intelligence (AI) “Involves programming computers to do things which – if done by humans – would be said to require “intelligence,” whether it be planning, learning, reasoning, problem-solving, perception, or prediction.”

The use of either automatic number-plate recognition (ANPR) and live facial recognition (LFR) technologies depends on diverse databases, and measures should be in place to protect people’s rights and privacy (Gallagher 2020). Most of the data that retailers collect from individuals through debit, credit or loyalty cards are enriched. The companies profile the person’s location and purchasing habits, and tailor offers to the person in the proximity of the same retailers based on previous buying habits (Zikopoulos et al. 2013: 8).

AI brought a critical advantage during the covid-19 pandemic, where updates and changes were displayed on an online interactive map for the world to see information about the virus in real time (John Hopkins University 2020) (Figure 2-10).

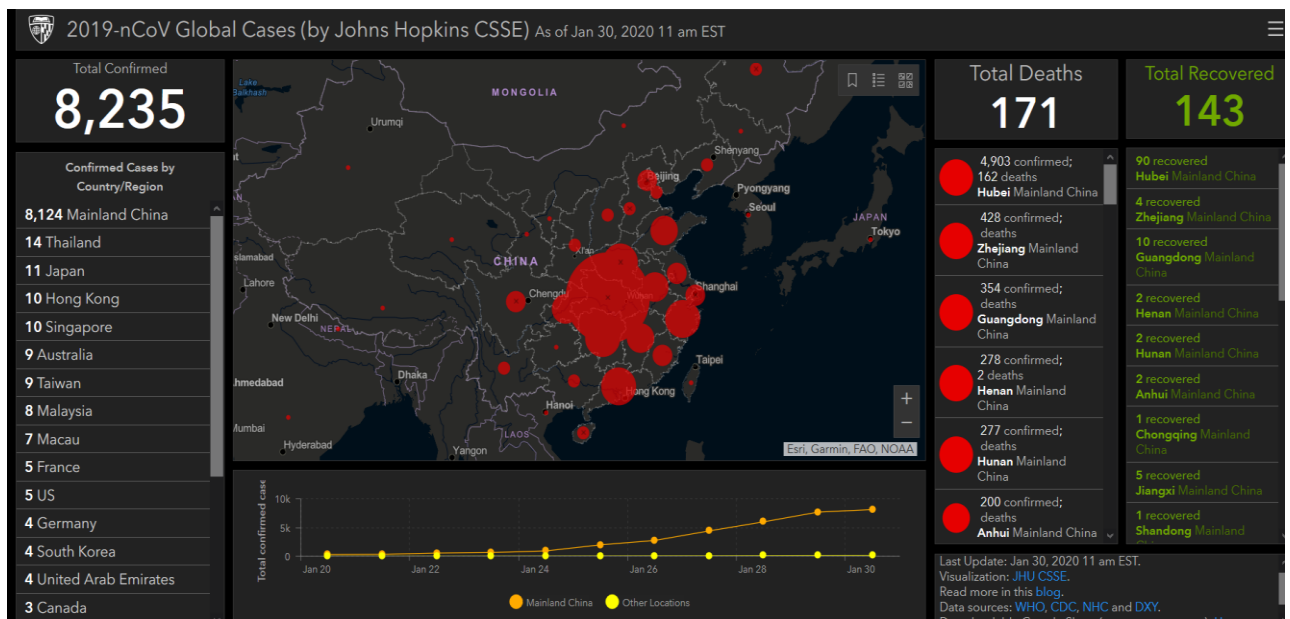


Figure 2-10: John Hopkins coronavirus interactive map Source (John Hopkins University 2020)

According to Andrew (2020), the interactive covid-19 dashboard collects data from the US Centre for Disease Control and Prevention (CDC), the World Health Organization (WHO), the European Centre for Disease Prevention and Control (ECDC), the Chinese Centre for Disease Control and Prevention, and the Chinese website DXY, which aggregates data from China's National Health Commission and the CCDC. Polzonetti and Sagratella (2018: 1481) contend that the AI real-time analysis has become one of the most useful technologies for the integration of knowledge gathered from the analysis of big data in support of an organisation's strategy.

While there are benefits of implementing AI, the US National Institute of Standards and Technology (NIST) found in a study conducted that most face recognition systems are returning a higher rate of false positives or discriminate against Asian and African-American faces over Caucasian faces (Grother, Ngan & Hanaoka 2019).

2.3.5 Portfolio management

The objective of portfolio management is to optimise the performance relating to the overall portfolio of programmes in response to a programme, product and service

performance and changing priorities, and demands in an enterprise (Ansoff et al. 2019: 198). The portfolio management process ensures that new proposals are evaluated, adopted and prioritised, while existing projects are expedited and resources granted to active projects (Aas, Breunig & Hydle 2017: 2). The service portfolio management and service catalogue management are used to determine service “offerings, identification of business needs, analysis of IT capabilities, documentation of the service catalogue and catalogue acceptance” (Mendes & Mira 2010: 4).

See Figure 2-11 for the development and maintenance of a service portfolio.



Figure 2-11: Service identification process
Source: (Mendes & Mira 2010: 4)

Figure 2-12 depicts what organisations need to manage their service portfolio with information related to the current service provided (service catalogue), past history of each service (retired services) and future service (service pipeline).

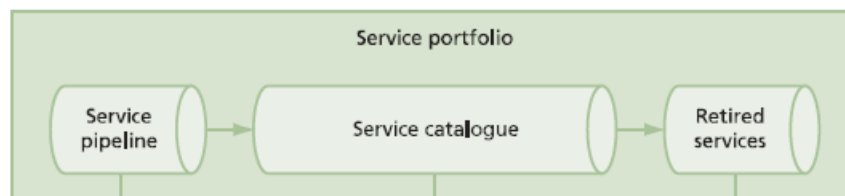


Figure 2-12: Service portfolio
Source: (The Cabinet Office 2011a: 173)

It is important that the organisation should make sound business decisions on I&T services contained in the approved business case and document the use and benefits when drafting organisational strategy. The selected portfolio that presents value to the organisation is costed in section 2.3.6.

2.3.6 Budgeting and costing

ISACA (2018a: 94) defines the budgeting and costing process as the creation of a partnership between key IT and enterprise stakeholders to provide transparency and accountability of the costs and value of solutions that the business would realise in order to make informed decisions in using the I&T solutions and services. RSA (2010: 48) relays that "...public entities must develop and maintain an appropriate procurement and provisioning system which is fair, equitable, transparent, competitive and cost-effective".

Accurate planning and forecasting of a budget needed to cover the cost of a service helps in recovering the usage costs of their service and maintaining profitability (The Cabinet Office 2011a: 204). It is also the responsibility of the executive management to monitor and evaluate the expenditure of ICT while ensuring that there is valid business-enabling reasons for the management of benefits, opportunities, costs and risks resulting from the expenditure, while ensuring that information assets are adequately managed (RSA 2012: 16). A budget planning cycle through the Expenditure of National Estimates (ENE) takes a period of 12 months, as indicated in Figure 2-13 (RSA 2019c: iii).

Month	ENE process
April	Departments prepare budget, including detailed spending plans for new proposals
May	
June	
July	Intergovernmental and technical forums
August	
September	Sector and focused budget hearings
October	
November	Departments revise medium term plans and finalise budget inputs
December	
January	
February	Strategic Plans tabled
March	

Figure 2-13: South African public sector budget cycle key milestones
Source: RSA (2019c: iii)

Public budgets are vulnerable to economic changes; however, other factors such as public outcry, natural disasters, political changes and disease outbreaks can derail a planned and approved budget (Shabalala 2005: 21).

2.3.7 Human resources management

Human resources management (HRM) makes provision for a structure to ensure optimisation / sourcing, planning, evaluation and development of talent needed to support enterprise objectives that are as productive as possible (Wild & Wild 2016: 476). Due to the emergence of the new roles in digital transformation, information and communication technologies, and software engineering, organisations moved to the adoption of a common reference model called the Skills Framework for the information

Age (SFIA) to find flexibility and fit in seamlessly with the organisation’s established ways of working, as highlighted in Figure 2-14 (SFIA Foundation 2019). The SFIA framework defines job families and position descriptions, structure, staffing, promotion and remuneration decisions of ICT professionals or digital delivery teams (Von Konsky, Miller & Jones 2016: 37).

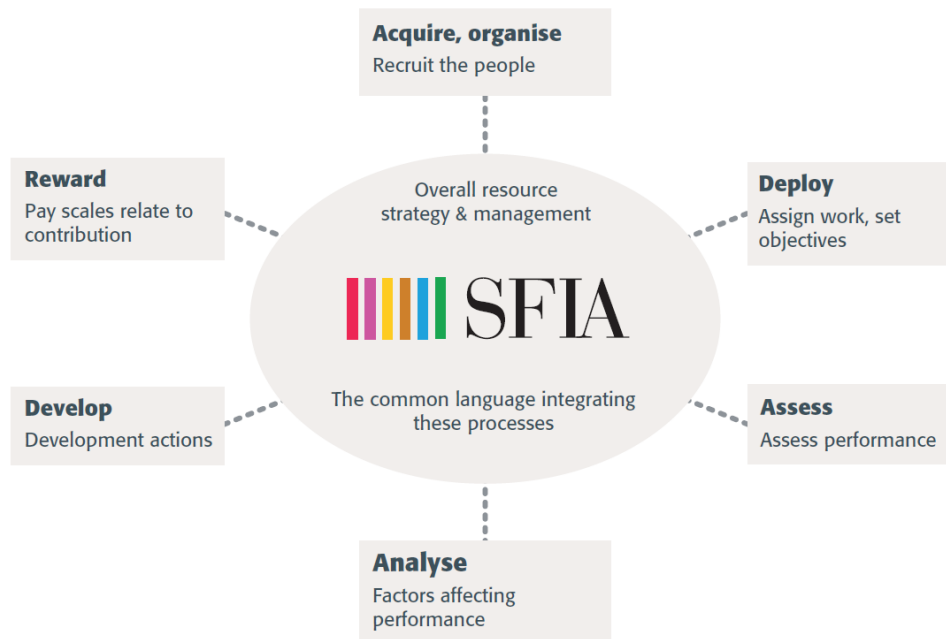


Figure 2-14: Skills management cycle
Source: (SFIA Foundation 2019)

The Australian government started a transformation initiative to better skill its employees in support of digital transformation by making government services easier to access and faster to use (Australia Public Service Commission 2019). However, there have been challenges and critical issues of acquiring skills in order for organisations to continuously create innovative services and products through the analysis of data (Polzonetti & Sagratella 2018: 1480). There has been a growing trend towards new employment relations for highly skilled knowledge workers for the skills they have through outsourcing work that cannot be done within the organisation (Griffin et al. 2016: 72). However, for an organisation to gain competitive advantage over its competitors, it must have resources and capabilities such as innovation, agility and quality that help to pursue the organisational strategy (Valacich & Schneider 2018: 86). On the negative side, Osipov (2019: 112) laments that professions such as

accountants, statisticians, loan managers, journalists, bank clerks, call centre operators, couriers, security guards and trainers will disappear from the market by 2030.

2.3.8 Relationship management

ISACA (2018a: 107) outlines the objective of relationship management (RM) is to enable the right knowledge, skills and behaviours that ensure mutual trust with a focus of achieving the strategic goals and having a transparent relation with business stakeholders. The Cabinet Office (2011b: 95) states that RM provides a plan domain with intelligence and information regarding the outcomes, customer needs and priorities required by the customer and serves as an interface with the customer at strategic level. Relationship management is coordinated by the business relationship manager whose role is to coordinate appropriate responses to customers; marketing, selling and delivery of services; and maintaining relationships throughout the activity's lifecycle. Motii and Semma (2017: 52) advise that RM's main concern should be customer focused and not technology focused; it should rather meet the functionality need of the customer in the most realistic and favourable way.

2.3.9 Service level agreements

The service level agreement (SLA) process is to align I&T solutions and service levels with enterprise requirements, including the related agreements that state the monitoring of such I&T solutions, service levels and performance indicators (ISACA 2018a: 113). The service level management (SLM) function provides consistency to the business on agreed service targets and the required information management to ensure that the targets are met (The Cabinet Office 2011b: 107). This process ensures that organisations can define, document, agree, measure, report and are able to review the quality of services rendered (Mendes & Mira 2010: 3). Such I&T services are specified in the portfolio of the organisation.

2.3.10 Vendors management

Vendor management involves the management of all the vendors if I&T related products and services are delivered as per I&T strategy, including procurement, selection and monitoring of contracts and performance (ISACA 2018a: 119). Vendor management “allows an institution to select its suppliers carefully and negotiate the best prices for the goods and services that it needs” (RSA 2015: 17). In order for the vendors selected to do business with South African government and its agencies, they have to register with the National Treasury’s central supplier database (CSD) (RSA 2020a). Vendor management should determine the selection of a vendor based on prioritising customers’ needs by devising a scoring system for each criterion and benchmarking the results as described when developing a business case (Valacich & Schneider 2018: 405).

2.3.11 Quality management

ISACA (2018a: 125) outlines the definition and communication of quality requirements of all the processes and procedures of the enterprises, to the satisfaction of the stakeholders. The process helps to identify quality requirements and/or standards and its deliverables and documenting how it demonstrates compliance with quality requirements and/or standards (PMI 2017: 277). The quality of services provided is determined by the customer based on whether their needs were met (Motii & Semma 2017: 53).

Enterprises should ensure that the sources of their data are quality checked before being analysed (Zikopoulos et al. 2013: 228). According to Heim (2020), the US National Archives altered images of the women’s march that was critical to US President, Donald Trump, which is concerning regarding the quality of data presented to unsuspecting public consuming this information. The process involved blurring, editing and digitally altering the images, thereby erasing something that was accurately captured by camera. The same happened to a young climate activist, Vanessa Nakate from Uganda (Nakate 2020), who tweeted that she was cropped out of a group photo taken at World Economic Forum (WEF) in Davos 2020. When she

complained about the omission, the altered photo was removed and the original picture was published (Dahir 2020) (Table 2-4). The original intent with the digitisation of records was to improve access and this is evident in the increased access on access to online museums and libraries (Borgman 2003: 64).

Table 2-4: Data quality implications

Original picture



Source: Tama (2017)

Altered version



Source: Georges (2020)

Original picture



Source: Associated Press (2020)

Altered version



Source: Associated Press (2020)

A data quality assessment approach that must be adopted by organisations dictates that data should be explored, transformed, prepared, and cleansed before the application of algorithms (Polzonetti & Sagratella 2018: 1481).

The components that are needed in data quality assessment are indicated in Table 2-5 to ensure cleanliness and accuracy of information.

Table 2-5: Data quality components

Source: Zikopoulos et al. (2013: 228)

Component	Component explanation
Parsing	Separation of data and parsing it into structured format
Standardisation	Determination of the placement of data in a certain field and ensuring its storage in standardised format
Validation	Ensuring the consistency of data against the pre-set validation rules
Verification	It involves checking of data against a source of verified information
Matching	It identifies duplicate records and merging those records correctly

The data quality challenges, technological issues, natural disasters and risk mitigation, are dealt with in the risk management.

2.3.12 Risk management

Risk management is referred as a process of conducting risk management planning, identification, analysis, response planning, response implementation, and monitoring risk on a project (PMI 2017: 395). According to Aerts & Walton (2018: 448) a good risk management "... provides the means for central management to effectively deal with uncertainty and associated opportunities, with ultimate goal of achieving the company's objectives."

ISACA (2018a: 131) places more emphasis of the integration of I&T-related enterprise risk within the tolerance threshold set by management. According to ISACA (2020: 46), it enables management to distinguish, evaluate and select appropriate responses in showing broad processes for selecting and prioritising risk response.

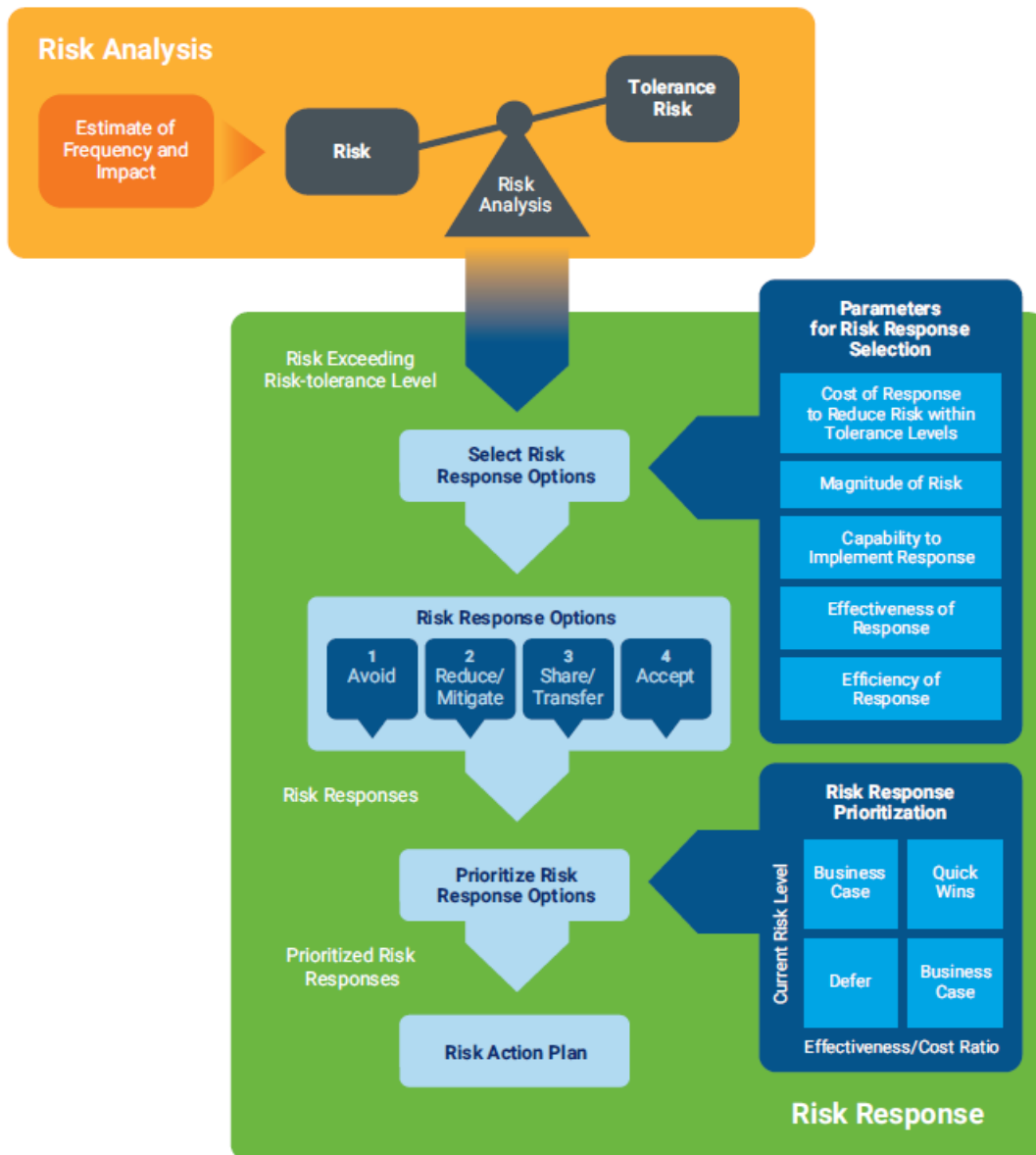


Figure 2-15: Risk response plan
Source: (ISACA 2020: 46)

While organisations relied on traditional security systems for protection, smart working through the use of combined professional and personal digital lives has broken down the enterprise security perimeter that was used as a defence mechanism (Polzonetti & Sagratella 2018: 1483). Organisations are moving from owning IT infrastructure to

using cloud services, which poses the risk of over-reliance to external resources, a lack of privacy and loss of data (Mosweu, Luthuli & Mosweu 2019: 7).

2.3.13 Security management

ISACA (2018a: 139) describes security management (SM) as a definition, operation and monitoring of information security incidents while taking care of the impact and occurrences within the enterprise. The cyber security occurrences necessitated the adoption of the National Cybersecurity Policy Framework (NCPF) by the South African government with the aim of coordinating and countering the increase in cybercrimes (Gwala 2016: 15). The framework's intention is "... to implement an all-encompassing approach pertaining to all the role players (State, public, private sector, civil society and special interest groups) in relation to Cybersecurity."

South Africa is in the top three countries that are targeted for phishing purposes (RSA 2015b: 77). The Cybersecurity Hub is South Africa's National Computer Security Incident Response Team (CSIRT) that has been established to be a coordinating point for all cybersecurity threats such as phishing, malware and software vulnerabilities that need to be reported (RSA 2020b).

ISO/IEC 27002:2013 provides the following guiding principles that include best practices and legal requirements (Motii & Semma 2017: 53):

- Information security policy
- Allocation of responsibility for Information security (IS)
- Escalation of problems
- Business continuity management

Protection and non-disclosure of personal data are significant for how organisations gather, save, utilise and disseminate personal information under their control (De Bruyn 2014: 1316). Security of data is further compromised when data are hosted in the cloud, because the organisations no longer have control over the data or where data are hosted (Mosweu et al. 2019: 7). Organisations implement Virtual Private

Networks (VPNs) and firewalls to protect their data stored on the internet and in their internal network (Jingyao, Chandel, Yunnan & Jingji 2020: 1051).

Some of the initiatives that are being advocated is the move from perimeter defence systems to the application of more sophisticated solutions such as a data-centric approach based on data flows and risk analysis, since devices are infected by ransomware that limits access to information on those devices (Polzonetti & Sagratella 2018: 1483). Ali (2017: 89) defines ransomware as

...a type of malware that encrypts a victim's files and subsequently demands payment in return for the key that can decrypt said files. When ransomware is first installed on a victim's' machine, it will typically target sensitive files such as important financial data, business records, databases, personal files, and more...

Once a user experiences an attack, as indicated in the ransomware screen variant in Figure 2-15, their computer would be locked and their intellectual property inaccessible (Simoiu, Gates, Bonneau & Goel 2019: 4).



Figure 2-16: Ransomware screenshot
Source: (Simoiu et al. 2019: 4)

Organisations need to protect their IP rights such as trade secrets from commercial exploitation and thereby give themselves a technical advantage over its competitors

(Patino 2009: 138). One solution to achieve this is to implement good sophisticated solutions to act as a prevention front and to limit attacks that may deny services and applications the ability to operate optimally (Polzonetti & Sagratella 2018: 1483).

2.3.14 Data management

Data management is regarded as achievement and sustenance of “effective management of the enterprise data assets across the data life cycle, from creation through delivery, maintenance and archiving” (ISACA 2018a: 143).

Data embedded in paper records have been accumulated and preserved for decades by public institutions, which made it difficult for organisations to digitise legacy documents to support data-driven decision making (Brown & Toze 2017: 587). This data will become inaccessible because of degradation of storage media or because of obsolescence of the hardware and software used to create them (Borgman 2003: 230). Han, Kamber and Pei (2012: 5) point out the challenges encountered by organisations with accumulated large deposits of data in their databases known as big data. Gartner (2012) defines big data as “high-volume, high-velocity or high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight, decision making and process optimisation”.

Walker and Brown (2019: 1) state that big data has three characteristics, namely: volume, which is regarded as a large amount of data; velocity, which refers to the speed of data creation; transfer; and variety, which refers to different types of data collected. However, there is a serious challenge with analysing large amounts of data when an organisation tries to harness big data for making business decisions (Valacich & Schneider 2018: 43). Other researchers worked on “deep learning” to address the same challenge of computing machines to self-learn, unassisted in support of cognitive computing that is used for big data exploration applications for help desk services such as automation (Polzonetti & Sagratella 2018: 1481).

Once data have been processed, the contents need to be described and organised in such a way that it facilitates access through metadata (Borgman 2003: 68). Metadata are “...the information and documentation which makes data understandable and shareable for users over time. Data remains usable, shareable and understandable as long as the metadata remains accessible” (ISO 2015).

Metadata provide the link between organisational requirement (policy) and information or data value (RSA 2019a: 2) (Figure 2-17).

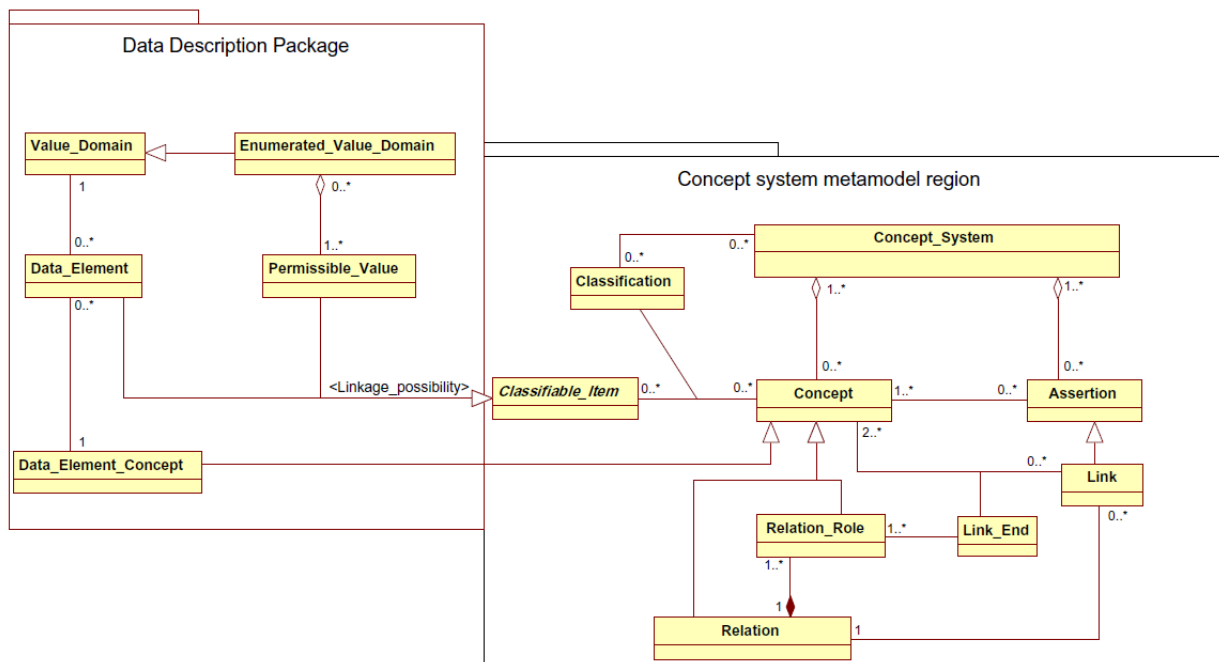


Figure 2-17: Data linkage possibilities
Source: (ISO 2015)

Data cleansing can happen when data are transferred between systems, where document plans should be utilised with all record content and its associated metadata in the originating system should be retained until the cleansing process is concluded and the reliability of the destination system has been controlled and secured (ISO 2016: 18).

One of the challenges experienced with data growth is the impact it has on existing systems since such growth leads to the high cost of maintenance and applications

performing poorly (Zikopoulos et al. 2013: 230). The legislation that is governing proper management and care of the records of government agencies in South Africa is the National Archives and Record Service (NARS), which guides the transfer, erasure, destroying and disposal of records (RSA 2001: 13). Poole (2016: 2) explains the process called digital curation, which embraces the digital preservation, data curatorship and the management of data assets through their lifecycle. Whenever records are converted from analogue to digital, it should be documented and communicated to all affected stakeholders (ISO 2016: 18).

Due to regulatory and audit requirements, data need to be stored for a specific period and made available when required (Cabinet Office 2011c: 138). Regulatory Acts such as the Sarbanes-Oxley Act ratify the archiving of organisational documents, internal communication, emails and instant messages (Valacich & Schneider 2018: 131). ISO (2016: 17) prescribes that all data records should be stored in a way that protects them from unauthorised access, change, loss or destruction, including theft and disaster, by ensuring that there is an appropriate storage environment and media. Ngulube, Ngoepe, Saurombe and Chaterera (2017: 76) echo the need for an archives repository to contain relevant records that can be consulted to fulfil people's requests. Digital preservation of information encounters challenges such as technology and the solutions proposed becoming obsolete, and the migration, emulation and maintenance of digital museums that are said to be expensive (Borgman 2003: 66). The use of cloud technology ensures that digitised data, information and records are always available because they are backed up on a number of computing storage devices, which increases the possibility of data availability and retention (Mosweu et al. 2019: 2).

2.4 BUILD, ACQUIRE AND IMPLEMENT

ISACA (2018a: 153) mentions the realisation of desired business value and reduction of the risk of unexpected delays, costs and value erosion as important aspects. They also advise that improvement in communications to and involvement of business and end users would ensure the value and quality of programme deliverables and the follow-up of projects within the programmes, and would also maximise programme contribution to the investment portfolio. Mourad et al. (2017: 4) state that the build

domain is the identifier, developer and acquirer of IT solutions, their implementation and integration with business processes, and updating and maintaining of existing systems. Figure 2-18 depicts 11 build processes.

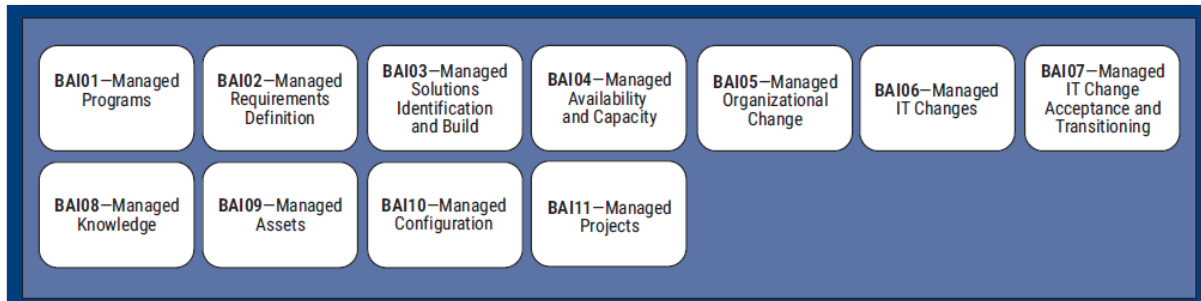


Figure 2-18: Build, acquire and implement domain processes
Source: (ISACA 2018a: 12)

2.4.1 Programme management

Programme management involves the realisation of the desired business value from the portfolio of investments while there is a mitigation of risks of unexpected delays by involving the business and end users (ISACA 2018a: 153). Programme management ensures that the activities of I&T are well coordinated to create a comprehensive and appropriate design that will support the achievement of the required business outcomes as agreed upon in sections 2.3.2 and 2.3.5. Programme management focuses on the linkages between projects, and between projects and programmes to establish the most appropriate approach to managing them (PMI 2017: 12).

2.4.2 Requirements definition

The process deals with the identification of requirements and proposed solutions to be used to meet the needs of an enterprise (ISACA 2018a: 163). Transformation of requirements into I&T services is the foundation of IT service management and without it, an organisation would be considered a cluster of resources that does not bring value to the business (Mendes & Mira 2010: 2). Value is realised by setting SLAs, operational level agreements customer satisfaction standards and agreed service

improvement plans that will be effected for the service level agreements designed in section 2.4.9 on page 63.

2.4.3 Solutions identification and build

ISACA (2018a: 169) outlines the process to ensure the agility and scalability in the delivery of digital products and services in a timely and cost-effective manner that involves technology, business processes and workflows that are capable of supporting the enterprise and its operational objectives. Products and services needed include hardware and software, which forms part of the organisational information infrastructure (Valacich & Schneider 2018: 129). Companies adopt a hybrid infrastructure to benefit from the flexibility and scalability required to support a data-driven environment (Polzonetti & Sagratella 2018: 1481). Table 2-6 gives the different models that organisations can adopt for their sourcing needs. While there are benefits to the use of cloud services, low bandwidth and cost of access to these services have been a challenge in Botswana, Namibia and South Africa (Mosweu et al. 2019: 2).

Table 2-6: Solution sourcing model

Sourcing model	Sourcing definition
Insourcing	An organisation providing its own resources and service
Outsourcing	An organisation contracting in I&T services from a third party
Cloud	An organisation making use of a cloud service provider to provide I&T services
Hybrid	An organisation using a combination of sourcing models for provision of I&T services to a certain degree.

(Source: (ISACA 2018b: 26; The Cabinet Office 2011b: 77)

Larger organisations opt for custom-developed applications based on a specific problem using methodologies such as Agile and DevOps. The other approach of building systems is software development life cycle (SDLC), which must be used when

requirements are highly structured and straightforward (Valacich & Schneider 2018: 399).

2.4.4 Availability and capacity management

Availability and capacity management (ACM) is the assessment of the current trends and future needs for the availability, performance and capacity of the service provided, which includes forecasting of the future enterprise requirements (ISACA 2018a: 181). ACM depends on strategic management (section 2.3.2 on page 31), SLA and the requirements defined. The Cabinet Office (2011b: 125) indicates that the availability of management defines, analyses, plans, measures, and improves all the aspects of the availability of IT infrastructure, processes, tools, and roles, among others things, that are appropriate for the agreed upon availability-related matters, relating to both services and resources, ensuring that availability targets in all areas are measured and achieved (Figure 2-18). Sawhney, Raisinghani and Idemudia (2018: 445446) and National Archives and Records Administration (2019), note the alarming statistics recorded by NARA that the degree to which a system was not operational and accessible when it was required, was 93% among businesses that had lost availability in their data centre for 10 days or more, which contributed to that business filing for business rescue within one year.

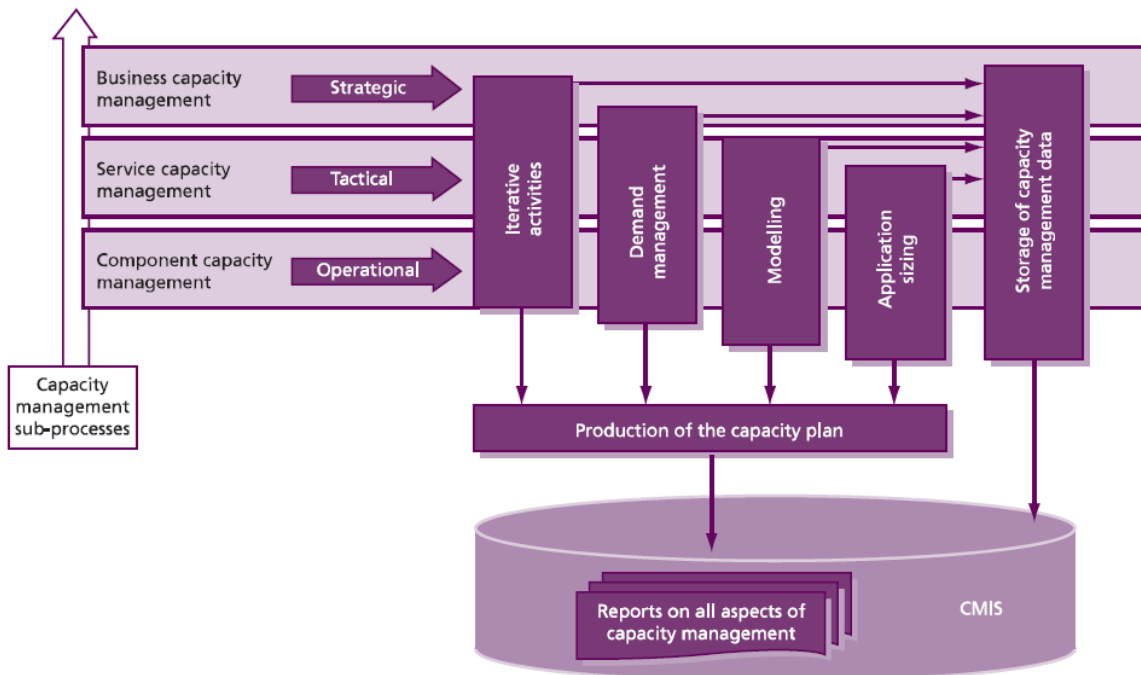


Figure 2-19: Capacity management process
 Source: (The Cabinet Office 2011b: 162)

2.4.5 Organisational change management

According to ISACA (2018a: 187), the organisational change management (OCM) process involves the preparation and commitment of all affected stakeholders in relation to the pending business change and the reduction of the risk of failure. Griffin et al. (2016: 554) explain that there are different forces for change, where people are the major force affecting organisations. The pressures category, examples and types are mentioned in Table 2-7.

Table 2-7: Pressures for organisation change

Source: (Griffin et al. 2016: 555)

Pressure category	Example	Pressure type for change
People	Generation X, Y, millennials Global labour suppliers Senior citizens Workforce diversity	Demands for different ways of training, benefits, workplace arrangements and compensation systems
Technology	Manufacturing in space Internet Global design systems	More education and training for workers at all levels, more new products, products move faster to the market
Information processing and communication	Computer, satellite communications Global sourcing Videoconferencing Social networking	Faster reaction times, immediate responses to questions, new products, different office arrangements, telecommuting, marketing, advertising, recruiting on social networking sites
Competition	Global markets International trade agreements Emerging nations	Global competition, more competing products with more features and options, lower costs, higher quality

One of the challenges to the availability of most research from developed countries is that it does not apply to the developing countries due to cultural differences and the fact that it focuses on technological and operational features rather than on human, managerial and strategic factors (Serumaga-Zake 2017: 1). Organisational culture is a system of shared assumptions, values and beliefs which governs how people behave in organisations (Mclaughlin 2017: 1). Thompson, Peteraf, Gamble and Strickland (2020) define organisational culture as “The character of a company’s internal work climate and personality as shaped by its core values, beliefs, business principles, traditions, ingrained behaviours, work practices and style of operating”.

Du Plessis and Mabunda (2016: 55) advise organisations to avoid a big bang approach and rather follow a phased approach when introducing change so that barriers can be overcome. Trust is an important cultural element that strengthens the

relationships that form part of cultural elements (Baskerville & Dulipovici 2006: 91). Any change that is introduced to any organisation presents difficulties and, therefore, leaders are encouraged to evaluate the preparedness of their organisation to adopt those changes in advance (Jalaldeen, Karim & Mohamed 2009: 128). RSA (2012: 16) cautions executive managements to ensure that any I&T service delivery is sensitive to organisational behaviour/culture. The intention of any change is not to extremely change the organisational culture, but to tailor the behaviour of people in a manner that suits the demands in the context of the organisation in the same way that the strategy needs to be compatible with the organisational culture (Sunassee & Sewry 2002: 240). Baskerville and Dulipovici (2006: 91) present organisational culture as a mesh of several elements: paradigm, symbols, power structures, organisational structures, control systems, routines, rituals and myths. These elements are said to coincide, converge and even support each other.

Yiua, Sankatb and Punc (2013) outline that knowledge often becomes embedded not only in documents or repositories, but also in organisational traditions, procedures, practices and standards. Factors such as communication, management support, change management, emotions, attitudes to computer information systems and the project management approach affect the adoption of the electronic document management system (EDMS) in New Zealand (Mosweu, Bwalya & Mutshewa 2016). The disclosure exemplifies that organisational culture, best practices, core competencies, expertise and strategic vision are critical parts of the total stock of knowledge in an organisation. Wowczko (2016: 1110) opines that culture is a determination of conditions under which organisations exist and the values held and promoted through their daily workings.

2.4.6 IT change management

The purpose of IT change management (ITCM) is to serve as a control measuring tool for all the standard and emergency changes relating to business processes, applications and infrastructure while maintaining the integrity of the changed environment (ISACA 2018a: 193). The change management process is responsible

for controlling the lifecycle of all changes, enabling beneficial changes with minimum disruption to IT services (Axelos 2020a: 92).

2.4.7 IT change acceptance and transitioning management

This process outlines the implementation planning, system and data conversion, communication or changed business processes and I&T services, early support and post-implementation review (ISACA 2018a: 197). One of the change business processes is to perform transition planning and support, which decommission the current way of operating and prepare for the installation of a new solution together with the provision of training and an early system support (Valacich & Schneider 2018: 396). The following process ensures that a data migration tool is needed for transition to a new system by applying data cleansing to allow transformation such as replacing missing strings. Data auditing tools will find discrepancies that violate conditions by analysis to discover rules and relationships. Manual intervention is needed for data referencing of external sources (Han et al. 2012: 92).

Release and deployment management ensures that a release unit (hardware or software) is released based on "... plan, schedule and control the build, test and deployment of releases, and to deliver new functionality required by the business while protecting the integrity of existing services" (The Cabinet Office 2011d: 114).

Service validation and testing are done as per the utility and warranty specified in the strategy objectives and requirements processes indicated in sections 2.3.2 on page 31 and 2.3.5 on page 40, respectively. The change evaluation report, based on validation and testing of the new system, ensures that the implementation plan was evaluated and predicted against the actual performance (The Cabinet Office 2011d: 175).

2.4.8 Knowledge management

The management of knowledge requires the maintenance of relevant, current, validated and reliable knowledge and management of information to support all the

processes to allow for informed decision-making (ISACA 2018a: 205). Knowledge management (KM) is “Responsible for sharing perspectives, ideas, experience and information, and for ensuring that these are available in the right time. It enables informed decisions, and improves efficiency by reducing the need to rediscover knowledge” (Axelos 2019: 92).

Knowledge is an important instrument and ingredient for the beneficiary, which is described as information integrated with experience, skills, facts, intuition, experience, selection, principles and learning (Mládková 2011: 250).

Yiua et al. (2013) and Boisot (1999) opine that knowledge often becomes embedded not only in documents or repositories, but also in organisational routines, processes, practices and norms. This revelation illustrates that corporate culture, best practices, core competencies, skills, or strategic visions are critical parts of the total stock of knowledge in an organisation.

Nonaka and Takeuchi (1995) propose the following KM process (Figure 2-20 on page 62):

- Socialisation (from tacit knowledge to tacit knowledge)
- Externalisation (from tacit to explicit knowledge)
- Combination (from explicit knowledge to explicit knowledge)
- Internalisation (from explicit knowledge to tacit knowledge)

As indicated in the previous paragraph, the organisational KM theory identified socialisation, internalisation, externalisation and combination (SECI) as the four modes of interaction that facilitates KM in an organisation (Maluleka 2017: 26).

The SECI theory was developed for the Japanese context and can be applied in any environment (Maluleka & Ngoepe 2018). Grillitsch, Müller-Stingl and Neumann (2006: 24) recommend the harmonisation of knowledge-oriented programmes in an organisation and the steps to be undertaken below:

- Executive management commitment

- Procedures organised for implementation
- Training and skills transfer to internal staff
- The collection and documentation of best practices and lessons learnt
- Interrogation and assessment of project meetings
- Stakeholders' needs and documentation inputs effected accordingly
- Implementation of IT infrastructure to support knowledge transfer
- Clear roles and responsibilities in meetings and for documentation

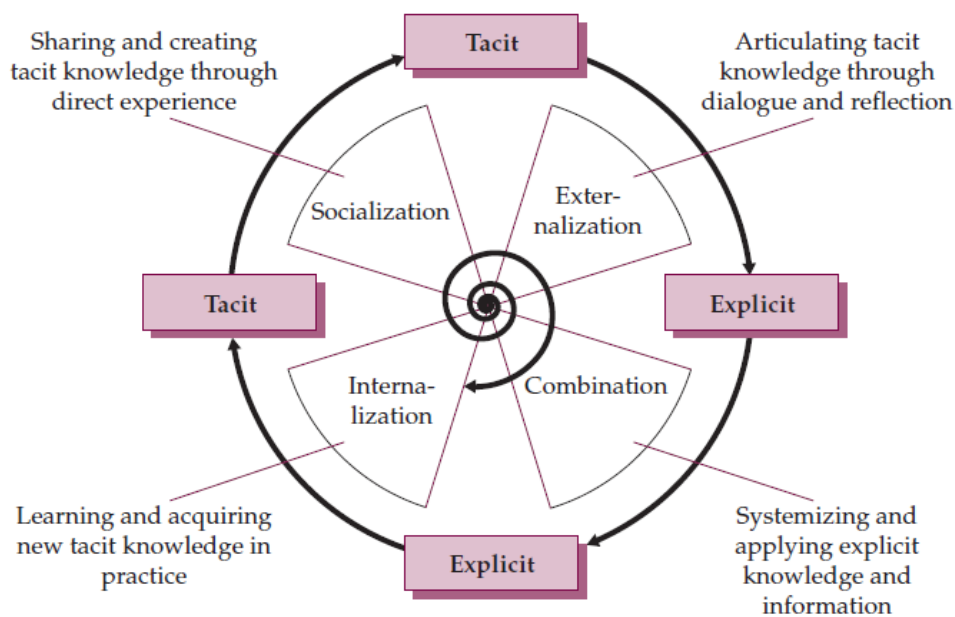


Figure 2-20: SECI Model
Source: (Takeuchi 1996)

Sharing of knowledge is done through human actions that have both tacit and explicit elements that are developed further through collaborative actions and interactions (Bettoni, Andenmatten & Mathieu 2006). Knowledge can be synthesised tacitly among individuals during collaborative activities (Becerra-Fernandez & Sabherwal 2014: 194). The challenge encountered in organisations is a lack of information sharing among employees and usage of KM systems (Valacich & Schneider 2018: 283). Hafeez and Alghatas (2007: 34) advocate for the creation of a virtual community of practice (CoP), whose purpose is having an interest in the same topic over a longer period of time and who is engaged in an activity of sharing their opinions on a specific topic with the use of technology.

2.4.9 Asset management

According to ISACA (2018a: 209), the process seeks to manage the software and hardware assets and optimise the value provided by utility and warranty and they are accounted for and protected physically. Information (explicit) assets mentioned in Table 2-8 can be easily documented, archived and codified for future use in the organisation (Valacich & Schneider 2018: 282). The Cabinet Office (2011d: 89) advises that “Assets are required to deliver services properly, and that accurate and reliable information about those assets is available when and where it is needed”.

I&T assets must include, but not be limited, to what is stated in Table 2-8.

Table 2-8: I&T asset classification

Asset	Asset type
Information asset	databases, and data files, contracts, agreements, system documentation, research information, user manuals, training material, operational and support procedures, business continuity plans, audit trails, and archive information
Software asset	application software, system software, development tools, and utilities
Physical assets	computing and communications equipment
Services asset	computing and communications service, power and environmental controls

Source: The Cabinet Office (2011d: 89)

Rules for the acceptable use of information assets associated with information processing facilities must be identified, documented and implemented. These assets must include electronic mail, internet and mobile devices (Valacich & Schneider 2018: 131).

2.4.10 Configuration management

Configuration management is the definition of the provision of sufficient information about service assets that includes the collection of configurations and the updating of the configuration repository in order to be managed (ISACA 2018a: 215). According to The Cabinet Office (2011d: 90), an integrated configuration management system should be implemented to hold all relevant attributes such as contracts, software licences, suppliers and anything that the organisation deems fit to be stored and maintained in a central location with a linkage to an incident, problem management. The purpose of configuration management is to ensure that information about the configuration of services and configuration items (CI) is reliable and available when needed. Figure 2-21 depicts that different CIs such as hardware, software, networks, users, and documents are collected and managed, and the interaction, relationships and dependencies of CIs are provided to create value for users and customers (Axelos 2019: 130).

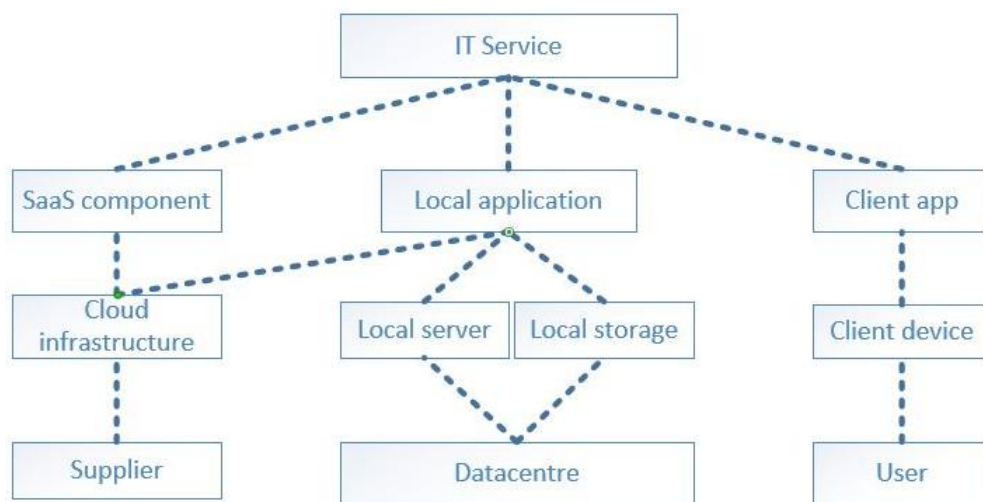


Figure 2-21: Configuration Items contribution to IT service (Axelos 2019: 130)

Operating procedures must be documented, maintained and made available to all users who need them. The Cabinet Office (2011d: 90) states that configuration management provides visibility of accurate representations of a service that enables the following:

- Prepares documented procedures for system activities associated with information processing and communication facilities, such as computer start-up and shut-down procedures, backup, equipment maintenance, media handling, computer room and mail handling management, and safety.
- Reduces time and cost to locate configuration information when needed.
- Treats operating procedures and the documented procedures for system activities as formal documents, and ensures that changes are authorised by management.
- Traces changes from approved requirements.

2.4.11 Project management

ISACA (2018a: 221) describes that all projects should be initiated in alignment with the enterprise strategy, which includes the initiation, planning, controlling and execution of projects, and post-implementation review. PMI (2017: 10) defines project management as “the application of knowledge, skills, tools, and techniques to project activities to meet the project requirements”. It is imperative that project managers should have the requisite knowledge and knowledge in utilising formal KM methods and apply practices, documents, procedures or deliverables deemed to be needed for design success of the project (The Cabinet Office 2011b: 89). Khumalo and Mearns (2019: 1) opine that organisations should implement a platform that has the ability to share project knowledge, manage its content / documents and collaborate during the course of projects. Two PM methodologies, namely Project Management Body of Knowledge (PMBOK) and PRjects IN Controlled Environment Version 2 (PRINCE2) are the most widely used project management methodologies in the world (Karaman & Kurt 2015: 1). Currently, the South Africa government adopted the PRINCE2 project management framework to implement its continuous improvement and delivery of quality services mandate (RSA 2015c: 8).

2.5 DELIVER, SERVICE AND SUPPORT

The purpose of this domain, as indicated by ISACA (2018a: 231), is the delivery of I&T operational and service outcomes as per the plan. The Run domain consists of six

processes, as shown in Figure 2-22. The Run domain is regarded as the description of the complete conditions of IT services supply (Mourad et al. 2017: 5).

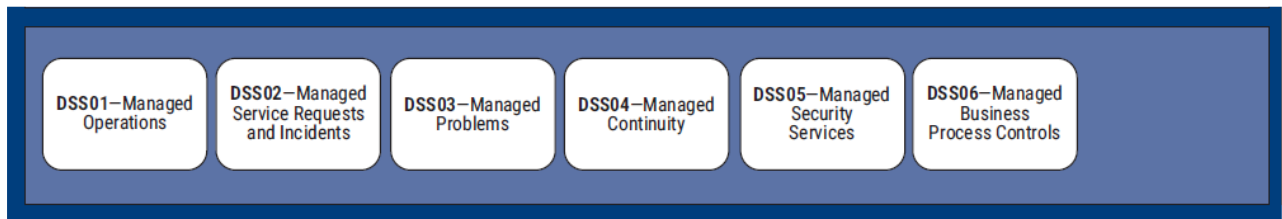


Figure 2-22: Run domain processes
Source: ISACA (2018a: 12)

2.5.1 Operations management

The operations management process is the coordination and delivery of internal and outsourced I&T operational product and service outcomes as per the plan (ISACA 2018a: 231). Operations management is focused on ongoing I&T services provision and on the fact that those operations continue efficiently by using the most appropriate resources needed to meet customer needs (PMI 2017: 16).

2.5.1.1 Perform operational procedures

According to ISACA (2018a: 232), it is important to document operating procedures and maintain and perform operational procedures and operational tasks reliably and consistently. The standard operating procedures (SOPs) help groupings such as organisations, departments, divisions or units to develop a standard practice and daily processes to ensure the execution of tasks that can be followed without deviation (The Ohio State University 2020). QuickBooks Canada (2020) state that some of the benefits for using for SOPs are:

- control of quality and consistency of your product
- simplification of performance management
- readiness for future expansion
- protection from knowledge loss

- saving on training costs.

RSA (2015c: 84) outlines the following limiting factors of an SOP:

- More restrictions and details that reduce individuals' autonomy and how an individual approach their work.
- Too much paperwork needed to be completed is time consuming.
- Implementation of an SOP to minor tasks creates a complete bureaucratic environment.
- Lack of updating of an SOP with best practices and new regulatory requirements will degrade the process.
- Unless they are used by all, they will be seen as part of the system put in place to appease employees rather than as a key universal management tool.

Having SOPs creates uniformity of organisational processes and the same processes can be used by external providers that would be discussed in the next section.

2.5.1.2 Managed outsourced I&T services

ISACA (2018a: 232) explains that the process ensures the outsourced I&T services adhere to contracts and SLAs with third parties hosting or providing such services. The outsourced I&T services are enforced with penalties agreed upon in section 2.4.9 on page 63 that if the SLA are broken (Mendes & Mira 2010: 6). Valacich and Schneider (2018: 407) give some advice on managing an outsourcing relationship:

- The organisation should continually manage the legal and professional relationship with the outsourced service provider.
- There should be clear and realistic performance metrics of the systems and of the outsourcing arrangement, such as tangible and intangible costs and benefits that should be deployed.

- There should be multiple levels of interface between the customer and the outsourced service provider to deal with relationship issues, policy and links to deal with operational and tactical issues.

The next section monitors the insourced and outsourced I&T services.

2.5.1.3 Monitor I&T infrastructure

Monitoring of I&T infrastructure and related events involves storing of sufficient chronological information in operations logs to reconstruct and review time sequences of operations and other activities surrounding or supporting operations (ISACA 2018a: 232). The process involves environmental monitoring software, hardware, electrical loss in facilities housing the I&T infrastructure and triggering alerts when they are not operating according to set standards. Implementation of a central monitoring application helps to ensure that there are predictable performance and availability of essential applications (Tang & Todo 2013: 195).

2.5.1.4 Manage the environment

The process involves the maintenance of measures for protection against environmental factors. Specialised equipment and devices must be installed to monitor and control the environment (ISACA 2018a: 232). ISO 14000 is an environmental management system (EMS) and an operational procedure that can be used once the data centre has been built.

The EMS ensures that organisations can “identify, manage, monitor and control the environmental issues in a holistic manner” (ISO 2016b: 2). Data centres require cooling and humidity control that should be done through an independent air-conditioning system that is not connected to the main building’s cooling system and that is set at cooler temperatures by blowing cool air through the ventilators installed on the raised floor of the data centre (Sawhney et al. 2018: 447-452).

2.5.1.5 Manage facilities

The management of facilities includes power and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines (ISACA 2018a: 233). A facility that houses a data centre should be fed by two electrical connections from different substations and an additional UPS or generator should be installed to start in case of power failure (Sawhney et al. 2018: 447452).

2.5.2 Service request and incident management

ISACA (2018b:237) states that service request and incident management provide timely and effective responses to customer requests, restore services back to normal and resolve requests and incidents. Service requests are managed throughout their life cycle from initial request to fulfilment using separate request fulfilment records/tables to record and track their status (The Cabinet Office 2011c: 220). They are the mechanism by which users formally request something and communicate with the IT service provider through the service desk (Al-hawari & Barham 2019: 5). Service requests are associated with the standard services that a provider delivers and are associated with a request model that defines any prerequisites, authorisations required, and standard work steps and activities needed to fulfil it (Mendes & Mira 2010: 3). As part of that request model, standard changes and other types of requests for change (RFC) may be needed to complete fulfilment actions.

According to The Cabinet Office (2011c: 219), incident management concentrates on restoring unexpectedly degraded or disrupted services to users as quickly as possible, in order to minimise business impact. Incident management handles incidents, service requests, access requests, and events and alerts are part of service request and incident management activities, as depicted in Figure 2-23.

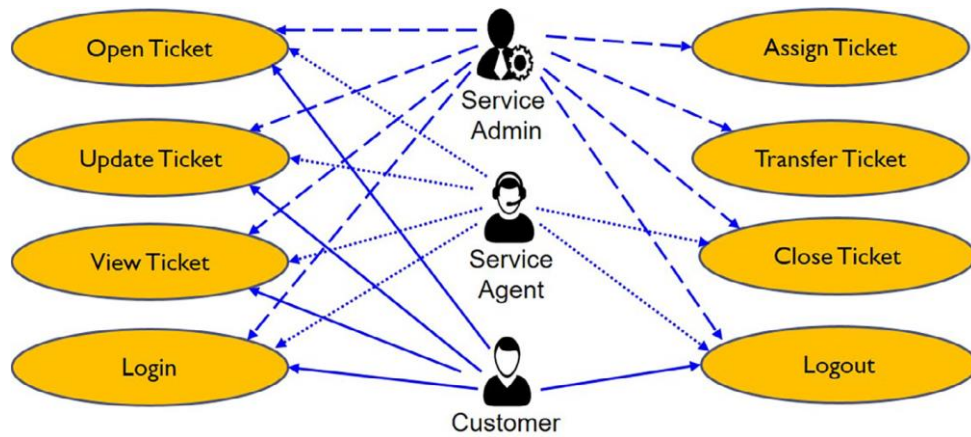


Figure 2-23: Service desk activities
 Source: (Al-hawari & Barham 2019: 3)

Table 2-9 highlights the differences between service and incident management processes.

Table 2-9: Service and Incident management differences

Incidents	Service requests
Unplanned	Planned
IT failure of service quality	Agreed service is not disrupted
Risks and costs for resolution can be volatile	Risks and costs are known and accepted
Resolution provided by incident management process	Resolution provided by Request Fulfilment process
An incident can be led to a service request – standard change or access request to resolve the incident	A service request will not use Incident Management as part of fulfilment process

Source: The Cabinet Office (2011c: 86–96)

When incidents as described in Table 2-9 are not timeously resolves, they lead to problem management that is explained in the succeeding section.

2.5.3 Problem management

This is a process of identifying and classifying problems and root causes for the prevention of recurring incidents (ISACA 2018a: 243). The process involves root cause

analysis to determine and resolve the underlying causes of incidents, and to implement proactive activities to detect and prevent future problems/incidents. This also includes the creation of known error records that document root causes and workarounds to allow quicker diagnosis, and then comes up with a resolution should further incidents occur (The Cabinet Office 2011c: 220). The function of operation management is to ensure that further investigation is conducted after service restoration to establish the root cause and permanent resolution to eliminate reoccurrence of an incident (Kush 2013: 98).

2.5.4 Continuity management

Continuity management ensures that effective business continuity management from the I&T point of view is implemented and maintained, so that the I&T services continue in the event of a major disruption, crisis, or disaster that threatens the ongoing existence of the department's IT environment (ISACA 2018a: 249). The international standards body, ISO, documented ISO 22301:2019 that

Specifies the structure and requirements for implementing a business continuity management system (BCMS) that develops business continuity appropriate to the amount and type of impact that the organisation may or may not accept following a disruption (ISO 2019).

In order to implement a successful business continuity management (BCM), all business units must be involved in the continuity planning function so that it can lead to synergy among the business units (Jedynak 2013: 89). The business impact analysis (BIA) and business continuity (BC) strategy documents should be the foundation that business units and staff rely on for guidance in the event of a disaster (Heng 2015: 13). Organisations rent server rack space in a secondary location or use a cloud service to ensure the organisation survives disruptions when there is power failure, equipment failure or natural disaster (Valacich & Schneider 2018: 455). Disaster planning ensures that when an organisation is under the worst-case scenario

of losing equipment or data, there is at least a plan that is readily available to recover it (Valacich & Schneider 2018: 446).

2.5.4.1 Continual improvement

Continual improvement:

...describes best practice for achieving incremental and largescale improvements in service quality, operational efficiency and business continuity, and for ensuring that the service portfolio continues to be aligned to business needs (The Cabinet Office 2011e: 7).

Continual improvement is a recurring activity that is performed at all levels to make sure that the organisation's performance continually meets stakeholders' expectations throughout the whole service value system (Axelos 2020b: 69).



Figure 2-24: Continual improvement model
Source: Axelos (2020b: 69)

A Plan-Do-Check-Act (PDCA) model ensures a system that can be utilised for establishing, deploying, monitoring, maintaining, evaluating and enhancing the business continuity management.

2.5.5 Security services management

Security services management's purpose is to assist enterprises in ensuring risks are managed and enterprise information is maintained according to the security policy (ISACA 2018a: 257). It is on that note that Culot, Nassimbeni, Podrecca and Sartor (2021: 77) set out standards for all types of organisations to implement an information security management system (ISMS) that is influenced by the objectives and the security requirements of an enterprise. Motii and Semma (2017: 53) advise that implementation of a security service management should have factors that need to be considered, namely:

- Approved security policy: its objectives and activities should reflect the business objectives outlined in sections 2.2.2 on page 28; 2.3.1 and 2.3.2 on page 31.
- The implementation should consider the organisational culture.
- There should be executive management support.
- Exhaustive knowledge of the organisation's security requirements (section 2.3.13 on page 50), risk assessment and risk management (section 2.3.12 on page 48) should be required.
- Effective security awareness should target all employees of an organisation.

Another implementation is an authentication process, which confirms the user's identity to access restricted applications or websites (Valacich & Schneider 2018: 448). Sawhney et al. (2018: 447–2) state that the method of using biometric or key card access allows one to enable/disable access when the role of a person changes and can be audited if the person entered or exited the restricted facility. Galiev et al. (2019: 2) advise that organisations should further implement a certificate authority (CA) as a trusted entity that would issue digital certificates and public-private keys by performing the following roles:

- Maintaining the certificate revocation list.
- Setting administrator roles.
- Distributing public and private authentication keys.
- Validating the identity of the entity who requests a digital certificate.

Zikopoulos et al. (2013: 232) advise that consideration for security should include segregation of duties, separation of concern, principle of least privilege, and defence in depth, which need to be applied to data that are stored anywhere. There are three information security requirements that should be addressed to mitigate risk, namely confidentiality, integrity and availability (CIA) (Bakar, Yaacob & Udin 2015: 132), which are explained as follows (ISO 2013: 2):

- Confidentiality – Non-disclosure of information to unauthorised entity.
- Availability – Information assets that are readily accessible and usable when needed by an authorised entity or process.
- Integrity safeguards the completeness and accuracy of information assets. ISO (2016a: 5) indicates that a record with integrity should be complete, unaltered and where there was any authorised insertion or erasure to a record, it should be clearly indicated and trackable.

Organisations need to implement a security patch management system that would be linked to the hardware or software vendor to look for available critical patches to fix hardware or software flaws on systems that the organisation has configured and installed (Valacich & Schneider 2018: 399).

2.5.6 Business process controls management

ISACA (2018a: 265) state that the purpose of business process controls management is to “maintain information integrity and the security of information assets handled within business processes in the enterprise or its outsourced operation”. Bakar et al. (2015: 132) opine that the adoption of ISO 27001 may assist in streamlining the internal processes, eliminating redundancies, preventing costly litigation and enhancing competitive advantage.

Morland-Austin (2020) suggests the following list of control activities:

- Align control activities embedded in organisational processes with enterprise objectives. Continually assess and monitor the execution of the organisation's process activities and related controls.
- Control the processing of information. Operate the execution of the organisation process activities and related controls.
- Manage roles, responsibilities, access privileges and levels of authority. Manage the organisational roles, responsibilities, levels of authority and segregation of duties needed to support the organisation process objectives.
- Manage errors and exceptions. Manage organisational process exceptions and errors and facilitate their correction
- Ensure traceability of information events and accountabilities. Ensure that organisational information can be traced to the originating organisation event and accountable parties.
- Secure information assets. Secure information assets accessible by the organisation through approved methods.

The section, monitor, evaluate and assess addresses the performance monitoring and conformance of I&T with internal performance targets, internal control objectives and external requirements.

2.6 MONITOR, EVALUATE AND ASSESS

According to Mourad et al. (2017: 5), the monitor domain looks at currently deployed solutions throughout all domains and lifecycles with a view to improving them. The monitor domain provides transparency of performance and conformance, and drives the achievement of organisational goals (ISACA 2018a: 273). A proper monitoring process consists of four domains mentioned in Figure 2-25.

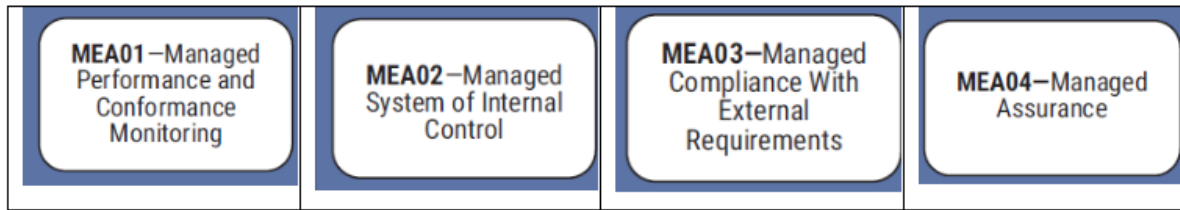


Figure 2-25: Monitor domain processes
Source: ISACA (2018a: 12)

2.6.1 Performance and conformance monitoring

This entails the provision of transparent performance and conformance and the implementation according to the goals set (ISACA 2018a: 273). This can be achieved by implementing a corporate governance system that involves a set of relationships between an organisation’s management, its board, its shareholders and other relevant stakeholders to provide a structure from which the objectives set can be monitored for performance and conformance (Aerts & Walton 2018: 439).

2.6.2 Internal control system

The key stakeholders should assure transparency in the adequacy of the system of internal control system in use so that it can give trust in the operations and confidence for the enterprise to achieve its objectives (ISACA 2018a: 279). Section 45 of the PFMA further states that the effectiveness of the system of internal control should be informed by the work of the internal auditors and the executive managers who have the responsibility of developing and maintaining the internal control framework and replying to comments made by the external auditors in their management letter and other reports (RSA 1999: 44). The corporate governance framework emphasises that there should be an effective system of internal control whose accountability lies with the board, the audit committee and a plan to address weaknesses and ensure continuous improvement of the system is in place (Aerts & Walton 2018: 447).

2.6.3 External requirements compliance

ISACA (2018a: 285) outlines that the enterprise should ensure compliance with external requirements. According to the European Union (EU) (2016: 6), public entities that collect data in accordance with a legal obligation, should process it in compliance with the data-protection rules according to the purpose of the processing. There has been widespread non-compliance with regulatory and legal requirements in cloud data hosting services due to outdated and inadequate legislation or the lack thereof (Mosweu et al. 2019: 8).

Corporate Governance requirements defined by the Sarbanes-Oxley Act (SOX) and the King IV code of good governance altered the way in which organisations report and audit (Aerts & Walton 2018: 440; IODSA 2016). In South Africa, the Companies Act of 2008 requires that companies should always prevent human rights violations that might be linked to their daily operations (Gwanyanya 2015: 3119). To provide compliance with the state and stakeholders, an organisation that is funded in terms of the Public Finance Management Act (PFMA) or through subscriptions from members, must be audited by the national auditing body, the Auditor-General of South Africa (RSA 2018:5). Furthermore, RSA (2019d: 16-20) promulgated regulations to deal with investigations and remedial actions when a material irregularity is suspected. What is clear is that I&T governance failures can also have an external impact and cause reputational damage, and losses incurred by the business and regulatory disapproval (Omari 2016: 34).

2.6.4 Assurance management

Assurance management seeks to enable the organisation with assurance initiatives that would assist in complying with external requirements, regulations and strategic objectives of the enterprise (ISACA 2012: 289). The executive management is required to put in place an assurance framework to ensure they have the necessary evidence to satisfy themselves on the efficiency and effectiveness of the internal control framework and to provide the required level of assurance to the board through an audit committee (RSA 2012: 16). Auditing functions in the cloud computing

environment are constrained by a lack of clear responsibilities between the client, the cloud service providers and the auditors. This is further exacerbated by the fact that the client's data are stored in multiple jurisdictions; therefore, the owner loses control and assurance (Mosweu et al. 2019: 7). In Figure 2-26, Abedian, Strachan and Ajam (1998: 12) propose the following activities that can give assurance.

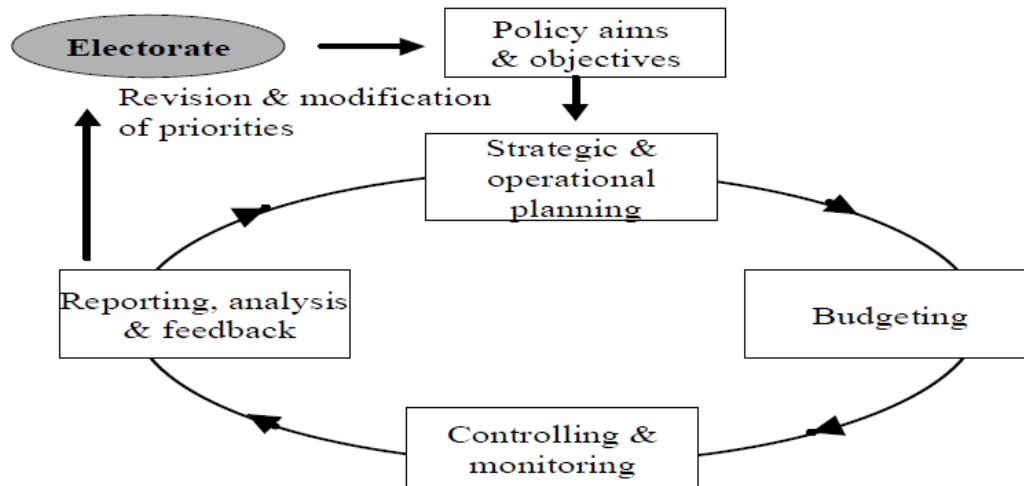


Figure 2-26: Planning, monitoring and reporting
Source: Abedian et al. (1998: 12)

2.7 SUMMARY

The main objectives of this chapter were to discuss the theoretical frameworks and justify the selection of the COBIT framework to underpin this study. COBIT was discussed as this study's theoretical framework. The chapter further discussed the relevance of the COBIT framework. Some examples where COBIT was used in the information governance field were also discussed. As this study aimed to develop an information governance system at SACSSP, with a view for entrenching a culture of good corporate governance. The five COBIT constructs that the research deemed to be appropriate in entrenching a culture of integrated information systems implementation at the SACSSP were also discussed in this chapter, namely evaluate, direct and monitor (EDM); align, plan and organise (APO); build, acquire and implement (BAI); deliver, service and support (DSS) and monitor, evaluate and assess (MEA). The following chapter examines and justifies the research methodology utilised in this study.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 INTRODUCTION

The previous chapter highlighted the literature on the evaluate, direct and monitor; plan; build; run; and monitor domains. The constructs derive from the COBIT model, which has been used as a framework for this study. These constructs also assisted in the formulation of questions that would be used in the study to answer the research questions stated in chapter one. A brief discussion of the research methodology was outlined in chapter one. This chapter discusses the detailed systematic approach and design that were employed for the purpose of this study.

Pickard (2013: 99) states that a research method is “defined as the bonded system created by the researcher to engage in empirical investigation, the overall approach to the investigation”. Bryman (2016: 40) points out that a research method is a necessary instrument that can be used in participants’ observation, or in a questionnaire or in conducting an interview schedule. The strategy used by the researcher to collect data and analyse it to solve a particular problem requires careful planning of resources, procedures and the form that data would take on (Leedy et al. 2019: 82). Creswell and Creswell (2018: 179) indicate that this chapter is about the role of a qualitative researcher.

... plays in the study, drawing from an ever-expanding list of types of data sources, using protocols of recording data, analysing the information through multiple steps of analysis and mentioning approaches for documenting the methodological integrity or accuracy or validity of data collected.

This chapter covers the research paradigm, research approach, research design, qualitative research methods, data collection instruments, research procedure population, sampling techniques, data quality, data collection tools used by the researcher to answer the research questions, data analysis and presentation, ethical considerations and evaluation of research methodology (Figure 3-1).

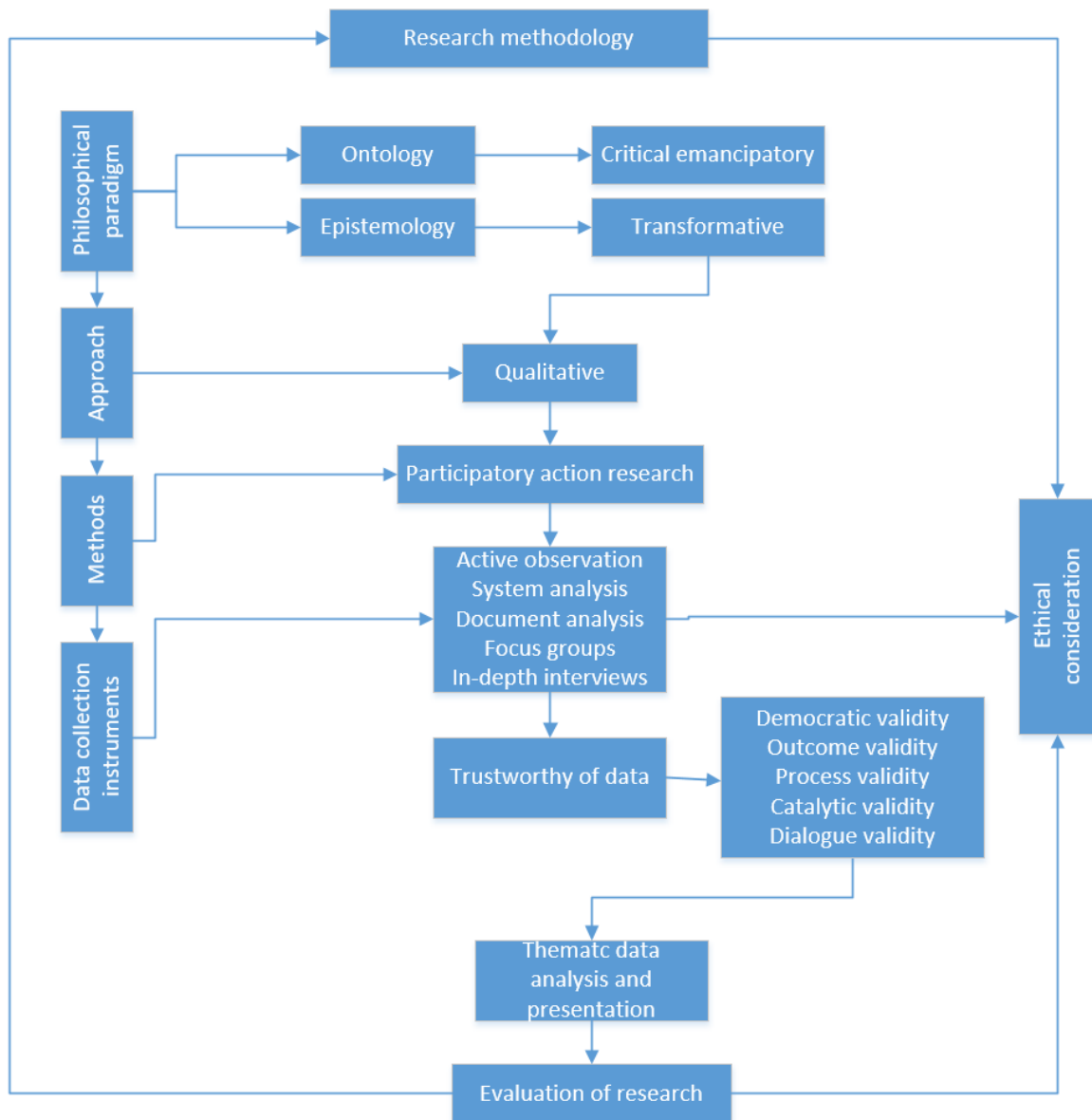


Figure 3-1: Research methodology roadmap

3.2 RESEARCH PARADIGM

Bryman (2016: 637) defines a paradigm as “... a cluster of beliefs and dictates which for scientists in a particular discipline influence what should be studied, how research should be done, [and] how results should be interpreted.”

A paradigm is seen as a common philosophical orientation about the world and the essence of research that the researcher brings to a study (Creswell & Creswell 2018:

5). There are four paradigms underlying research methodologies, namely positivism, critical emancipatory, interpretivism and pragmatism (Leedy et al. 2019: 8).

Table 3-1: Paradigm differences

Paradigm	Differences
Positivism	It supports the utilisation of the methods of the natural sciences to the inquiry of social reality and beyond (Bryman 2016: 24). The "...progress toward genuine understandings of physical, social, and psychological phenomena tends to be gradual and probabilistic" (Leedy et al. 2019: 8). Pickard (2013: 10) argues that the current post-positivism has its foundation in any perception of reality that cannot be an objective picture but is emphasised from empirical observation and existing theory.
Postcolonial / Indigenous	It is a paradigm that is used for hearing non-western voices and emancipating the voices of formerly oppressed generations from silence imposed by colonisation (Walker 2019: 161)
Critical emancipatory	"CER requires total immersion of both the researcher and the participants as equal partners in the research process, so that all senses of perception and understanding are simultaneously involved to be able to make as much sense of the myriad of signals and symbols coming from diverse perspectives as possible" (Nkoane 2012: 99).
Interpretivism	Knowledge is subjective. Participants in a study make meaning of a situation. There are multiple realities (Leedy & Ormrod 2015: 100).
Pragmatism	This paradigm uses the combination of the positivist and interpretive approaches since it is not committed to any one philosophical system and reality (Creswell & Creswell 2018: 10). Muro et al. (2019) and Denscombe (2010: 146) explain that pragmatism uses qualitative and quantitative approaches that are focused on triangulation with the main emphasis on devising practical solutions to research problems.

The critical emancipatory paradigm is the research paradigm that was implemented in this study, because it places value on deep analysis that has a motivation to transform and change people's lives and liberate them from less useful practices, while meeting real-life needs (Dube & Hlalele 2018: 79). In prior research conducted by Nkoane (2012: 99), CER was seen to have "an agenda to critique and challenge, to transform and empower; it is geared towards social justice and enhances the principles".

3.3 RESEARCH APPROACHES

Creswell and Creswell (2018: 3) define research approaches as "... plans and the procedures for research that span the steps from broad assumptions to detailed methods of data collection, analysis, and interpretation".

The three research approaches are known as quantitative, qualitative and mixed methods research.

3.3.1 Quantitative research

Ngulube (2020: 5) states that qualitative research designs are descriptive, correlational, quasi-experimental and experimental with evidence that is measurable through the use of numeric data and statistical analysis. Leedy et al. (2019: 6) describe quantitative research as intricate in studying the quantities of one or more variables that can be measured in a numeric way. This is made possible when data collection is relevant to the research question and the data allow the researcher to investigate the issues of concern (Pickard 2013: 284). This type of research is a tool to establish empirical relationships (Stockemer 2019: 9).

3.3.1.1 Advantages of quantitative research

Quantitative research is useful when the researcher does not have the variables to examine and intends to generalise the findings of such study to a population (Creswell & Creswell 2018: 19). Bryman (2016: 163) explains that generalised findings are not confined to a particular study. Leedy et al. (2019: 303) relay that the importance of

quantitative research makes better sense of the universe through numeric values and measurements since the numbers can represent certain characteristics that can answer critical questions and their meaning. This form of research assumes the objective reality of social facts (Pickard 2013: 13).

3.3.1.2 Disadvantages of quantitative research

There is too much reliance on data collection instruments such as questionnaires and structured interviews that are not flexible and this hinders the connection between everyday life and research (Bryman 2016: 166). According to Stockemer (2019: 9), quantitative research is less well-suited to explain the causal mechanism behind a statistical relationship.

3.3.2 Qualitative research

Qualitative research focuses on a phenomenon that is occurring or has occurred in a natural setting, while there is an involvement of capturing and studying the complexities of such phenomena (Leedy et al. 2019: 228). Given (2016: 2) describes qualitative research as an exploration process that thoroughly investigates people's experiences, perceptions, behaviours and beliefs, while providing a window of understanding of participants' actions and their thinking. A qualitative research study is designed to provide an engagement platform for researchers and research participants to be involved directly for extended periods and thereby producing negotiated outcomes (Pickard 2013: 14).

3.3.2.1 Advantages of qualitative research

This type of research entails the richness of and the detail to data, as well as the tolerance of ambiguity and contradictions, that give a researcher the opportunity to obtain a correct explanation (Denscombe 2010: 302). Data are collected from a natural setting where the participants experience the problem under study (Creswell & Creswell 2018: 180). Qualitative research brings a combination of textual methods with direct human-focused behaviours that give researchers better insights into rich

and rich data about participants' experiences (Given 2016: 2). This type of methodology assumes social constructions of reality (Pickard 2013: 13).

3.3.2.2 Disadvantages of qualitative research

Qualitative researchers must be well trained in observation techniques and interview strategies because the method requires significant preparation and planning, which makes data collection longer over the course of months (Leedy et al. 2019: 229). Bryman (2016: 398) points out that qualitative research is criticised because it does not use any standardised procedure and, therefore, it is difficult to replicate due to small numbers in the locality of study. It is also too subjective and relies on inconsistent views. Furthermore, there is a lack of transparency in how the conclusion was reached and it has problems of generalisation.

3.3.3 Mixed methods research

Creswell and Creswell (2018: 14) define mixed methods research (MMR) as "...a combination or integration of qualitative and quantitative research and data in a research study". Ngulube (2020: 426) explains mixed methods research as "...Suited for complex research problems comprising many components, or people and contextual factors that cannot be fully addressed by using one methodology". Pickard (2013: 18) regards MMR as a combination of methodologies that falls within post-positivist paradigm in order to address the same overarching research question.

3.3.3.1 Advantages of mixed methods research

The advantage of employing MMR is its strength of drawing on qualitative and quantitative research methods and minimising the limitations of both (Creswell & Creswell 2018: 217). Leedy et al. (2019: 260) state the advantages of using MMR as: it addresses the research problem completely; it uses both methods to complement each other; it brings insights into generalisation and assists the researcher in testing in controlled quantitative research; and is useful in the development of relevant research tools and strategies of collecting data from one type of data to another.

3.3.3.2 Disadvantages of mixed methods research

Extensive data collection and the time-intensive nature of analysing both qualitative and quantitative data require the researcher to be familiar with both methods (Creswell & Creswell 2018: 217). The method is seen as restrictive because it dictates that quantitative data focus on meanings, while qualitative data interpret people's behaviour, which brings collusion between the two methods together under the phenomenon "behaviour versus meaning" (Bryman 2016: 626). Leedy et al. (2019: 260) decry that MMR is time consuming to the researcher and requires energy for the collection, analysis, interpreting and integration of both qualitative and quantitative data.

3.3.4 Justification for using a qualitative approach

The qualitative research method was employed to answer the research questions because it "...examine[s] the human condition in a range of settings and across various populations" which, includes "...the nature of human relationships, including the ways that people engage with organisations, social structures, and each other..." (Given 2016: 4). Qualitative research is primarily about gaining an in-depth understanding of the study problem (Leedy et al. 2019: 230).

3.4 RESEARCH METHODS

Bryman (2016: 40) regards a research method as a framework that can be utilised for the collection and analysis of data. Creswell and Creswell (2018: 11) equate research methods as strategies available to the researcher to provide specific direction for procedures applied in quantitative, qualitative and mixed methods approaches. Furthermore, authors such as Leedy et al. (2019: 82) consider a research design as providing the overall architecture planning for the data collection and analysis of such data by the researcher. The types of research design and their purposes are discussed in Table 3-2.

Table 3-2: Common research designs / approaches

Design	Purpose
Action research	This form of research aims to use research not to describe or understand a problem at hand, but to act and make transformative changes in conditions (Leedy et al. 2019: 281).
Case study	The purpose of a case study is to provide a holistic account of the case and in-depth knowledge of the specific case through rich descriptions situated in a context (Pickard 2013: 102).
Content analysis	Bryman (2016: 283) explains the approach to the analysis of documents and text in a systematic way that seeks to quantify content in terms of predetermined categories and in a replicable manner.
Correlational research	Leedy et al. (2019: 148) declare that it is a statistical investigation that examines the extent to which differences in one variable are associated with differences in one of more variables, but it does not necessarily probe for causal reasons underlying them.
Design-based research	It aims to produce theories and knowledge about learning and teaching that are based on real-life context by manipulating these contexts in particular ways and conducting and refining experiments and interventions so that researchers can make evidence-based claims about learning (Leedy et al. 2019: 284).
Developmental designs	It is the study of particular characteristics changes that is either a cross-sectional study or a longitudinal study (Leedy et al. 2019: 150).
Ethnography	It is a type of a qualitative inquiry where a researcher spends considerable time in the field forming part of the setting among the people whose lives are being studied with a totality of all social, cultural and psychological aspects of the community (Denscombe 2010: 80).

Design	Purpose
Experimental research	Experimental research involves a researcher conducting experiments when there is an assessment after giving one group a specific treatment and withholding to the other and determines how both groups fared based on the outcome (Creswell & Creswell 2018: 12).
Grounded theory research	Grounded theory is a qualitative research method that uses a systematic set of procedures to develop an inductive theory about a phenomenon by utilising generalisations and making comparisons across social situations (Neuman 2014: 71).
Historical research	This is a type of approach where a historian gains access to the past through primary and secondary evidence along with personal interpretation of such evidence (Pickard 2013: 169).
Narrative research	The researcher studies the lives of individuals and asks one or more individuals to provide stories about their lives; and this information is narrated by the researcher in a chronological manner (Creswell & Creswell 2018: 13).
Observation study	It is associated with qualitative research where there is a relatively prolonged involvement of the observer in a social setting in which the same researcher seeks to observe the behaviour of participants of that settings and draw out meaning they ascribe to their environment and behaviour (Bryman 2016: 270).
Participatory action research	PAR is an extension of action research. PAR research projects “are designed to engage participants in investigating issues of importance and relevance to their lives and, furthermore, to challenge status-quo explanations of complex issues and problems” (Leedy et al. 2019: 285)
Phenomenological research	The research coming from philosophy and psychology in which the researcher describes the lived experiences of individuals

Design	Purpose
	about social reality as described by participants (Creswell & Creswell 2018: 13).
Survey research	Used to systematically collect data from respondents using standardised procedures and sampling such as random or representative of the population about their perceptions, attitudes and behaviours (Stockemer 2019: 23).

PAR was chosen based on Leedy et al. (2019: 285) who state that, in PAR, a researcher makes a particular effort to engage individuals who have a history of being marginalised in a particular social group. Ngulube (2020: 250) contends that the benefit of a PAR is that it believes in collaborative, participatory, action research, which is characterised by interactions between the researcher and the participants, together with their methodology that brings respect for cultural norms of the researched. Furthermore, PAR is eliciting knowledge out of direct actions of participants by giving the participants an active role in formulating, designing and carrying out the research (Neuman 2014: 31). PAR is considered a continuous process of data collection and analysis where there are two agendas that must be achieved – the practical agenda that focuses on the attainment of integrated online system goals and the research agenda with which the researcher would produce new knowledge (Martincic & Dovey 2011: 9).

The researcher got involved with the participants in order to form part of solving the problem because there was a lack of skills and capacity internally (SACSSP 2018b). The PAR design is a research method approach that was used by Kurt Lewin to describe the work in the field of human dynamics with individuals affected by post-war social challenges (Pickard 2013: 157). According to Leedy et al. (2019: 92), it is a form of applied research that focuses on finding a solution to a local problem in a local setting. Leedy et al. (2019: 281) refer to PAR as an approach where the aim of the research is not just to describe or understand an issue or problem, but also to act and make concrete changes to and transformation in conditions, resources, practices and / or policy.

The following factors were benefits of applying PAR in this study:

- There was collaboration between the researcher and the participants at the SACSSP in defining the problem, and selecting an approach, research methods, data analysis methods and manner in which the findings would be utilised based on the diagnosis (Bryman 2016: 387).
- There was systematical access to the voice of the SACSSP community to plan context-appropriate action and collaborate with them in shaping the research (Creswell & Creswell 2018: 230).
- The SACSSP participants of the study population were involved as active and equal participants in all phases of the research project to facilitate change and the dissemination of results (Given 2016: 19).

According to Stringer (2014: 9), PAR has as three phases, namely:

- Look phase: getting to know stakeholders so that the problem is defined on their terms and the problem definition is reflective of the community context.
- Think phase: exploring and analysing what was learnt in the look phase.
- Act phase: planning, implementing, and evaluating, based on information collected and interpreted in the other phases.

These phases show that the method of enquiry can be repeated over time (Figure 3-2).

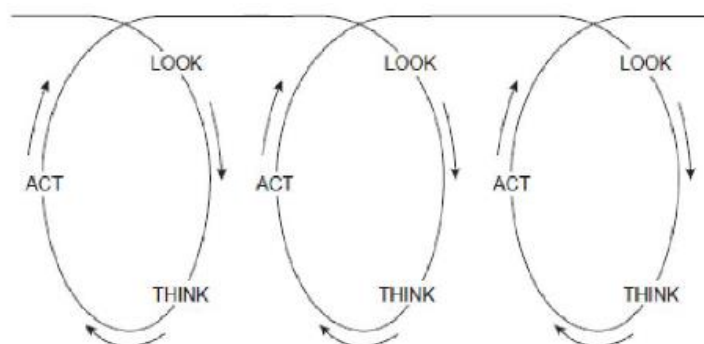


Figure 3-2: Action Research Interacting Spiral
Source: Stringer (2014: 9)

The first cycle confirmed the problem that was highlighted in the exploratory meeting. The participants were given an opportunity to explore, comment and discuss issues raised. This involved providing inputs into benchmarking activities and drafted documents and receiving invitations to present during board meetings, IT and Business Re-engineering Committee meetings, and other scheduled focus groups meetings linked to specific subjects around information governance to support corporate governance. Table 3-3 indicates the action research work plan and timelines for the study.

Table 3-3: Action research work plan and timelines

Implementation steps (What will be done)	Responsibilities (who will do)	Resources (Funding / Time / People / Materials)	Timeline (By when? / Day / Month)
I. Submit result (action research) to management and the board	Researcher	SACSSP	March 2019
II. Show the outcome and intervention to management and Business Re-engineering Committee	Researcher	SACSSP	March 2019 to December 2019
III. Use the findings of benchmarking in addressing the problems on information governance	Researcher	SACSSP	July 2019 - September 2019
IV. Conduct an action research similar intervention to address a specific problem (network upgrade, hardware refresh and system development) in solving to SACSSP staff and board	Researcher	SACSSP	September 2019 – March 2021

The following section discusses population and sampling for the study.

3.5 POPULATION AND SAMPLING

The description is given of different techniques that were used to sample and collect data, namely population and sampling. The population of the study consisted of SACSSP staff, including board members and members of the IT and Business Re-engineering Committee. The staff members participating came from the following business units: registration, education training development (ETD), professional conduct and finance, which are all the areas of interest for this study. Access to the population was obtained through the express approval by the board to overhaul IT systems (SACSSP 2018b).

The study involved the participation of the selected SACSSP staff, board members (SACSSP 2018), current and potential service providers, and other councils that were benchmarked from the inception of the project. In terms of section 10 of SACSSP Act, the SACSSP established 10 committees to assist with the performance of its functions (SACSSP 2018c: 8). The executive management, under the stewardship of the registrar, deals with daily operational matters. All the committees, including the executive management, report the recommendation back to the council for approval.

Additional committees, depicted in blue background, were added later through regulations in anticipation to deal with unprofessional conduct of social professionals (SACSSP 2019b: 21). Figure 3-3 outlines the population sampled.

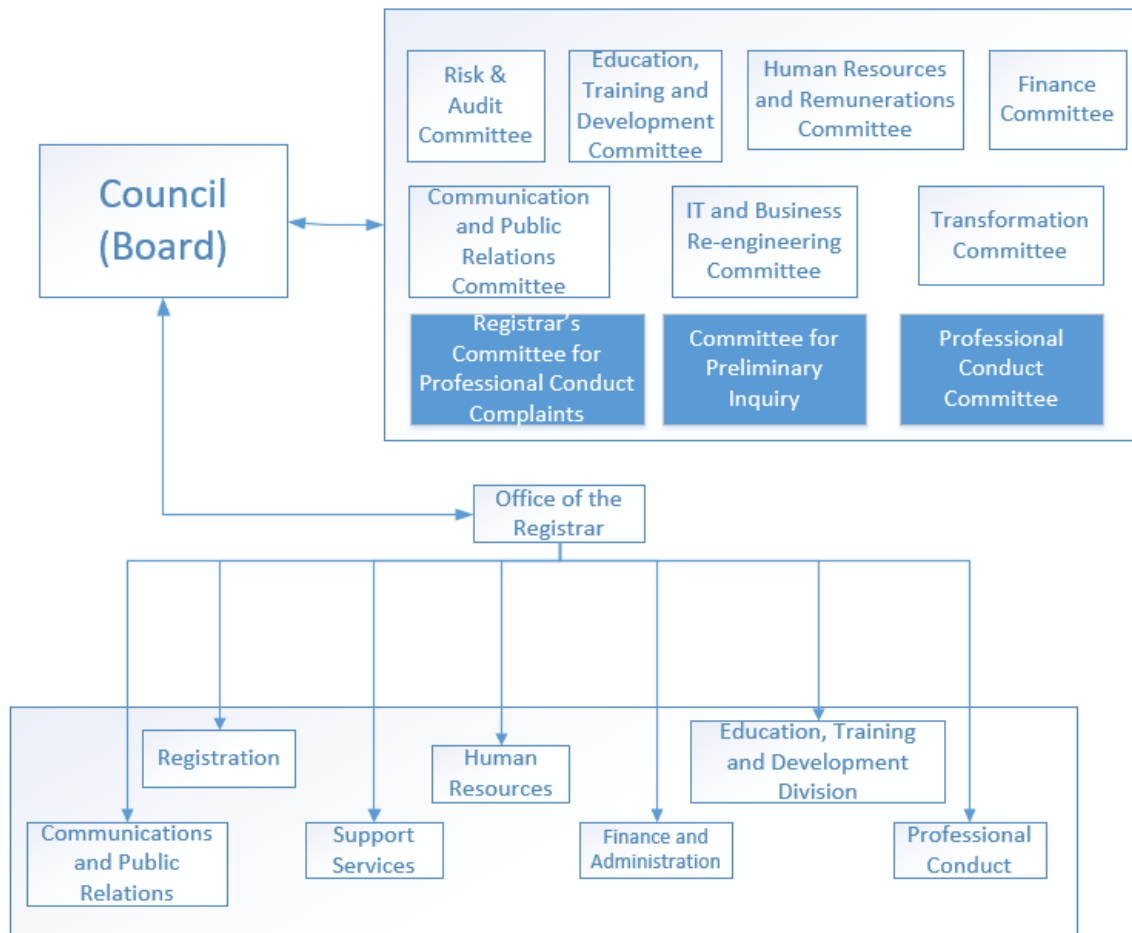


Figure 3-3: SACSSP organisational structure
 Source: SACSSP (2018c: 7–8)

Sampling is a process used when it is not possible to include the whole population that a researcher wants to investigate or study (Pickard 2013: 59). The approach includes people, documents or sites being selected to fit with the inductive intentions of a qualitative research (Given 2016: 61). For the purpose of the study, a researcher was introduced to the participants and their roles at the SACSSP and participants were sampled directly (Creswell & Creswell 2018: 150). The four sampling types are discussed in the next sections.

3.5.1 Purposive sampling

Purposive sampling was used to select participants because of the information-rich cases from which one can learn a great deal about issues of central importance to the

purpose of the research (Pickard 2013: 64). The initial consultative contact with the key informants, one board member and three managers revealed that there was a need for a system overhaul with a view to maximising efficiency and ensuring integration within administration in support of information governance (SACSSP 2018b: 1). For other matters on which key contacts were not knowledgeable, the researcher was referred to other participants who had experience and knowledge relevant to the study; therefore, snowball sampling was used (Leedy et al. 2019: 242).

3.5.2 Theoretical sampling

Given (2016: 61) indicates an approach of people, documents or areas that are selected because they fit a certain criterion to be studied. That criterion involves collecting data for the generation of theory in the form of an iterative process that will cease when saturation is reached (Bryman 2016: 410). Pickard (2013: 64) points out that this form of sampling assists with the generation of a theory using collected data that were coded and analysed in order to give direction to where the data can next be found for the emergence of a theory.

3.5.3 Generic sampling

According to Bryman (2016: 412), generic sampling is an open-ended approach and places the main emphasis on the generation theories and concepts, and it is not an iterative process.

3.5.4 Snowball sampling

The sampling process starts with initial participants or text that leads to new potential participants (Given 2016: 61). This form as sampling requires a small group of sampled participants who have experience relevant to the research questions asked. The initial participants would propose other participants who are also relevant to the research (Bryman 2016: 415). In snowball sampling, there should be a reduction of

bias by taking the initial participants as a pilot and it should never be declared as representative of a population being studied (Pickard 2013: 66).

3.5.5 Justification for sampling technique used

With this sampling procedure, the researcher was able to interview and observe diverse participants involved in registration, finance, professional conduct, education and training development, and he could observe the whole setting (Bryman 2016: 415). Purposive sampling was used to find participants from the overall population as presented in Table 3-9.

Table 3-9: Overall population classification

Key area	Population	Total population
Governance domain	Board members	13
Management domain	Senior management	5
	Rest of staff	27
TOTAL		45

The table above lists the participants in diverse roles within the social service council to ensure that there is representativity. Eight participants were interviewed using structured interview schedule. The upcoming section details the data collection instrument used.

3.6 DATA COLLECTION INSTRUMENTS

The researcher made use of survey methods indicated in chapter one to develop a framework for information governance, with a view to entrenching a culture of supporting corporate governance at the SACSSP. The study used interviews, focus groups, observation, system and document analysis. The focus group identified a

problem and the researcher collected data and formulated solutions to the problem with the participants.

3.6.1 Interviews

Qualitative research employs an interview process due to the flexibility of the engagement, and it is considered attractive because more data can be collected (Bryman 2016: 466). Interviews can be conducted through audio (telephone) means, video-conferencing or face-to-face participation (Creswell & Creswell 2018: 187). This study used a qualitative interview that was less structured and greater emphasis was placed on the interviewee's own perspective (Bryman 2016: 466). This data collection technique was beneficial to the interviewer because it allowed access to the interviewees' mind and some degree of interaction in order to receive the data needed to answer the research question (Pickard 2013: 196). The researcher made use of the Zoom video communications® solution, LimeSurvey online tool, physical interviews and email to interview some of the participants (Table 3-4).

Table 3-4: Interviews sources

Mode of interview	Number of participants
Zoom video communications	3
Email	1
LimeSurvey	1
Face-to-face interviews	3

Covid-19 protocols followed participants that were interviewed physically. According to Pickard (2013: 199), unstructured interviews are “used to gain a holistic understanding of the thoughts and feelings of the interviewee...” where it is used to investigate the noteworthy features for later research. See Annexure A for the structured interview schedule used.

3.6.2 Focus groups

A focus group is a form of group interview with participants with the notion that they have a certain amount of experience, while examining the manner in which those interviewed interpret the general topics the researcher is interested in (Bryman 2016: 500). Six to eight participants can form part of interviewees in focus groups (Creswell & Creswell 2018: 187). The focus groups given in Table 3-5 were existing governance and management structures already implemented at the SACSSP as depicted in Figure 3-3. The focus groups for the study were structured as follows:

Table 3-5: Focus committee meetings activities

Focus group	Area of focus
IT and Business Re-engineering Committee	<ul style="list-style-type: none"> • Revised records management policy • Skills development plan • IT systems terms of reference • Recruitment of an IT practitioner. • IT risk register • Integrated business processes • Board decisions on IT projects • Data verification
Financial Committee	<p><u>Evaluation of bids (technical queries)</u></p> <ul style="list-style-type: none"> • The evaluation of IT networking upgrade
SACSSP management	<ul style="list-style-type: none"> • Advisory on I&T related matters • Development of operational processes
SACSSP staff	<ul style="list-style-type: none"> • Return postage challenge • Archiving
Current service provider(s)	<ul style="list-style-type: none"> • Development of AS-IS architecture baseline document • IT service operations
Other councils	<ul style="list-style-type: none"> • Benchmarking – involved visiting other councils and viewed systems implemented
Winning bidder	<ul style="list-style-type: none"> • Drawing system specifications • Preparation of bidding documentation • Monitoring of implementation

Focus committee meetings were held physically (bid evaluation committee for hardware tender opening of bids, software development tender briefing) and virtually through (Microsoft Teams®) during the covid-19 pandemic (March 2020 – February 2021). March 2020 was for the opening of bids for software development and February 2021 for the bid evaluation committee software development tender and interviews for the said tender.

The focus group’s composition for the study is explained in Table 3-6. According to Creswell and Creswell (2018: 150), there is a requirement that characteristics of the population members should be known so that the population can be stratified. However, the structures have already been set in this study and the researcher is obliged to work with the available structures.

Table 3-6: Composition of focus committee meeting groups

Focus group	Area of focus	Size of group	COBIT constructs covered	Meeting frequency
IT and Business Re-engineering Committee	IT governance	10	EDM, APO, BAI, DSS & MEA	Once per quarter
SACSSP management	Management function	5	EDM, APO, BAI, DSS & MEA	When required
SACSSP staff	Administrative, archiving	29	DSS	When required
Current service provider	IT service operations	6	DSS & MEA	When required
Potential service providers	Benchmarking	4	MEA	Once and followed up when required
Winning bidder	Integrated system implementation	2	APO, BAI, DSS & MEA	Project and progress reporting

Having tabled the composition of focus committee meeting groups for the study, the adjoining section discusses observations data collection instrument.

3.6.3 Observations

Observation happens when a researcher observes the behaviour and activities of people under study using structured and unstructured ways to record their activities (Creswell & Creswell 2018: 186). In this study, the researcher was a participant observer because of his deep involvement in the social setting at the SACSSP by observing the research participants' behaviour and eliciting meanings they attribute to their environment (Bryman 2016: 270).

3.6.4 Document analysis

Document analysis is a process in qualitative social research to analyse non-reactive documents, such as personal documents, official documents derived from the state or private sources, mass-media outputs and virtual documents (Bryman 2016: 546). Based on the information obtained from the body of material that was systematically examined, the researcher is able to find patterns, themes or biases (Leedy et al. 2019: 235). The documents that could be collected for analysis include minutes of meetings, personal journals, official reports, diaries, letters, newspapers, e-mails, living stories, photographs, websites, social media, sound, metaphorical visual narratives and digital archives (Creswell & Creswell 2018: 187).

System documentation, policies (approved or draft) and procedures were requested to build a baseline in preparation for an integrated system. In some cases, no documentation was available, and reverse engineering was performed by analysing the system components and their relationships. A complete listing coded documents utilised in the study is available (See Annexure B). Part of the data collection method was system analysis that described system utilised by the organisation in the succeeding section.

3.6.5 System (applications) analysis

The process consisted of objectively doing quantitative assessments of systems through modelling and simulation, and technical risks analysis in order to assist in technical decision-making for the proposed system architecture based on the organisation’s system requirements (Stevens Institute of Technology 2020: 363). Applications identified in Figure 3-7 were evaluated for data that were useful for future system development planning for the SACSSP’s integrated online system. Proof of qualitative analysis activities are further presented in Annexure F.

Table 3-7: Applications analysis

System	Purpose
SACSSP hardware & software audit	Preparing of AS-IS documentation and checking hardware warranty status and suitability for the proposed ERP solution and new hardware
System benchmarking exercise (Two organisations visited)	Benchmarking with organisations of similar operations to view systems implemented
Telephone and internet connectivity	Investing the telephony installations were able to accommodate VoIP digital phones and video conferencing
Hardware refresh	Invited hardware resellers for presentation on new hardware
SACSSP website portal	Harvesting of information uploaded on the website.

With every research study, the trustworthiness of data is evaluated for reliability and the discussions to that effect is explored in the following section.

3.7 Trustworthy of data

Trustworthiness and authenticity for the study are discussed.

3.7.1 Trustworthiness

The use of diverse strategies in qualitative research can strengthen the trustworthiness and credibility of data that a researcher collects (Leedy et al. 2019: 240). The following strategies can enhance the collection process:

- Triangulation – This involved the researcher analysing data derived from documents, systems, focus groups, and interviews
- Clearly distinguishing between data and reflections/memos
- Seeking of exceptions and contradictory evidence
- The researcher spent considerable time on site that was essential for finding an accurate and multifaceted understanding of the phenomenon under study.

The study utilised five measures of trustworthiness, namely: democratic validity, outcome validity, process validity, dialogue validity and catalytic validity.

3.7.2 Authenticity

The study observed fairness authenticity by giving the participants ample time to review baseline documents that were sent out for comments, and extension was given to update the business process documents (Bryman 2016: 386). Ontological authenticity was addressed by informing the participants about the importance of having correct data under their control and investing in proper IT infrastructure and securing such equipment. According to Given (2016: 61), this study presented multiple realities through the findings on people having comparable beliefs.

3.7.2.1 Democratic validity

Democratic validity was demonstrated through presentations were conducted during quarterly meetings to provide educative authenticity by giving a better perspective of other members in their social settings. The study was a result of a request to the overall current cogent IT system design and the disparaged IT systems inherited that are not compatible with new system innovations to ensure effective and efficient council

operations to support corporate governance (Pickard 2013: 163). Furthermore, democratic validity is depicted in Figures 4-4 on page; 4-8 on page; 4-12 on page; 4-13 on page; 4-18 on page; 4-19 on page; 4-23 on page, 4-24 on page; and 4-25 on page.

3.7.2.2 Outcome validity

According to Pickard (2013: 163), the intervention is demonstrated in the exploratory meeting to digitally transform the SACSSP's operations as highlighted in Figure 4-18. The intervention on the 21 May 2018 and 13 June 2019 resolved that an integrated online system including back-scanning of physical documents must be implemented.

3.7.2.3 Process validity

Process validity is demonstrated in section 4.8.6 in order to align to the desired outcome (Pickard 2013: 164). The consolidated processes to address organisation needs is highlighted in Figure 4-46.

3.7.2.4 Dialogue validity

Benchmarking process indicated in Figures 4-5 on page; 4-20, 4-21 on page and 4-22 on page; conducted as part of reflective dialogue to collect data, design and implementation of the action for digital transformation for SACSSP (Pickard 2013: 164).

3.7.2.5 Catalytic validity

Catalytic authenticity involved the development of an action plan to address the current challenges experienced at the SACSSP as raised by the participants. The process involved the clarification of responsibilities and authority for agreed actions, collaboration plans, accessibility of reports that are produced, and evidence of practical applications (Amin et al. 2020: 1480). Table 3-10 emphasises that the

participants and the researcher focus on really knowing and understanding their reality to ensure that there is change (Pickard 2013: 164).

Table 3-10: Catalytic authenticity process

Collaboration Plans	Responsibility	Accessibility of reports	Evidence of practical application
Organisational processes	Researcher and division's managers	Processes were sent to managers through emails	Approved process document was issued as an annexure of tender for system development (Figure 4-46 – consolidated processes)
System requirements	Researcher and IT and Business Re-engineering Committee	System requirements were sent to the committee and discussed during meetings	<u>Tender document:</u> Appointment of service provider for the development of the integrated online system for a period of two years. BID NO: SACSSP/02/2020
Hardware requirements	Researcher and IT and Business Re-engineering Committee	Hardware analysis was done and report was sent to the committee for consideration and approval	Proposed server hardware solution (Figure 4-27)
Benchmarking exercises	Researcher, communication officer, finance manager and registration manager	Benchmarking exercise report shared with all stakeholders	Drafted AS-IS document. Similar organisation Hardware benchmarking visit (Figure 4-20)

The study has tactically empowered the SACSSP staff to better understand their environment and document every project in which the members were involved.

3.8 DATA ANALYSIS AND PRESENTATION

Data were analysed thematically as per the objectives of the study, which were based on constructs from the COBIT framework in Table 3-11. Interview transcripts, documents, pictures were uploaded into a computer assisted qualitative data analysis software, Atlas Ti 9, to be coded and analysed. The thematic analysed data identified themes that led to coding of such data.

Table 3-11: COBIT 2019 constructs questions linkage

COBIT 2019 framework constructs	Research questions
Evaluate, direct and monitor	How can information governance be used for the evaluation, direction and monitoring of the SACSSP's strategy by the board members?
Align, plan and organise	How can information governance planning assist in business alignment?
Build, acquire and implement	What programmes and projects can be implemented by the SACSSP to support business processes?
Deliver, service and support	How can the outcomes of information governance and related technologies be reviewed?
Monitor evaluate and assess	What monitoring can be provided to bring transparency of performance and conformance to drive the achievement of goals by management?

The primary concern for any research study is to protect all participants and data collected. The successive section presents ethical consideration for the study.

3.9 ETHICAL CONSIDERATIONS

For the ethical issues that arose during the study, ethical clearance was requested as prescribed by the policy of Unisa. One of the ethical principles in governing research

is that people should never participate in research unless they had voluntarily agreed to do so (Neuman 2014). The researcher observed the policy by requesting ethical clearance from UNISA (Annexure C), and further approval was received to access the data collection site and the population under study at the SACSSP (See Annexure D). All pictures taken during the study were presented to management and permission was granted to include them in the study. According to Unisa (2013: 2), the policy on research ethics aims to:

- “Enable researchers to enhance their capability to undertake ethical research and maintain their independence, especially when confronted with undue influence or pressure which may compromise their integrity or that of their research.
- Discourage unethical research practice.
- Serve as a basis for policymakers and provide an enabling environment for the practice of ethical research.
- Provide an additional resource for the teaching and training of students in research and ethical practice.
- Make ethics an integral part of the planning and methodology of research.
- Preserve and promote the autonomy, quality, legitimacy and credibility of research.
- Protect and promote the rights of research participants and honour their trust in researchers and research.
- Strengthen the research ethics review system in the university where research involves human participants, animals, data, institution or other living or genetically modified organisms.”

Leedy et al. (2019: 121–123) present the following four categories that are widely accepted in the scientific community as fundamentals of the enquiry process and are regarded as ethical foundations:

- Protection of respondents from any harm
- Voluntary and informed participation

- Respect right to privacy
- Honesty with professional colleagues

One of the ethical principles in governing research is that people should never participate in research unless they had voluntarily agreed to do so (Neuman 2014: 149). All the sources used in the study were cited and the Turnitin® plagiarism detection software solution was used for the promotion the researcher's work integrity.

3.10 EVALUATION OF RESEARCH METHODOLOGY

The researcher made use of a qualitative approach and PAR as a method to collect qualitative data. The foundation of this study followed a critical emancipatory ontology and transformation epistemology. The different levels of the covid-19 lockdown made it difficult to access the research site and presented connectivity problems for participants to gain access. The involvement of the researcher was mainly as an advisor and participant in IT and Business Re-engineering Committee meetings related to the development of proposed integrated online system. In order to address bias, the research findings were reviewed by peers to identify things that might have been missed or gaps that were not addressed. Participatory action research is recommended in other settings because its role is designed and led by a specific community that and solve a problem using three phases look, think and act.

To address the shortcomings, the research made use of the Microsoft Teams® video-conferencing solution to attend focus groups meetings and Zoom® video communication to conduct interviews. While this form of engagement was applied, it became difficult to find participants in their environment of study. The virtual gathering was a limiting factor to collect data.

3.11 SUMMARY

The research methodology was discussed and the choice of data collection tool explained. The study used interviews, focus groups, observation and document analysis to collect data, as informed by the research problem. The population relevant to the study was found through the purposive sampling method. The ethical considerations of the study were explained and that the values and standards would be upheld when conducting the research. The following chapter focuses on the presentation of the results that were obtained from the interviews, focus groups, observations and document analysis.

CHAPTER FOUR

ANALYSIS AND PRESENTATION OF RESULTS

4.1 INTRODUCTION

The previous chapter described the methodology that was applied in this study and the data collection tools used to find answers to the research questions. This chapter focuses on the analysis and interpretation of data collected from the selected participants, observations, system and document analysis in the study to draw conclusions and generalise the findings to a problem statement (Creswell 2014: 163). The research objectives were adopted from the COBIT 2019 framework. The questions asked in focus groups and interviews were structured interview schedule. Furthermore, the results of data collected from participants were presented in the form of themes, charts, tables and graphics to assess whether the research questions were adequately addressed and responded to as per the objectives of the study. The following section presents the analysis of data collected from the interviews and focus groups. Themes were listed and followed by the sub-themes; examples of quotations to support the sub-themes and interpretation are also presented.

4.2 PARTICIPANTS' PROFILE

The participants of this study were drawn from various departments and governance structures at the research site, that is, administration, benchmarking and the board. Figure 4-1 below presents the participants' profile mapping, providing a clear view of where participants were drawn from.

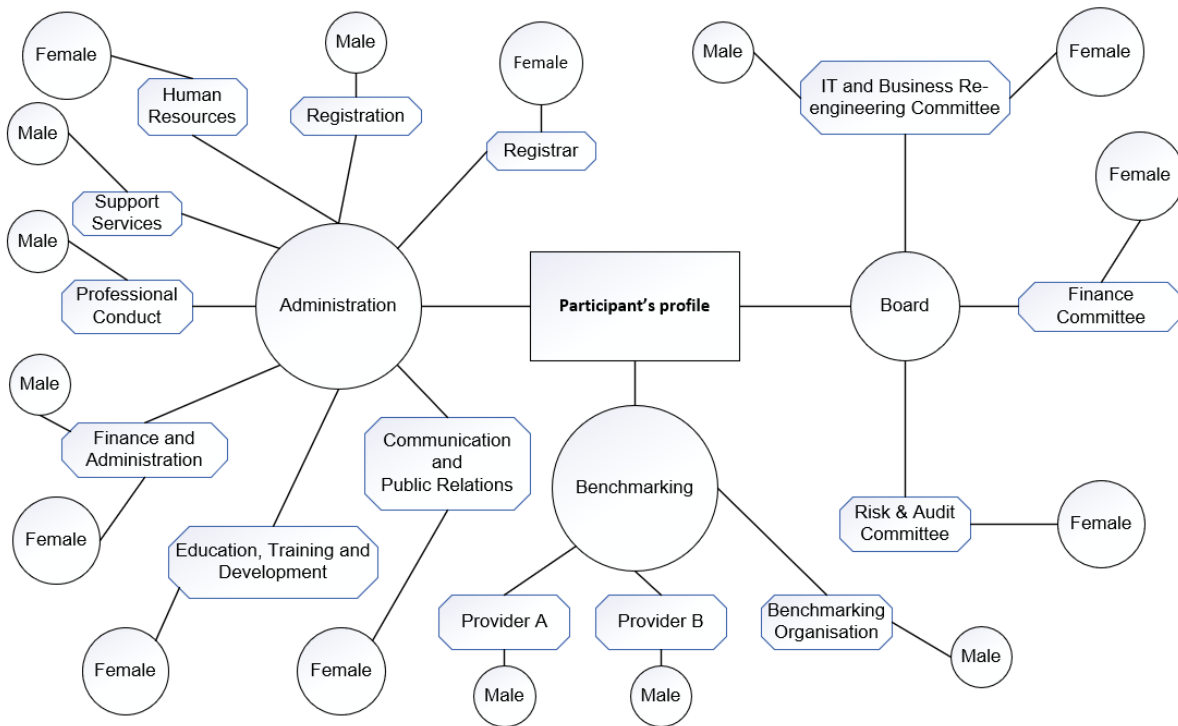


Figure 4-1: Participants profile

From Figure 4-1, it can be noted that representatives from three board committees, that is, Risk and Audit Committee, Finance Committee, and Information Technology and Business Re-engineering Committee, also participated in this study. The participation of these participants provided insights from a strategic level to understand how governance-related issues are being handled. The participants from administration were instrumental in aligning strategical and operational issues across the four domains.

4.3 DATA ANALYSIS PRESENTATION

The results are presented in themes that were derived from the participants' one-on-one semi-structured interviews, focus groups, and various organisational document analysis such as board committee meetings. See Figure 4-2 for data groupings.

	Name ▲	Size	Created by	Created
◇◇	APO	14	Tshepo Chauke	2021/07/11 14:11
◇◇	BAI	11	Tshepo Chauke	2021/07/11 14:58
◇◇	DSS	6	Tshepo Chauke	2021/07/11 15:07
◇◇	EDM	5	Tshepo Chauke	2021/07/11 13:16
◇◇	MEA	4	Tshepo Chauke	2021/07/11 15:20

Figure 4-2: Data groupings

From the five data groups presented in Figure 4-2, a total of 607 quotations were generated which were later grouped as per the domains of the COBIT framework adapted to this study’s theoretical framework (Figure 4-3).

ID	Reference	Name	Text Content	Document
231:1	p 8		Only 22 % of social workers received a salary increase in 2020; 21% di	solidarity Social workers Guild-comments
234:1	p 9		SERVERS Specifications Price (VAT Included) Dell PowerEdge R540 Ser	SUPPLY AND DELIVERY OF ICT HARDWARE AND SOFTWARE...
234:2	p 10		VEEAM AVAILABILITY LICENSES Specifications Price (VAT Included) Vee	SUPPLY AND DELIVERY OF ICT HARDWARE AND SOFTWARE...
237:1	874 × 601		System development tender picture.PNG	System development tender picture
239:1	¶ 9 – 30		New application learners CPD event applications - providers Complaint	TEMPLATE BUSINESS PROCESS MAPPING
239:2	¶ 1 – 30		TEMPLATE FOR BUSINESS PROCESS MAPPING: SACSSP List the process...	TEMPLATE BUSINESS PROCESS MAPPING
246:1	p 1		Attached herewith is the Website redesign content. The service provider	WEBSITE DESIGN - plan
247:1	¶ 466 – 468		Stakeholder enquiries Email address and other contact details where st	website redesign content not structure
247:2	¶ 37 – 127		SOUTH AFRICAN COUNCIL FOR SOCIAL SERVICE PROFESSIONS HOME...	website redesign content not structure
248:1	770 × 323		Wrongly divided server room.PNG	Wrongly divided server room

Figure 4-3: Quotations generated

After the successful completion of the data coding, the researcher reviewed the codes for commonalities and grouped them into themes which were guided by the theoretical framework adopted for this

The following sections present and discuss the study's results in detail.

4.4 PRESENTATION AND DISCUSSION OF RESULTS

This section presents and interprets the results of this study from the data collected. As outlined in chapter one, the specific research objectives were to determine how information governance can ensure that corporate governance plays a role in the evaluation, direction and monitoring of the council's strategy, to review how the information governance planning can assist in business alignment at the SACSSP, to determine how the SACSSP can implement programmes and projects that support business processes, to review the outcomes of information governance and related technologies as per the planning, to establish how information governance can provide transparency in the monitoring of performance and conformance to drive achievement of the goals, and to suggest an information governance framework for the SACSSP.

In order to strengthen the researcher's arguments, examples of quotations from the collected data was provided. The quotations extracted from the semi-structured interviews will be identified by the letter "P" followed by the number representing the participants, that is, p1 for participant 1 and so forth. While quotations from the document analysis will be identified by the letter "D" followed by the number representing document listing.

Therefore, to ensure that the listed objectives were achieved, the following themes were generated.

4.5 THEME ONE: EVALUATION, DIRECTION AND MONITOR

This theme is about understanding some of the characteristic of the SACSSP in relation to how information governance can ensure that corporate governance plays a role in the evaluation, direction and monitoring of the council's strategy. In doing so, the following sub-themes were generated from the collected data.

Governance framework setting and maintenance; Benefits delivery; Risk optimisation; Resource optimisation; and Stakeholder engagement.

4.5.1 Governance framework setting and maintenance

The collected data from the document analysis indicated that the SACSSP had adopted the King Code of Governance Principles as a guidance or a framework for its governance. The following are quotations to support this view:

“The establishment, management, maintenance and monitoring of council record keeping is guided by King IV’s principle, which states that the governing body should govern technology and information in a way that supports the organisation setting and achieving its strategic objectives.” (D4)

“Council also adopted the ‘King Report on Governance for South Africa’, and the ‘King Code of Governance Principles’ to guide its conduct and governance.” (D2)

The quotations above as highlighted in the sub-theme indicated that the King Code of Governance principles were adopted, documentary evidence was presented and different governance structures were in operation. Organisational management, the council, and section nine and ten committees’ calendars were published at the beginning of the year and scheduled meetings were attended quarterly. The current board adopted nine strategic objectives that the SACSSP needed to achieve in the five years (2016 to 2021), together with its professional boards.

The setting of the organisation’s framework is arranged into mission, goals and objectives, as stated on the approved strategic document and the website of the organisation. The governance of the council and its professional boards is guided by the Social Professions Act 110 of 1978 and the regulations thereto.

4.5.2 BENEFITS DELIVERY

This sub-theme was about establishing and understanding whether participants believed that they did derive some value from the use and adoption of information technology. Therefore, interview questions such as “How do you get value from the use of IT?” and “Are end users satisfied with the quality of IT service?” were asked to the participants. It is important to note that where participants’ responses were similar or sounded the same, they were grouped and treated as one.

Most of the participants indicated that they did derive value from using information and technology and they were satisfied with the quality of IT services they received. The following are examples of comments from participants:

“I get value from the use of IT. Communication is easier when using technology. I am satisfied with quality and faster response times” (P5)

“Get value and it simplifies how we do things. Quick turnaround times. Yes, users are satisfied because it is prompt and swift. Closed quicker.” (P2)

“We get value for money in terms of IT. It reduces the time you take to prepare reports and moving away from manual work. Quicker way of responding and integrate the process together and reduction of processing of tasks.” (P1)

The respondents did acknowledge that there were some benefits to the use of information technology, as it simplifies communication and reduces paperwork. Even though participants indicated that value could be derived from information technology, a few participants expressed their frustration with the use of the technology.

“The frustration is access to data and develop our own reports. Lack of integration, as well as doing work manually. Registration – manual

registration. Real files and work manually. Not efficient, time wasting.” (P3)

“I can’t work from home because we don’t have VPN...” (P7)

The participants’ responses showed that even though they were satisfied with the use of technology, there were some areas in which the organisation should improve to increase efficiencies. The participants indicated that access to data should be improved to allow them to develop their own reports. Additional functionality such as a VPN, processes and systems integration might be of great value.

4.5.3 Risk optimisation

This sub-theme was about establishing and understanding how the organisation addressed the IT-related risks. In order to extract the organisational characteristics in relation to IT risk, the following question was asked “Did you address all IT-related risks?”

The participants were of the opinion that all IT-related risks in the organisation were addressed and mitigated. The participants indicated that the organisation did perform daily and quarterly reviews of the IT-related risk and did make sure that the required resources to mitigate those risks were provided or catered for. Examples of participants’ comments are shown below:

“All IT risks are minimised, especially finance and registration and all risk. Ransom malware. Can never be ready for these attacks. Reactive and now tighten the firewall for those risks not to take place. Review on quarterly basis. Review risks as they happen. Ensure that what IT needs to address the risks is catered for. Plan in the beginning of the year; all risks are addressed.” (P1)

“Yes, and are monitoring emerging risks daily.” (P4)

Participants further indicated that they did address the IT-related risk in accordance with their risk level:

“We do address IT-related risk depending on the risk level...” (P2)

The study revealed that there were some critical information technology policies that were not documented in the organisation. This was identified from the participants’ responses, which indicated that only when a new associate was hired, it was pointed out that the organisation should not allow people to bring their own external hard drives, as it exposes the organisation to viruses.

“When we hired IT person. We were hit by a virus. He made us aware not to bring external hard drives and not open spam emails.” (P5)

From the participants’ responses, it can be noted that the organisation did not have IT policies in place or the policies did not cover critical components, such as Bring Your Own Devices (BYOD). As a result, the absence of this policy or coverage placed the organisation at risk as they were hit by a virus.

4.5.4 Resource optimisation

Most of the participants indicated that there were sufficient IT resources to meet the required enterprise strategic objectives. The participants stated that new servers and laptops were procured to increase productivity. Below are some of the responses:

“Currently, we have a whole new equipment. These are going to meet the strategic objective.” (P2)

“Current implementation will take us there. Immediate needs we identified and the plan is correct. Budget allocation has moved and satisfied to move the plan forward. Look at lifestyle management to

come with a forward plan. Avoid the ad hoc requests and look at long-term extension.” (P3)

“We are getting them slowly” (P4)

“Now we have sufficient IT resources. Replacing old and slow laptops and productivity has increased.” (P5)

“I feel that the structure is fine and responding to the needs of the organisation. The improvement that can happen is the capability to work from home.” (P6)

“We have built a new server system, bought the latest high-end laptops and desktops. In process to digitise certification, avoid onsite certificate and receipt collection. The internet speed and connection improved.” (P8)

There were three participants who indicated that there were still not enough resources, as stated below:

“No, we plan how we execute IT projects. Not enough funds...” (P1)

“Not enough. We still in short of digitising of documents because the store rooms are full and there is no longer space to store more.” (P5)

“Not enough resources and shortage of staff. According to me, I am happy.” (P7)

From most of the participants’ responses, it was clear that they were impressed by the resource improvements of computing hardware and internet speed improvements. A conclusion can be drawn that those who indicated that there were not enough resources were considering issues of digitisation, finances and shortage of staff.

4.5.5 Stakeholder engagement

Document analysis was performed and the SACSSP was found to have stated in the strategic plan that one of the objectives was to “*Nurture and consolidate partnerships and stakeholder relations (nationally, regionally and internationally)*”. The key stakeholders indicated in Table 4-1 were identified at the SACSSP through the promulgation of the Act (RSA 1998: 6).

Table 4-1: Key stakeholders for the SACSSP

Stakeholder	Role
Board and executive	The provision of guidance regarding stakeholder needs (including customer needs), business strategy, priorities, objectives and guiding principles with respect to EGIT
Organisational management	Management, together with IT, ensures that stakeholder needs and business objectives are stated with sufficient clarity to enable translation into business goals for I&T.
Staff	Provision of business processes and consumer of I&T services at the SACSSP
Department of Social Development	Provision of legislative / policy direction and appointment of board members for the SACSSP and training of social service professionals (RSA 2020: 11)
Internal audit	Performs an appropriate audit for internal organisation and provide audit findings and recommendations to take appropriate remedial action (RSA 2018: 6)
IT & Business Re-engineering Committee	The ICT steering committee, which coordinates and oversees the planning, implementation and execution of the corporate IT governance and strategic alignment and related monitoring activities (RSA 2014: 9)
Finance Committee	Oversees a financial oversight system compliant with applicable and appropriate frameworks place
Social service practitioners	A primary stakeholder who can be registered based on prescribed qualifications and to the satisfaction of conditions to practice in the profession of social work (RSA 1978: 17)

Stakeholder	Role
University students	Required to register as social auxiliary workers with the SACSSP from the second year of study or where they are involved with social work learning in a real-life situation (RSA 2011: 2)
Social Work training institutions	Determination of prescribed qualifications (continuing professional development (CPD)) and standards that are acceptable for social service professionals and accreditation of training providers
Industry (Professional associations)	The professional organisations that social service practitioners can belong to: <ul style="list-style-type: none"> • South African Association for Social Workers in Private Practice (SAASWIPP) • National Association of Social Workers in South Africa • Association of South African Social Work Education Institutions • National Association of Social Workers (South Africa) • National Association of Child Care Workers (NACCW)
Third party providers	Provision of services to the SACSSP
Qualifications assurance authority	Verification of qualifications submitted. The stakeholder does “the evaluation and processing of applications for recognition of professional bodies and registration of professional designations for the purposes of the National Qualifications Framework Act 67 of 2008” (SACSSP 2019b: 4)

Adapted from COBIT 2019 Implementation Guide: ISACA (2018c: 50)

The responses from interview participants revealed the following to the question “How long does it take to make major IT decisions?”

“Takes long because going to relevant structures (management, IT & Business re-engineering are involved.” (P1)

“It takes quite some time. It starts from management, IT Committee and Exco. It cannot resolve some things such as funding and it takes a long time.” (P2)

“Not a long process. Take a submission to committee and take this to council and Exco to approve. Operational takes long and the implementation gets delayed. Delays: Submissions from management and not meeting timeously or taking it for round-robin.” (P3)

“It used to depend on availability of IT and Business Re-engineering Committee members who must make recommendations for Finance Committee and Exco. Fortunately, with the advent of covid-19, the attendance of virtual meetings and quorums has improved. The turnaround time is shorter than when we held face to face meetings.” (P4)

“It takes about three to six months. For instance, system development project had to go through different committees for approval.” (P5)

“It takes too much time. It must go to all the committees (IT and Business Re-engineering, Exco and council.” (P6)

“It takes long. IT develops specifications and SCM advertises. Once proposals are received, they go to IT and Business Re-engineering and Finance Committee for evaluation and recommendation. Then it is sent to Exco and finally to council for approval.” (P7)

Participants agreed when responding about stakeholders (structures) involved when making decisions within the organisation. What was clear was that there were checks and balances when approval processes were sought. One positive aspect was that the

covid-19 pandemic brought the adoption of virtual conferencing solutions that ensure that a quorum can be formed in order to speed up approval processes. The improvements brought by / implemented because of Covid-19 should be retained once work schedule returns to normality

4.6 THEME TWO: ALIGN, PLAN AND ORGANISE

The purpose of this theme was to review how the information governance planning could assist in business alignment at the SACSSP as per objective section 1.3 of chapter one. The said section covers the following sub-themes:

Managed I&T management framework; Strategic management; Innovation management; Portfolio management; Budget and cost management; Human resources management; Relationships management; Service agreements; Vendor management; Quality management; Risk management; Security management; and Data management.

4.6.1 Information and technology management framework

The presentation of responses satisfies the objective in section 1.3 of chapter one to identify the I&T management framework for successful planning for the organisation. Document analysis was conducted and the study revealed that the I&T management framework components assisted with the accountability and responsibilities with regard to ICT functions and operations. Some of the documents found to assist with the development are presented in Table 4-2.

Table 4-2: I&T management components

Doc #	Document	Purpose of document
D29	Public Finance Management act	“To regulate financial management in the national government and provincial governments; to ensure that all revenue, expenditure, assets and liabilities of those governments are managed efficiently and effectively; to

Doc #	Document	Purpose of document
		provide for the responsibilities of persons entrusted with financial management in those governments; and to provide for matters connected therewith.” (RSA 1999: 2)
D22	Governance framework	The institutionalising of governance of IT by providing the principles and practices that must be complied with and the implementation approach that can be used in organisations to tailor their governance solution (ISACA 2018e: 15)
D4	Corporate governance	It is “...an exercise of ethical and effective leadership by the governing body towards the achievement of the following governance outcomes <ul style="list-style-type: none"> • Ethical culture • Good performance • Effective control • Legitimacy” (IODSA 2016: 11)
D3	Records management policy	It “...is an essential part of good corporate governance of any organisation and facilitates accountability and transparency. Record keeping in a systematic manner is important for the day-to-day management of financial and non-financial information of an organisation, while it also underpins its ability to participate in internal audits as well as external audits”. (Ngoepe & Ngulube 2014)
D1 D2	Social service professions act and regulations	“To provide for the establishment of a south African Council for Social Service Professions and to define its powers and functions; for the registration of social workers, social auxiliary workers and persons practicing other professions in respect of which professional boards have been established; for control over the professions regulated under this act; and for incidental matters.” (RSA 1978: 1)
D21	Risk management policy	The process that will enable management to identify, asses and manage risks in the face of uncertainty and is, therefore, integral to stakeholder value creation and preservation. This gives guidance to the organisational

Doc #	Document	Purpose of document
		risk response whenever I&T-related risk exceeds tolerance (ISACA 2020: 10).
D30	Social development strategic plan	Assisting in professionalising the social service provider (SSP) through training (bursaries) and capacity building. (RSA 2020c)

The tabled documents regulate how the organisation aligns its daily operations to the approved strategic plan. The assessment and reporting of organisations give assurance to the SACSSP's stakeholders on performance and stated goals.

4.6.2 Strategic management

This sub-theme revealed that the SACSSP developed a five-year strategy document that was approved and published on 31 August 2017. The strategy's purpose was anticipated to achieve the digitisation of current physical records and automating to address IG. As highlighted, IG challenges found in the document analysis related to the SACSSP strategic plan (2016 – 2021):

- “Inadequate IT system
- Unreliable database
- No synergy between systems”

The following are the responses of five participants to the question: “Is IT standing in the way of executing the business strategy?” The question was asked to find out if the organisation had performance measures in place to monitor targets, as stated in the annual performance plan (APP).

“We have got an annual performance plan to manage IT performance...” (P1)

“Clearly define IT strategy that will define our strategy to meet organisational objectives.” (P2)

“Systems bought must support strategy. Delays in getting to a point to get a provider. Standing in the way of enterprise strategy.” (P3)

“No, it is not. It actually enhances business strategy and access.” (P4)

“This will help the business to deliver on its business strategy.” (P5)

It can be concluded that the organisation has clear performance goals and strategy that can guide organisational operations. Five participants viewed IT as enhancing and helping business to achieve its strategy.

4.6.3 Enterprise architecture

Two quotations are depicted in the enterprise architecture sub-theme. Most of the participants did not have an opinion on the sub-theme enterprise architecture. The responses obtained during the interviews were noted as:

“All divisions of council – registrations, professional conduct, ETD, finance and the office of the registrar and the strategic units require IT.” (P4)

“We’re working towards holding the whole architecture locally on site...” (P8)

Inference can be made that most of the participants had not been exposed to enterprise architecture. The responses of the two participants who mentioned EA did not relate to any established framework such as GWEA.

4.6.4 Innovation

The Innovation matters as depicted in Figure 4-4, were discussed in an exploratory meeting held on the 21st May 2018. The three initial requirements that were prioritised for system overhaul: Registration management; Digitisation of archives; and online registration and integration of organisational systems. The discussion resolved to

address the biggest challenge of integration and obsolete systems that is not compatible with new innovations.

Automation and digitisation of the Register and Files

- d) Register management (registrants' database)
- e) Digitisation of the archives (reduction of carbon footprint)
- f) Online registration and integration of Council systems (reduction of carbon footprint)

Figure 4-4: Innovation discussion items

Lack of innovation has prompted in addressing the current limitations of practice certificates that are prone to fraud. The organisation together with the researcher conducted three benchmarking processes of digitising the certificates in order to address innovation challenges. Two service providers were invited to present on their offerings. The first company wanted to completely control the issuance of the certificates with a requirement that the SACSSP should provide a comma separated values (CSV) files with list of social service professionals to the service provider.

The benchmarking process for digital certificates meeting held on the 05th February 2020. The innovation process included the conversion of manual and generate digital certificate and offer storage the created certificates into the service provider's digital vault. Benchmarking with the second service provider provided a proposal of development of a certificate vault that would be inhouse to be integrated with the enterprise resource planning (ERP) system and did not involve any human intervention. The discussions for the proposed solution addressed the innovation of the digital certificates concerns as noted in Figure 4-5.

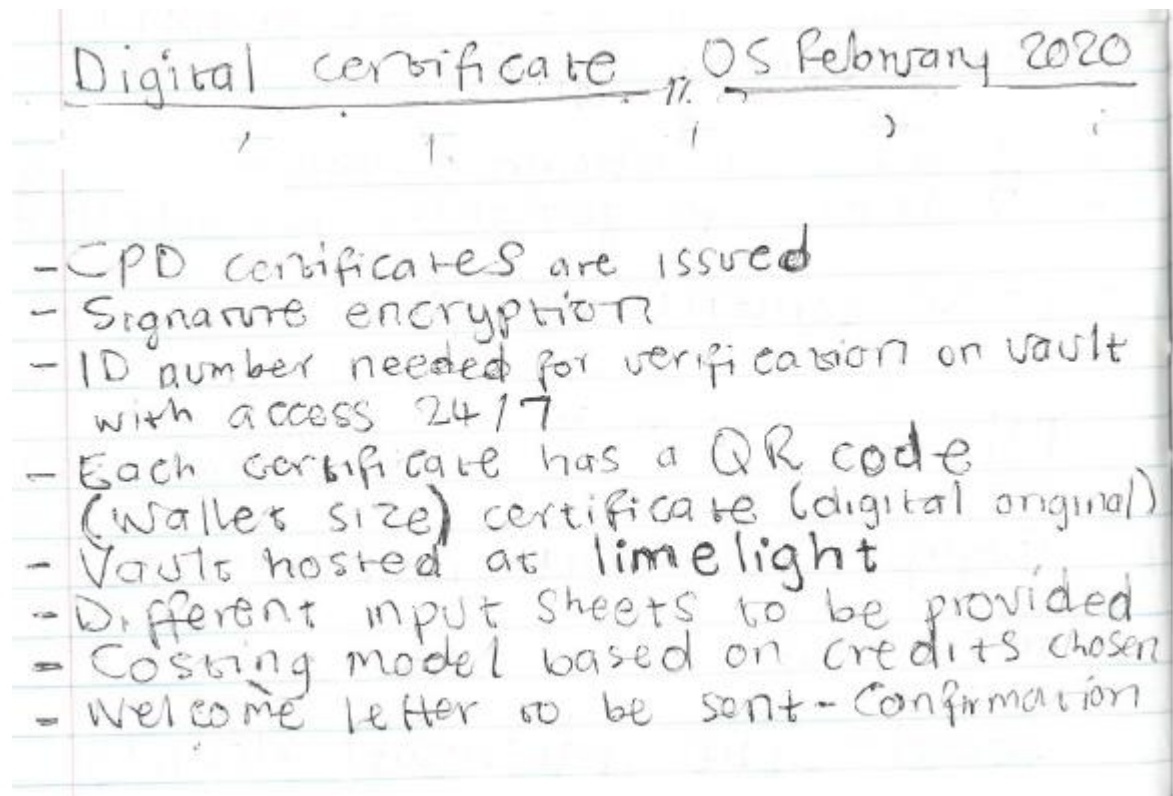


Figure 4-5: Focus group meeting - Digital certificates

An additional question was also posed to the interviewees to understand what are the innovation solutions that they might bring to improve the organisational IT environment. The following question was therefore asked: *“How do you improve business agility through a more flexible IT environment?”*

According to the participants, there is a need for the information systems revamped. Example of participants comment:

“The system to be revamped and be aligned to new technologies. We have done market benchmarking with other councils to see which systems are implemented and review what can be implemented. Have put a budget aside and come with a system with new functionalities; come with online applications and integrated with financial application. System responsive to the market to serve.” (P1)

“We are still in a process to secure agile system for the whole enterprise...” (P8)

The benchmarking process conducted was part of innovation components that can be included in the integrated online system. The organisation allocated a budget to the proposed system to include functionalities such as registration and other divisions.

4.6.4.1 Internet of things

The analysis of the SACSSP act as amended including the applicable regulations revealed that the SACSSP requires access to data from different institutions for identity, qualifications as per operational requirements (D1, D2, D4, D12, D20). Table 4.3 indicates data sources that the SACSSP has access in order to be able to execute its mandate. The current method of interface has human intervention, which could lead to manipulation since it is not connected directly from the source data (D23). What became evident was that when a request was sent to the Department of Home Affairs for access to the population register, their main aim was to be in line with the Privacy of Personal Information (POPI) Act in protecting the privacy of citizens using a “data protection measures questionnaire” to be filled in before access is given to verify from the population register. The Child Protection Act also has strict access to the National Child Protection Register against unauthorised intrusion (RSA 2006) (D31).

Table 4-3: SACSSP data sources

Data source (sensor)	Type of information	Institution	Type of access
Police clearance	Fitness verification	South African Police Service (SAPS)	Students apply themselves to the SAPS and provide the certified copy of Identity card/document and prescribed payment.
National child protection Register	Verification on suitability to work with children	Department of Social Development	Through application to the Director-General of Department of Social Development using the prescribed format and sending the completed form to the department for verification.
Population register	Identity verification	Department of Home Affairs	No identity verification has been done yet.
Training institution	Academic records	Universities	Students bring the certified copies of academic records.
Finance system	Confirmation that all due amounts have been paid	Internal	Registration enquires with Finance if the payment is reflecting.
Banking	Payment confirmation from social service professionals	SACSSP bank	A social service professional submits proof of payment and it is verified against the bank statement.
Qualification accreditation	Foreign qualifications, national learner records verification, tertiary qualifications verifications	South African Qualification Authority	File with learner/student details sent to a dedicated email address.
Application forms	Registration details	Social service professionals	Complete the forms and email, fax or submit the physical forms to the office.

Table 4-3: SACSSP data sources for verification type / source results in producing verification reports (See Annexure G for more information). The following section is the data presentation of data collected for artificial intelligence.

4.6.4.2 Artificial intelligence

The researchers found that there were no underlying technologies for the implementation of artificial intelligence (AI). Core services of the SACSSP are dealing with registration-related services such as requirements for registrations, foreign applications, registrations fees, restoration, banking details, and enquiries that one can make to the SACSSP. When asked about reporting to management and stakeholders, three focus group participants responded as follows:

“We currently verify applications, academic records and certificates for authenticity by observing the quality of a document and checking qualifying content” (P1)

“We used to have a call centre system and staff manning the calls; however, the system was replaced by a keyboard system here. The old system used to give statistics of calls handled and those lost. I normally speak to a person on average for about five minutes and in the process, I lose four calls. I use guesswork if I’m asked the number of calls I received” (P2)

“We used to have a call centre that came with the previous telephone system and it used to give us monthly statistics of calls attended and those that were dropped. Ever since the contract ended, there is nothing in place.” (P7)

The presence or lack of portfolio of services for the organisation is outlined in the next section.

4.6.5 Portfolio management

The portfolio of services offered is not clearly catalogued; however, the following can be found on the SACSSP website: searching of the status of the service professional. Figure 4-6 is a depiction of the input screen that displays when a potential employer or a member of the public wants to search a social service professional.

Search The Register

Registers are updated on a daily basis. If a practitioners name does not appear on the register, kindly contact Council Administration on 012 3568300 during office hours, for the practitioners status. Enter search text and click the **[Search]** button. Search using registration number, name, surname or employer name. Results will only reflect **Registered** or **Restored SOCIAL** and **SOCIAL AUXILIARY WORKERS**.

Search Text :

Reg. No.	Names	Surname	Type	Employer	
No Results!					

Figure 4-6: Search a register

A member of the public can lodge a complaint against a social service professional using a form downloadable from the SACSSP website (D1, D2). The screenshot depicted in Figure 4-7 is followed once a complaint is received. It was found that complaint forms could be accessed on the website, by asking the office to email or fax, and through walk-ins. The completed forms were submitted by hand, faxed or emailed. (D8)

Lodge A Complaint

Complaint Form

Complaint Form

Figure 4-7: Complaints management

Two stages were indicated in the process of dealing with claims and Figure 4-8 depicts the whole process (D8):

Stage one:

- Verification of the registration status of the respondent. The registration database and retrieval of a file from archive were accessed.
- The assessment the complaint is done to determine whether the organisation has jurisdiction to process the complaint lodged.
- If the person is not registered, the matter becomes a criminal matter and the client (complainant) is advised to lay criminal charges.
- If the person against whom a complaint is lodged, is registered, the SACSSP has the jurisdiction to print the documents and open a file accordingly.
- A letter of notice is prepared and processed to the respondent and request him/her to respond within 21 days upon receipt of the letter. All documents from the complainant are attached to the letter of notice.
- A copy of the letter of notice to the respondent is sent to the complainant for noting.
- If the office does not have jurisdiction, the client is advised on possible mechanisms to pursue his/her matter and the office closes the matter.
- Registration-related services such as requirements for registrations, foreign applications, registrations fees, restoration, banking details and enquiries that one can make to the SACSSP.

Stage two:

Upon receipt of the response from the respondent, it is printed and filed. If a response has not been received by the due date, the professional conduct division would follow up with the respondent. When respondents request extension, the office would assess their reasons for such request before granting or declining the request. The process moves to the Registrar Committee for Professional Conduct (RCPC) for further processing. Based on the weight of the matter at hand, the complaint is referred to the Committee for Preliminary Inquiry (CPI) for further investigation. The CPI process deals with matters referred to it by the RCPC as far as complaints against Social Service Professionals (SSPs) are concerned. (D8)

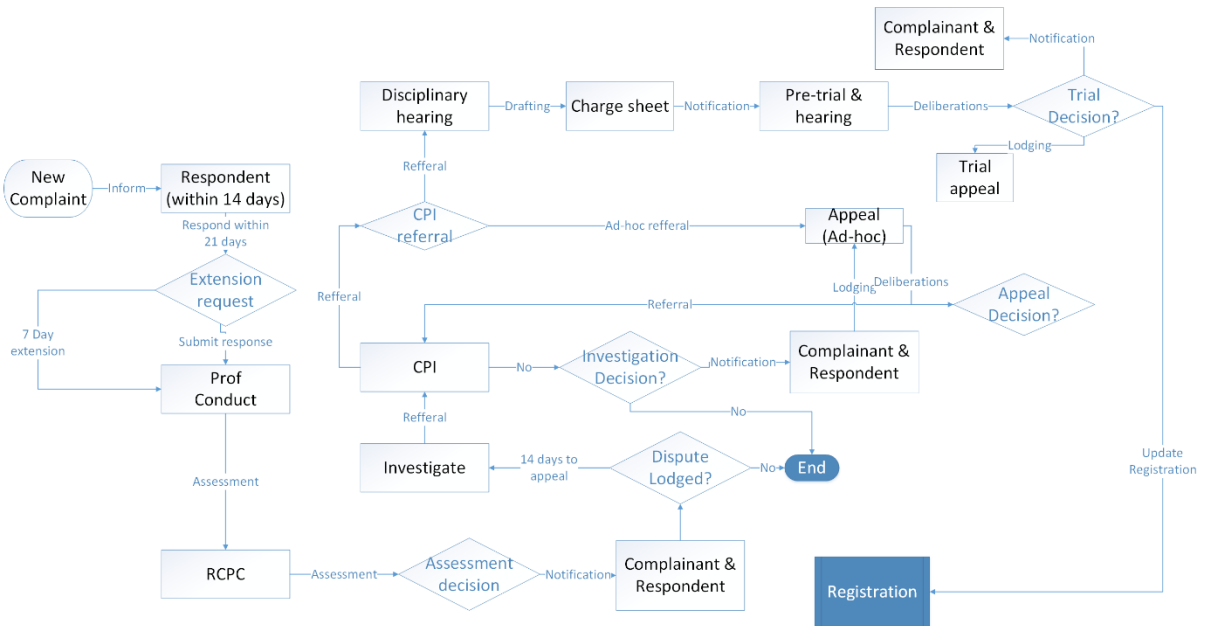


Figure 4-8: Professional conduct process

Based on system analysis, all the registration services highlighted in Figure 4-9 are available on the corporate website. These services are regarded as fundamental to the council’s functioning.

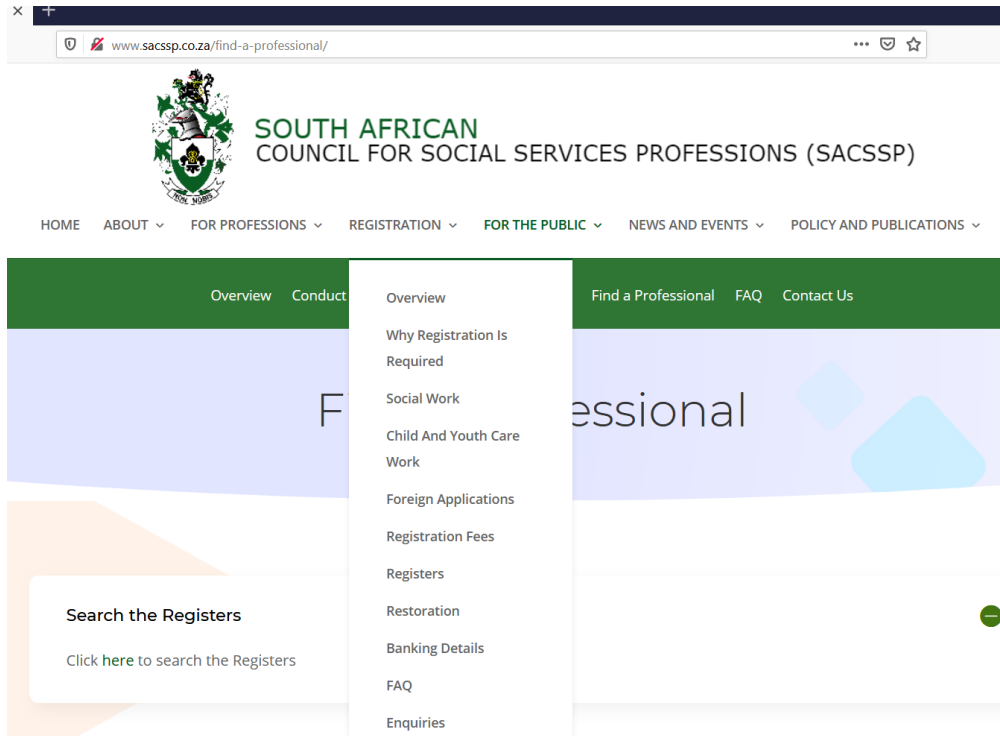


Figure 4-9: Registration services

While the current sub-theme presented the services provided by SACSSP, the next section shows the budgeting and costing results.

4.6.6 Budgeting and costing

The budget and costing sub-theme present data derived from official documents presented in different fora. The organisation has adopted a strategic objective that ensures (D4):

“An effective financial management system compliant with applicable and appropriate financial frameworks is in place and fully functional”.

The approved budget in Figure 4-10 was presented to the Portfolio Committee of Social Development. MTEF budget 2018 – 2021 was presented. (D13, D28)

South African
Council for Social Service Professions (SACSSP)



PROGRAMME	2017/18 Actual (R)	2018/19 Budget (R)	2019/20 Budget (R)	2020/21 Budget (R)	MTEF
TOTAL INCOME	15 723 500	19 999 177	22 239 647	24 781 181	67 020 004
TOTAL PROGRAMME COST	13 646 677	21 962 377	37 425 126	42 512 598	101 900 102
PROGRAMME 1: ADMINISTRATION	8 722 805	12 228 548	20 485 988	21 936 795	60 294 720
- SUB-PROGRAMME: OFFICE OF THE REGISTRAR	2 102 478	2 646 859	5 170 672	5 563 219	15 483 228
- SUB-PROGRAMME: FINANCE & ADMINISTRATION	3 540 910	4 707 654	6 745 021	7 328 275	22 321 860
- SUB-PROGRAMME: ORGANISATIONAL TRANSFORMATION	-	595 001	632 500	695 750	1 923 252
- SUB-PROGRAMME: HUMAN RESOURCES	1 170 011	1 741 870	2 550 447	2 713 763	7 006 080
- SUB-PROGRAMME: INFO, COMMS AND TECHNOLOGY	-	424 345	1 576 559	1 703 005	3 703 908
- SUB-PROGRAMME: PUBLIC RELATIONS AND COMMS	536 907	586 133	1 140 278	995 222	2 721 633
- SUB-PROGRAMME: GOVERNANCE STRUCTURES	1 372 498	1 526 687	2 670 510	2 937 561	7 134 759
PROGRAMME 2: REGISTRATION	2 951 605	4 509 201	5 798 944	8 749 651	19 057 795
PROGRAMME 3: PROFESSIONAL CONDUCT	741 657	2 544 332	4 585 002	5 169 927	12 299 261
PROGRAMME 4: EDUCATION, TRAINING AND DEVELOPMENT	1 230 610	2 680 296	6 555 192	6 656 225	15 891 714
PAYMENT OF CAPITAL EXPENDITURE	-	4 880 000	3 580 000	2 410 000	10 870 000
TOTAL PLANNED EXPENDITURE	13 646 677	26 842 377	41 005 126	44 922 598	112 770 102
SURPLUS / (DEFICIT)	2 076 823	- 6 843 201	- 18 765 480	- 20 141 418	- 45 750 098

Figure 4-10: SACSSP budget 2018 – 2021

Budget allocations for the digitisation project were approved after the presentation of a business plan that included projects in Table 4.7. Further allocations were made to cover the anticipated shortfall.

While the SACSSP is supposed to receive budget allocations, this did not happen between 2013 and 2018 when the organisation’s board and management presented the Portfolio Committee on Social Development (D13, D28). Staffing costs as indicated in Figure 4-11, were as a result of organisational affordability in the medium-term expenditure framework. (D11)

South African Council for Social Service Professions (SACSSP)



COMPENSATION OF EMPLOYEES	2018/19 Budget (R)	2019/20 Budget (R)	2020/21 Budget (R)	MTEF
PROGRAMME 1: ADMINISTRATION	6 005 927	11 547 336	12 344 278	29 897 541
- SUB-PROGRAMME 1.1 : OFFICE OF THE REGISTRAR	2 323 083	4 150 672	4 441 219	10 914 974
- SUB-PROGRAMME 1.2 : FINANCE & ADMINISTRATION	1 957 427	3 169 726	3 395 450	8 522 603
- SUB-PROGRAMME 1.3 : HUMAN RESOURCES	1 380 056	2 550 447	2 713 763	6 644 266
- SUB-PROGRAMME 1.4 : INFO, COMMS AND TECHNOLOGY	-	1 040 346	1 113 170	2 153 516
- SUB-PROGRAMME 1.5 : PUBLIC RELATIONS AND COMMS	345 361	636 146	680 676	1 662 182
PROGRAMME 2: REGISTRATION	3 809 201	4 662 244	7 499 281	15 970 725
PROGRAMME 3: PROFESSIONAL CONDUCT	1 507 832	2 304 102	2 660 937	6 472 871
PROGRAMME 4: EDUCATION, TRAINING AND DEVELOPMENT	1 977 317	4 236 917	4 106 123	10 320 358
TOTAL COMPENSATION OF EMPLOYEES	13 300 277	22 750 599	26 610 619	62 661 494

Figure 4-11: Employee compensation

The following two questions were asked to clarify the organisational budget and costing: “How do you control the cost of IT?”, “What has been an overrun of the IT operational budgets?” and “How often and how much do IT projects go over budget?” The main emphasis was that the organisation prepares a budget and monitors the spending and the reduction of costs, where possible. Below are some of the responses received:

“Budget aligned to APP. Budget ensures that whatever is spent on, is according to the plan.” (P1)

“IT is a very dynamic environment, difficult to control.” (P2)

“Budget prioritise most important needs and address the immediate needs and looking at long term and align IT procurement with long-term needs. (P3)

“We haven’t been fortunate to have large funding to overhaul our IT system. There was not even adequate budget set aside for IT.” (P4)

“IT overspends. Reason being that we end filling more posts, and more laptops are needed for planned and unplanned posts. It happens towards the end of the year. I am not sure of the over budget amount.” (P5)

“You cannot control costs because even if you need something. We have overrun our budget twice, hardware refresh and system development. The only time we are on budget was when we were connecting the two buildings.” (P6)

“They have planning and anything they buy must be according to plan. Other than if what they want to buy is urgent or out of their control.”

“We have overrun in the financial year 2020/21 because we had to buy servers and computers. Around 30% over budget.” (P7)

“Is not with all projects we overrun the budget, though we have to cover accumulating cost, as projects were active, as with the current project too, we still cover accumulating costs, which are not part of the budget. We scarcely overrun budget on operations, as we always have to cater for new employees with proper environment for duty.” (P8)

What was clearly stated by the participants was that IT costs were unpredictable. This is the case because all computing equipment is imported and currency fluctuation places a deciding factor on budget overruns.

4.6.7 Human resources management

Data for this sub-theme were collected using documents and interviews. The implementation of the approved organisational structure was on hold due to budgetary constraints. The organisation was wholly dependent on external service providers for all the IT requirements. There were positions that would be affected by the ongoing automation indicated in Table 4-4. It was found that the most affected department had ten vacant positions for the position of registration clerk. (D11)

Table 4-4: Positions affected by digital disruption

Position	Quantity	Role filled
Registration clerk	12	2
Secretary for boards	2	2
Archive clerk	2	1
Mailroom clerk	1	1
Data capturer	3	1
Call centre agent	3	2

Since the need was identified by the organisation and presented at the initial meeting, a job description was drafted and presented to the HR Committee for approval. Approval was granted by the HR Committee and the advertisement was posted to identify a suitable candidate. The researcher was part of the interview panel and assisted in drafting questions and submitting them for consideration. The implementation of an integrated online IT system would include a 24-month service level support contract (D12). Another mitigating plan was for the organisation to employ an IT intern who has a university qualification who would want to obtain workplace experience for the period of 24 months. Participants were asked the following question: “Do you have enough people for IT?”

“We do not have enough people. Division is still new – IT officer supported by intern. There is a relationship of mentor-mentee. Difficult because if the officer leaves, they leave with their own skill and won’t have anyone to take over.” (P1)

“Resource constraints, cannot have efficient operation.” (P2)

“Real empathy to the person who started last year. Intern is assisting.” (P3)

“It is a work in progress. Currently, there are two staff members – one full time and one intern.” (P4)

“We do not have enough people for IT. There is one person. The intern will leave at the end of the contract.” (P5)

The responses from participants were further validated by the audit report, which highlighted that critical positions remained vacant for extended periods of time, resulting in employees being overworked and an inability by council staff to execute all mandates. The IT division has one permanent employee, and a temporary solution was to employ interns to ensure that services are provided for a period of two years.

4.6.8 Relationships management

This sub-theme presented relations between different stakeholders. Due to the size of the organisation, all managers were involved in IT decisions. This was demonstrated as follows:

- When interviews were conducted for the IT officer, by forming part of the panel.
- Inputs were sought during the requirements of the proposed system.
- Receiving invites to quarterly board meetings.

The meeting was meant for discussion of networking, data integration and AS-IS architecture documents (D9) as per the notes in Figure 4-12. The meeting dealt with data verification of the SSPs (D20) and hardware proposed (D15).

SACSSP meeting // 09 October 2019

Evaluation

- Bill of material ✓
 - Pricing ✓
 - Capacity ✓
 - Work profile (Company)
 - BEE Scorecard
- Project manager

- Hardware setup (SACSSP) (Thondi)
- Environment setup
- AS-IS
- Home Affairs verification

Figure 4-12: Bid evaluation – networking

At the meeting, a discussion was held with potential service providers. One such meeting is highlighted in Figure 4-13. The meeting was based on assessment of a telephonic and data services and related costs. The costs included porting of telephone numbers for the new service. The deliberation indicated the features such as having an ability to access a portal to check usage statistic of data and telephones.

SADV fiber, meeting // 24 April 2019

- Number porting of Telkom numbers
- R100 per number
- 50 Mb line
- Lungi to give out numbers.
- Billing portal & services
- Checking of statistics and measuring usage.

Figure 4-13: Fiber requirements meeting

The organisation size dictates management's involvement in decision-making. It was important that the SACSSP should have relations with organisations of similar size or industry and service providers. This process ensured that the SACSSP found the information needed to build a bill of material (BOM) for an integrated online system and supporting infrastructure.

4.6.9 Service level agreements

Thematic representation of the SLA indicated the following responses from participants, and documents illustrated the challenges encountered. In the interviews conducted, the participants were asked "How well are outsourcing agreements being managed?" The responses are noted below:

"Normal day-to-day work. Management of email, functional queries; there is someone who does the work. SLA is monitored and the service we request is within the agreement. SLA managed on a tight project plan and ensure alignment with costs." (P1)

"Do have SLAs with all the external provides. Penalty on non-compliance." (P2)

"Not well manage (outsourcing agreements)." (P3)

"It was difficult to get full access and ownership of products developed and sometimes the organisation was held ransom." (P4)

"Service providers sign contracts and perform according to work at hand." (P6)

"Based on the agreements signed, we are able to pay external providers. They comply with the service levels." (P7)

Most of the participants highlighted that there had been SLAs with external service providers in place and they were paid according to services rendered. One participant indicated that those SLAs were not managed properly. It can be concluded that SLAs must be clear and understood by all stakeholders.

4.6.10 Vendors management

The results that thematically made up vendor management are highlighted in this section. It was found that no diverse I&T vendors were registered with the organisation. The organisation did not have access to the CSD that lists all vendors that are certified to do business with government entities. The vendors that were contracted on a time and material basis were dictating and making proposals to the organisation.

Figures 4-14 and 4-15 illustrate the bidding of IT-related services and hardware and system development advertisements of tenders on the SACSSP's website.

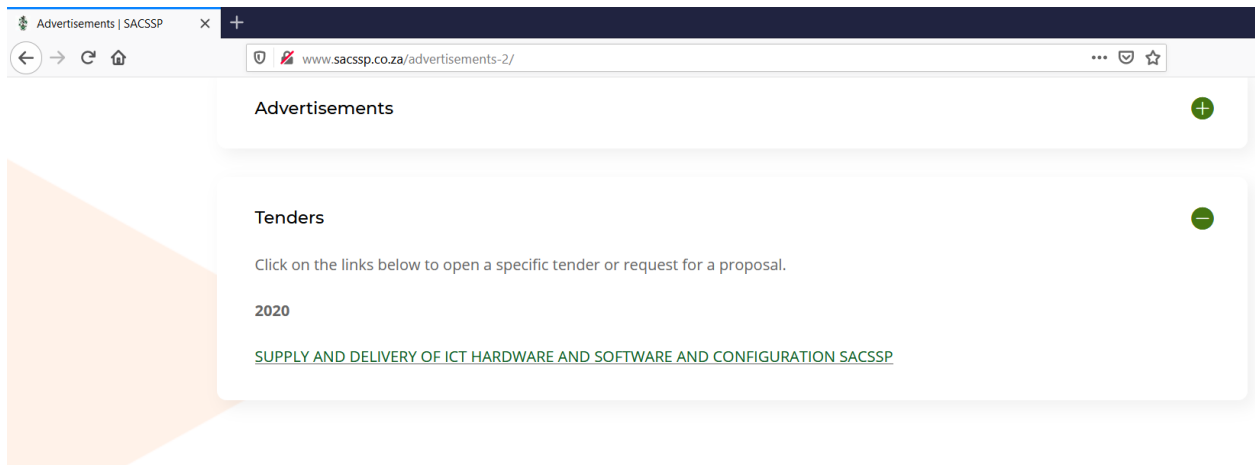


Figure 4-14: Hardware and software tender advertisement

The system development tender was advertised on the organisation's website, as depicted in Figure 4-15.

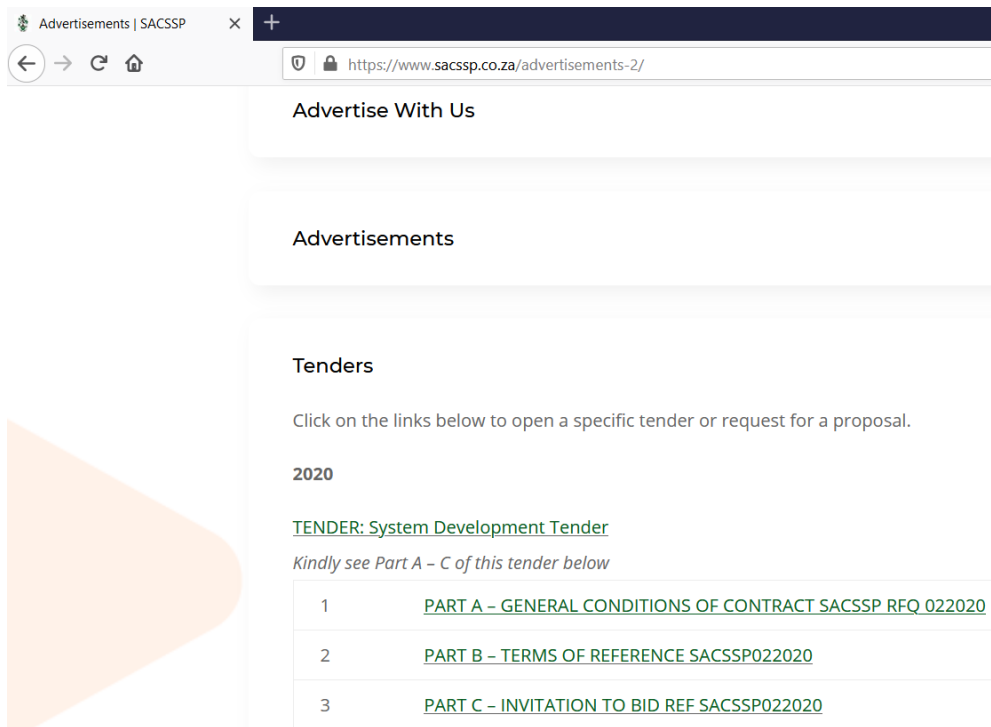


Figure 4-15: System development tender

The question to which the participants responded was “How dependent are you on external providers?” It was found that the organisation was mostly dependent on external vendors. Their responses were as follows:

“It is depended on what you are procuring. Sourcing of three quotations in order to get the value of money. Reliability of service providers.” (P1)

“Ever since I took over. Not much, it dependents. Insourced work done from four companies. Thing that can be done internally, they are done. Database is currently hosted outside.” (P2)

“To date, we are too dependent.” (P3)

“There has been an overreliance in the past, but we gradually improved weaning off.” (P4)

“Our IT go through the process of sourcing best IT providers.” (P5)

“Very important and needed. We make sure they do their job on time when rendering services and that service is good and complaints after they have left.” (P6)

“I think it is that much dependent.” (P7)

“We always looking ways for simplicity and stability of the environment, we make regular calls to SPs for quotes of any new developments on computing applications and IT Business Solutions.” (P8)

An organisational sourcing strategy needs to be formulated and agreed upon. It must have enforceable SLAs in order to mitigate challenges that might arise during the execution of a contract with service providers.

4.6.11 Quality management

The return of mail has been a concern for the organisation. In other instances, it was noted that social service professionals incurred costs when travelling to the SACSSP offices to physically collect the returned certificates (D8, D13). Figure 4-16 depicts files and cabinets with returned certificates that South African Post Office (SAPO) found to be undeliverable.



Figure 4-16: Files, cabinets with returned certificates
Photographer: Researcher (2021)

The statements below indicate the frustration experienced by participants and auditors (D25) (SACSSP 2016a: 14):

“Inadequate internal control processes in place to maintain adequate supporting information and records by the council.”

“The hardcopy files were obtained for testing but without the receipt slips for the correct period.”

When renovations were planned for a new project, it was found that the data centre plan was not updated with previous additions (D17). Furthermore, the qualification authority rejected records submitted for verification. The biggest issues found were the inconsistency of data that were rejected by SAQA due to following factors (D20):

- No identity or passport number were found on some records
- Incorrect identity values did not follow the numbering convention
- Date of birth not matching with identity number
- Garbage values rejected – records that would be rejected by SAQA
- Duplicate identity numbers
- Invalid email addresses – submitted e-mail address validation checks failed, records submitted with blank e-mails but need to be fixed on register for communications aspects, etc.
- Physical address fields left blank with the input field defined as not compulsory

Decisions were made with the available quality information. Integration with other government agencies such as the Department of Home Affairs can mitigate some of the data quality challenges already experienced.

4.6.12 Risk management

There were risks that were identified from analysed documents, interviews, meetings held and system analysis. The validity of the current database of the SACSSP has been questioned for the past number of years in terms of numbers and content (D20). The risks to the organisation were classified and mitigated. Risk management is a standing item on the agenda of management meetings and Business Re-engineering

Committee meetings (D18, D19). Management has the responsibility to action the seven stated risks and, on a quarterly basis, report to the IT and Business Re-engineering Committee for progress (D16). Data were not properly managed due to the fact that there were pockets of data on people's computers and hard copies in archives rooms (D20). Some of the identified risks are stated below (D21):

- "Management action plan to mitigate the risk of non-filing in archives room that were identified.
- Non-compliance with section 13 of the SACSSP act and Section 40 of the PFMA.
- Lack of audit trail due to lack of adequate filing records
- Enhanced risk for fraud or errors.
- Inability by the Council to support financial transactions reported on its annual financial statements."

The question, "Did you address all IT-related risk?" was asked to participants and some of these responses are given below:

"Risk register that addresses all IT risks are minimised, especially Finance and Registration and all risk. Review risks as they happen. Ensure that what IT needs to address the risks is catered for." (P1)

"High, medium risks we address. If an application can run in the cloud, risk transferred to Microsoft O365 platform." (P2)

"We were not made aware of risks. Working from the previous risks. Timeously inform councils of risks so that council can proactively mitigate them. Interface is critical for mitigate the state risks." (P3)

"Yes, we are monitoring emerging risks daily." (P4)

The risk register was created to track and mitigate identified risks. The risks were classified as strategic and operational to be actioned by the council and management.

Some of IT risks were mitigated through the use of cloud through the use of Microsoft Office 365.

4.6.13 Security management

The organisation was attacked by an Ink-Horse-Deal ransomware and all the information on the file server was encrypted (D21). The original message for the ransom that was sent and the request is as per Figure 4-17. The researcher advised that no contact or ransom should be made with the offending party. New server images were built and the organisation considered the loss of information (D23). A SLA with a cloud service provider should be considered in future.

All your files have been ENCRYPTED!!!
Write to our ICQ <https://icq.im/bigbosshorse>
Or contact us via jabber - bigbosshorse@xmpp.jp
Jabber client installation instructions:
Download the jabber (Pidgin) client from <https://pidgin.im/download/windows/>

After installation, the Pidgin client will prompt you to create a new account.
Click - Add
In the -Protocol field, select XMPP
In -Username - come up with any name
In the field -domain - enter any jabber-server, there are a lot of them, for example - exploit.im
Create a password
At the bottom, put a tick -Create account
Click add
If you selected -domain - exploit.im, then a new window should appear in which you will need to re-enter your data:
User
password
You will need to follow the link to the captcha (there you will see the characters that you need to enter in the field below)
If you don't understand our Pidgin client installation instructions, you can find many installation tutorials on youtube - https://www.youtube.com/results?search_query=pidgin+jabber+install
If you have not received a response from us then we may have technical problems and please write to us using Jaber here bigbosshorse@xmpp.jp or on icq
Attention!
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.
tell your unique ID
1D2FBUjedLMjS9kji1KwBfIK/Sbkt3v6VPWQomXmY8q5aIOZd/BILmgDRM6SXyL4cra/mXHCoa3T3j/cu
nH36d+vcaLkYndEszEg1+zWfZxAAsp2uTW4EXUhA7LrVKdRhXgV3fgPoSr44ZxBYORgalJ

Figure 4-17: Ransom malware message sent
Photographer: Researcher (2020)

However, the source of the ransomware attack could not be ascertained. The ICT policy provided assurance that access to the organisation's ICT system would be determined by the particular work requirements of staff members, with the understanding that all staff members will have access to their own allocated personal folders to archive the work information.

This question was asked "Is the information that you are processing well secured?"

"Ransom malware. You can never be ready for these attacks. Reactive and now tighten the firewall for those risks not take place. Review on quarterly basis. Issue of malware comes to picture. Other information (physical files) not secured." (P1)

"For soft copies, access level authentication to certain individuals." (P2)

"Safety and protection of information, firewall and software, procurement, threats (hacking), security of data. Concentrate on bigger threats. We thought so, until last time we thought we are. Detail is can't tell. We found out it is not as secure and safe as we thought." (P3)

"Yes, securing data is our first priority because we handle people's personal information." (P4)

"When we hired IT person, we were hit by a virus. It is well secured. IT has installed a firewall do that we do not get compromised." (P5)

"Desktops are locked with passwords. Yes, we have firewall and anti-virus updated." (P6)

“Have not lost emails. I think it is secured. They do awareness and install anti-virus software on our machines. There is a firewall that protects servers.” (P7)

“The systems are activated to receive daily updates, compatible to the domain controller and all security applications. Firewall in place for cyber-attack and antivirus installed in all resources. As previously mentioned, the current environment is secure. Laptops and desktops are antivirus secure.” (P8)

A wide range of security measures was employed: password, anti-virus, software patch management and firewall to secure IT-related assets. One participant stated that the physical files were not that secured. Enforcement of ICT policy is key to prevent future ransomware attacks.

4.6.14 Managed data

The data management sub-theme’s results illustrated that there were inadequate internal control processes in place to maintain adequate supporting information and records by the council. Furthermore, data that were considered unclear by the qualifications authority were rejected. It took longer to clean the submissions file. There has been a delay in data validation of data that could not be auto-cleaned and the updating of the database. Furthermore, it required additional effort by the SACSSP team to have the master data corrected while waiting for their database to be verified with the South African population register (D20).

The following responses were given to interview question “Is the information that you are processing well secured?”

“Normally, information is kept onsite in the form of physical files for members in archiving room. Currently, the database rendering the system inefficient.” (P1)

“Database – frustration is access to data and develop our own reports. Users can input data themselves and staff can validate, verify and approve application. Our database is hosted in the cloud and seems as if they own our data. If additional reports are needed, you cannot create your own reports.” (P3)

“Furthermore, we can improve access by bridging the gap in information dissemination. Securing data is our first priority because we handle people's personal information.” (P4)

Data management challenges were evident due to the high number of postal returns from posted letters. The primary challenge encountered was SSPs not updating records when changing addresses or employment. The following participant outlines that:

“To mitigate the challenge of post office, wrong addresses, missing certificates and returned mail, the application form must be accompanied by all required documents that must be captured on the database so that client can be issued with a certificate and practice card.” (P5)

Organisational data were not integrated and were inefficient, and delays were experienced in decision-making. A lack of access to data and reports was frustrating for the staff concerned. The high return rate of posted items was costly due to incorrect data, such as practitioners' personal details and addresses.

4.7 THEME THREE: BUILD, ACQUIRE AND IMPLEMENT

The theme, build, acquire and implement is about understanding some of the proposed solutions to support information governance that can ensure corporate

governance. Eleven sub-themes were generated from the collected data as highlighted:

Programme management; Requirements definition; Solutions identification and build; Availability and capacity management; Organisational change management; IT changes management; IT change acceptance and transitioning; Knowledge management; Assets management; Configuration management; and Projects management.

4.7.1 Programme management

This sub-theme displayed the realisation of desired business value and reduction of the risk of unexpected delays, costs and value erosion as important aspects. It further advised that improvement in communications to and involvement of business and end users would ensure the value and quality of programme deliverables and follow-up of projects within the programmes. It would also maximise programme contribution to the investment portfolio. The following were respondents' responses to the question: "How do you best build and structure IT department?"

"Have put a budget aside and come with system with new functionalities come with online applications and integrated with financial application. System responsive to the market to serve." (P1)

"Hoping to move faster where we can implement the business strategy." (P3)

"Align programmes and communication to reach wider stakeholders who are technologically savvy (youth stakeholders). Proper planning and introducing an integrated system linked to all strategic units." (P4)

"Most of projects are in progress and others to be finalised..." (P5)

“We have had projects taking place for upgrade and improvising on IT. The current projects taking place range from network rewiring, VOIP, System Development, etc. Projects like digital back scanning, digital certificate and PayPal have been paused due to budgets with no assurance of commencing date. It is not with all projects that we overrun the budget, though we have to cover accumulating cost, as projects were active, as with the current project too, we still cover accumulating costs, which are not part of the budget. We scarcely overrun budget on operations, as we always have to cater for new employees with proper environment for duty.” (P8)

Development of the integrated online system required a portfolio of service requirements. The requirements as mentioned by participant 8: network rewiring; system development, digital certificate and back scanning of documents were some of the projects that were components that required a budget that was reprioritised to support the strategic goal.

4.7.2 Requirements definition

The system requirements were drafted and solutions proposed to be used to meet the needs of an enterprise based on process documentation. It was found that the registrations division does not have full access to the database in use and the service provider does not allow organisational staff full navigation on all fields on the database. These needs were a summary of what transpired in a focus group meeting with SACSSP managers and were agreed upon to be included in the proposed system as indicated in the briefing notes in Figure 4-18. (D27). The business processes meeting was held at SACSSP offices on 13 June 2018 at 09 am.

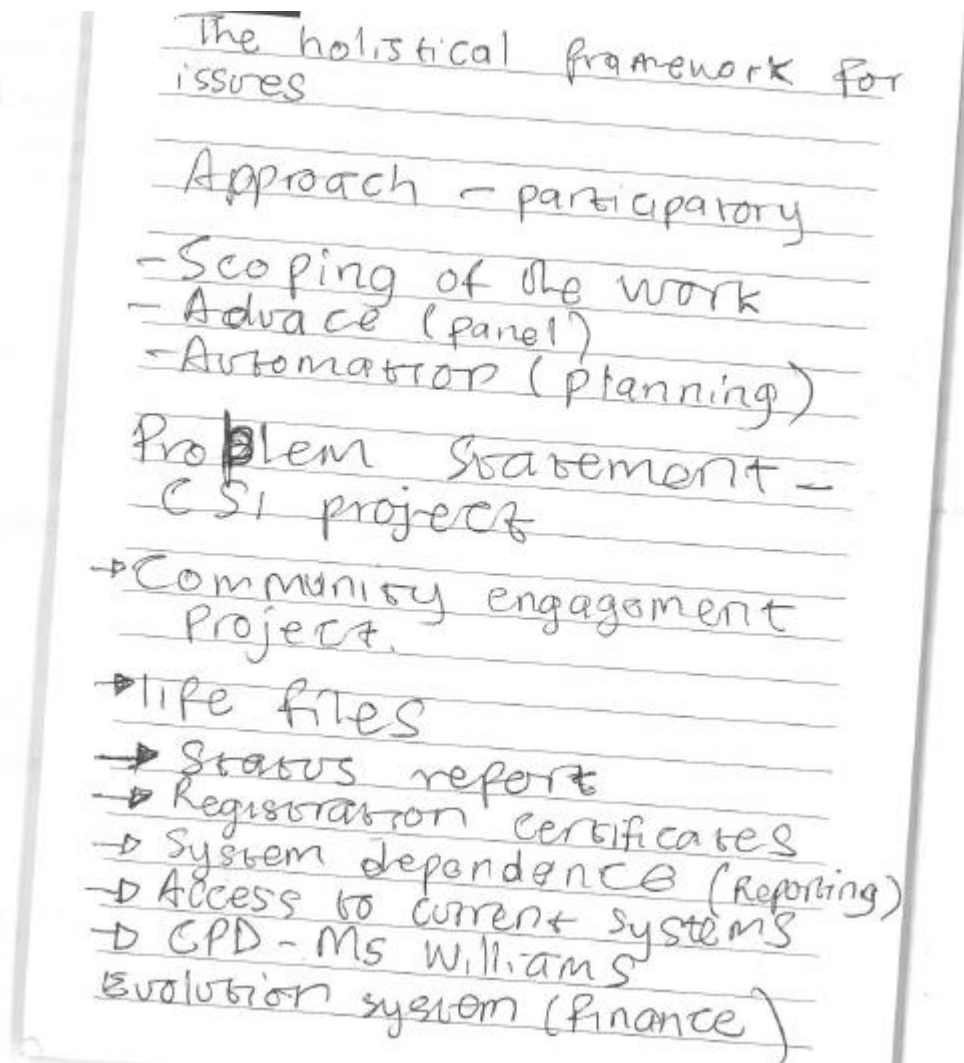


Figure 4-18: Initial briefing notes

Figure 4-19 depicts an extract of agreed scoping work that was required based on the exploratory meeting deliberations on 21 May 2018. (D9, D14)

- Scoping of the work required: To be
- a) Assessment of the 'As Is' and the 'Should be' status quo of Council's IT systems and future needs
 - b) Determining a scope for work for suitable system design. (migration)
 - c) Recommendations on the phased out model of intervention

Figure 4-19: Scoping requirements

Furthermore, a benchmarking exercise as evident in Figure 4-20, was done at an organisation of a similar size to identify server room requirements. It was found that the organisation had enough funding and received support from the board and

management to meet the minimum data centre standards. The site visit and meeting were held on 31 January 2019.



Figure 4-20: Benchmarking exercise - Similar sized organisation
Source: Researcher (2019)

The discussions indicated that the benchmarked organisation one had all their processes already online. All IT services are fully outsourced to external service providers and hosted at a Midrand, Gauteng hosting environment; There were different data integration points with the internal system; Their systems were hosted in the cloud. Field notes captured on similar sized organisation one benchmarking are stated in Figure 4-21.

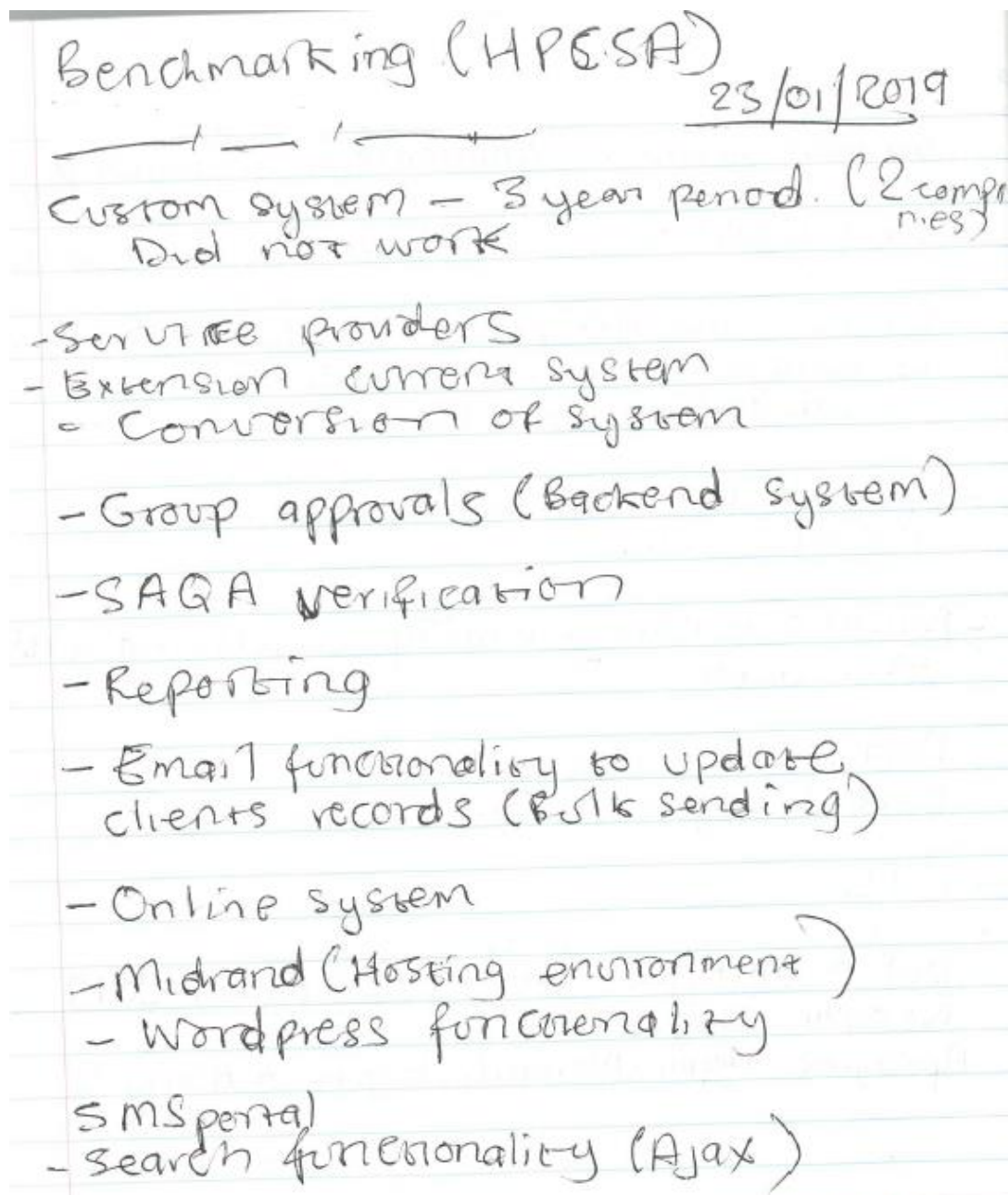


Figure 4-21: Benchmarking notes (similar sized council one)

Benchmarking done at a similar sized council in Figure 4-22. The discussion was to get better clarity on their processes in order to inform new processes, terms of reference for system development and hardware refresh (D8, D12, D15). The discussions indicated that the benchmarked organisation had 90% of their processes already online. They had online marking system; there was systems integration challenges. Over reliance to external service providers; data importation challenges; Their systems were hosted internally and fibre installation was supporting daily transactions.

Benchmarking (Pharmacy Council)

31/01/2019

Financial Applications (change control)

CPD - Online exam (System marking
(Competency standards))

- Internal IT (5 resources)
- Auditing finding (reliance of IT Service Providers)
- Registration form when approved by University (website) →
- CASE Mngmnt System →
- P-number (Registration)
- SMS notification (to log-in)
- Yearly application
- Student (Tutor - student) - Practice.
If select credit card option. If EFT
- Enforcement of online registration.
- Progress reports are online (tutor)
- SQL based
- App for inspection
- Online complaint (choose to be anonymous)
- Import challenges with finance
- Query Management tool (Accepac System)
- Custom-made system
- Reports (Standard report) custom reports for Business Units.
- Hosted at main office (possible move to cloud)

Figure 4-22: Benchmarking – similar sized council two

The evaluation meeting discussed the networking, hardware solutions proposed, as-is architecture document and database verification of SSPs personal details (D9, D14, D15, D20). Figure 4-23 depicts the notes that were captured by the researcher.

SACSSP meeting // 09 October 2019

Evaluation

- Bill of material ✓
 - Pricing ✓
 - Capacity ✓
 - ~~Work profile~~ (Company)
 - BEE Scorecard
- Project manager

- Hardware setup (SACSSP) (Thandi)
- Environment setup
- AS-IS
- Home Affairs verification

Figure 4-23: Solutions evaluation

Field notes of the digital certificates' fact-finding meeting. The attendees discussed the security concerns of digital certificates; the features and accessibility for certificate's verification; and costing model amongst the other matters. After the meeting as depicted in Figure 4-24, it was decided that further investigations to be conducted to ensure that a better solution can be sought to get a system that can be hosted internally instead of exposing SSPs data to external parties.

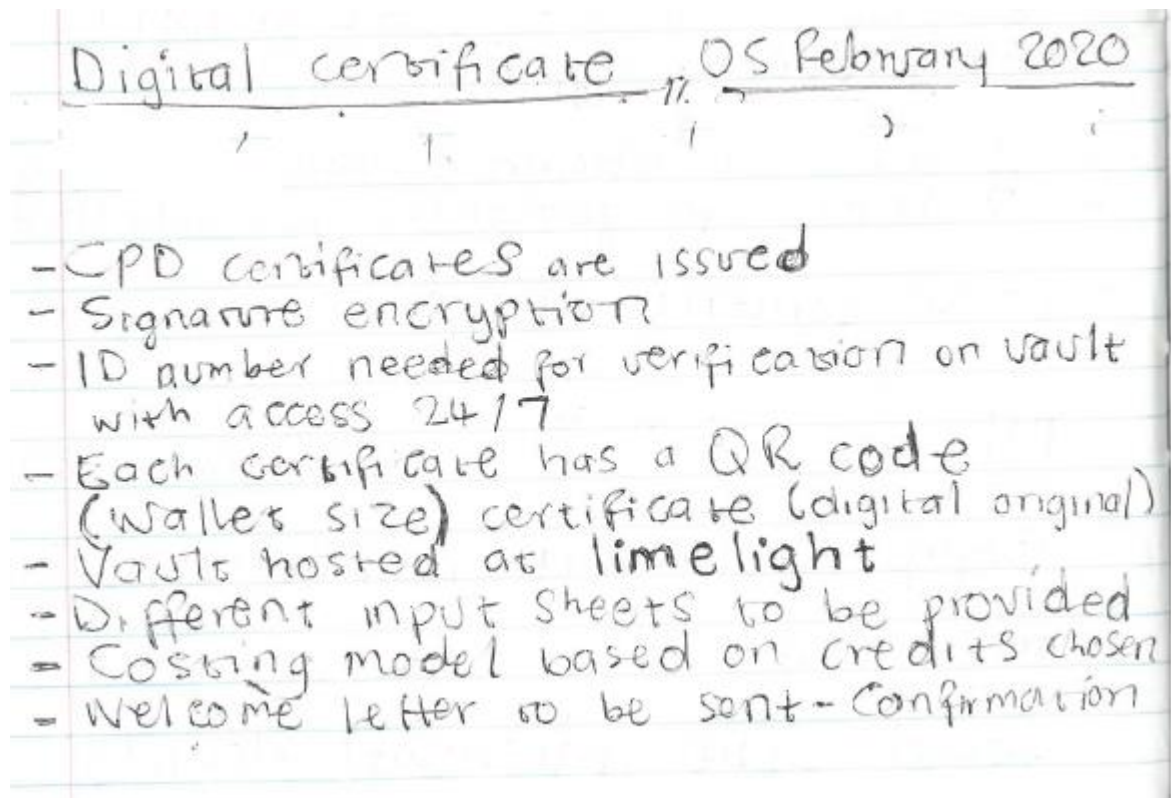


Figure 4-24: Digital certificate meeting

The organisation's strategy was to innovate the telephony to VOIP system (D22). The meeting held discussed and presented a switching network upgrade to accommodate the proposed changes. The discussion in Figure 4-25 made decisions on networking requirements (D13, D15).

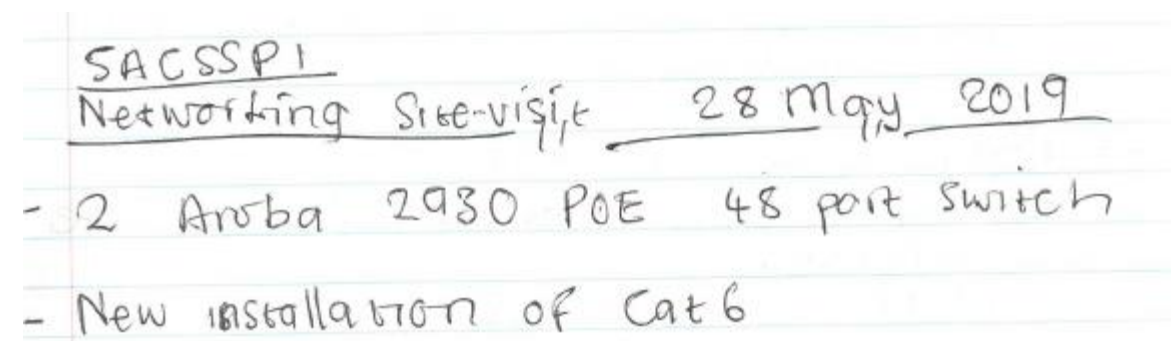


Figure 4-25: Networking requirements meeting

The data loss risk that was identified at exploratory meeting (D21). A backup solution was proposed for the organisation as shown in Figure 4-26 (D15). The scoping of a solution covered the current installation and future installations that were being discussed as per the organisational strategy (D4, D22, D27)

Vendor	Quantity
Veeam Availability Suite Standard – 5Yr Production Support	4
Veeam Availability Suite Instances – 5Yr Production Support	1

Figure 4-26: Backup requirement

A question to support the requirements sought was “How much of the IT effort goes to fighting fires rather than to enabling business improvements?” The responses outlined the following:

“Have put a budget aside and come with system with new functionalities come with online applications and integrated with financial application. System responsive to the market to serve. Current processes are slow and will ensure better to serve the market (stakeholders). Issue of communication network (installation of fibre) for better bandwidth and throughput. Introduction of Voice over Internet Protocol to reduce the costs of communication and exploited the use of technology. The current system is obsolete. I cannot respond better with the obsolete Silverlight application. Procuring server with enough space and restructure and move away from saving on external hard drives. Have an opportunity to evaluate the entire the system. Servicing 89,000 people and want efficient system and responsive market.” (P1)

We need to choose new tech to align to what we want to achieve – costing and output. Is it aligned? Correlate with the strategic opportunities. We need to keep us with latest technology. We have sent them to research if we implement new technology. Benchmarking monthly with other councils. Dynamic to change to suit the business requirement. Tailormade to a specific problem. Issue of benchmarking requires an IT department to go to other organisations

to fill the gaps quicker and respond more into our needs. Physical files back-scanning will have to be catered.” (P2)

“There is a lack of system’s integration, as well as doing work manually. There is manual registration. It is not efficient and it is time consuming. The requirement is a fully online integrated system of operational functions of the council. We need to move away from paper-based operations. The terms of reference were approved and finalised the appointment of development of provider in March 2021. If we get what we wanted as per TOR, then can really change how the council change to operate.” (P3)

“It is easier to start from scratch than try to adjust an existing system which might not be compatible.” (P4)

“We have IT budget. IT assesses the needs of staff. Needs analysis of laptop printer and routers.” (P5)

“We can have VPN to help us to work from home. The improvement can happen that can happen is the capability to work from home. Everything they need, they must comply.” (P7)

“We always looking ways for simplicity and stability of the environment, we make regular calls to service providers for quotes of any new developments on computing applications and IT business solutions. We make necessary researches before implementation, and always look for third party advice from experts. Local build and designed business model systems (servers, laptops and computers and cloud services, with Agile development). We run feasibility, quality check and results.” (P8)

The organisational staff had already identified their requirements and the involvement of the researcher brought focus to processes and assisted with the identification of

other requirements that made their needs a reality. The process required board and management commitment through financial support and buy-in. The governance structures supported benchmarking processes undertaken and consistent feedback was provided.

4.7.3 Solutions identification and build

The solutions identification sub-theme presented the hardware solution as proposed in Figure 4-27 as the solution suggested to the SACSSP by the researcher, which would include two physical servers hosting virtualised servers, one backup server, one storage server for scanned physical documents, and fibre channel switches for communication between the computing infrastructure in support of radical innovations and current business needs, as highlighted (D4, D9, D13, D14, D15). This was proposed to the IT Business Re-engineering Committee and the board after consultations with IT and management (D18, D19, D22).

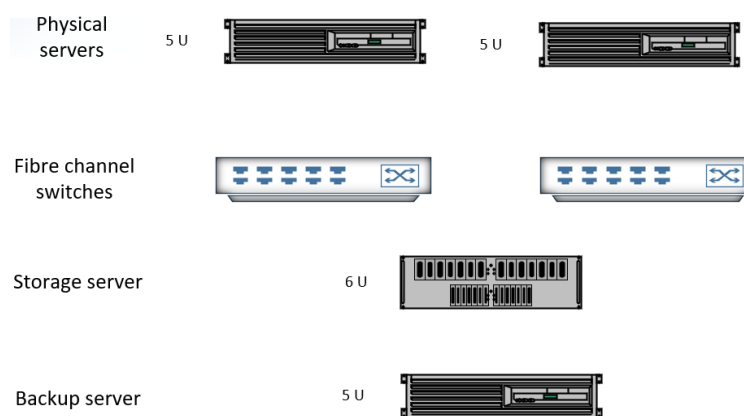


Figure 4-27: Proposed server hardware solution

This included the digital certificates implementation workshop held to identify the requirements needed for the system integration. The next phase involved the drawing of the individual divisions' processes using Microsoft Visio® software. Workshops were conducted with individual teams to obtain inputs. All the adopted solutions were identified after an exhaustive process with the participants.

The interview question “How do you best build and structure IT department?” was used to ensure that relevant solutions are identified and adopted:

“Procuring server with enough space and restructure and move away from saving on external hard drives.” (P1)

“What is outstanding is the system that needs to be developed.” (P7)

“We have installed latest big servers to run high-end applications. We are busy with integrated system development. For example, we took away the old telephone system to go with cost-effective VOIP solution, from monthly rentals of up to R20 000 to as little as R6 000 of combined rental and usage. We are in process to digitalise certification, and avoid onsite certificate and receipt collection.” (P8)

Two participants mentioned servers that were procured for the organisation to improve its daily operations. The identified system was delayed due to further requirements that were needed after consultation with the stakeholders.

4.7.4 Availability and capacity management

It was found that the sub-theme availability and capacity management’s (ACM) assessment of the current computing hardware and software did not meet future needs for the availability, performance and capacity of the service provided, which includes forecasting of the future SACSSP requirements. Figure 4-31, on page 167, shows the results of the hardware analysis that confirms that the server environment did not meet the organisational needs and hosting of the proposed system. This led to available storage not being able to archive daily backups, which was a challenge.

Figure 4-28 depicts the two backup storage mediums that were in use. The organisation used hybrid storage systems, namely cloud-based storage for systems hosted in the cloud and local systems that used an external hard drive. The AS-IS document that included backup and replication solution was presented at the 12th IT

Business engineering committee meeting that was virtually held on 29 April 2020.

(D9)

Backup and replication systems		
Hostname	Location	Store Capacity
External USB	Local	1 TB
Redstore Backup	Cloud based	20 GB

Figure 4-28: Backup and replication systems

This question was asked to address the availability and capacity management: “What do you do if IT is not available?” The participants responded as follows:

“Financial information – backup system that stored on cloud. Cost of IT – lost service provision. Malware attack of losing your information, reputational damages. Only finance information is not put on cloud. Reliance on the servers. No backup. Pay for more if moving on the cloud.” (P1)

“We back up; business continuity after impact. With backup there’s a single point of failure. It depends on the functionality. Microsoft 365 does all the work and setups. If there’s an attack, they will do a backup. System hosted on the cloud. It is a critical aspect / backbone of any organisation. You will not function at all with ICT. There’s no department that will operate as siloes. Database is currently hosted outside.” (P2)

“We can’t survive without IT. It has to be up to date.” (P4)

“Backup on the computer files on the server and cloud. We have an archive and we are in the process of converting them to be saved online. They can assist remotely and assist with your machine at home. IT is important in sustaining the council. We work with the social service sector. We are the only office in the country. Database must be operational and easy to use.” (P5)

“Very important. If there is no IT on site we are going to struggle and not achieve our goals. Not enough. Still short of digitising of document because the storerooms are full and there is no longer space to store more.” (P6)

“I can’t work from home because we do not have VPN. We prefer that they put their information on cloud. If anything happens, we have back up and we looking to have a DR for security and outsource such systems as cloud computing and disaster recovery. Cloud computing and back-up services.” (P7)

Financial information was considered important and loss of data would cause reputational damage. The systems were backed up and Microsoft Office 365 was in use. Staff saw a need for having a hosted database in the cloud. One participant stated unavailability of space for physical files as a challenge that can be sorted out by digitisation.

4.7.5 Organisational change management

The changes the organisation anticipated are given in Table 4-5 and were extracted from diverse organisational documentation. The categories of organisational change addressed were: people; technology; information processing and communication; and competition. It should be noted that in each of the change categories, characteristics of such change was extracted from more than one organisational document.

Table 4-5: Organisational change management

Doc #	Change category	Type of change
D18 D19	People	The development and provision of training materials and an orientation on the use of these materials to the relevant staff members.

Doc #	Change category	Type of change
D12 D18 D19	Technology	<p>Initiate and support the implementation of the integrated online system over a period of 24 months.</p> <p>Capacity support and training were requested as part of an integrated IT system development tender:</p> <ul style="list-style-type: none"> • The development and provision of custom technical and user-friendly manuals in relation to the online system. • Training sessions for end-users and staff members on site on the system through multiple sessions not exceeding 80 hours in total.
D4 D8 D9 D14 D15 D18 D19 D20 D21 D22	Information processing and communication	<ul style="list-style-type: none"> • It was stated that the current system does not offer faster reaction times and immediate responses to questions (Engelbrecht 2021: 9). <p>Following a focus group meeting, the following were stated and new system proposals:</p> <ul style="list-style-type: none"> • There was no full access to the organisational database for the divisions to be able to extract specific reports like adoptions, probations, international applicants, etc. • The new system should assist registrations to extract statistics for registered professionals within provincial municipalities (e.g. Gauteng, Soweto, etc.) • The new system should be designed in such a manner that the registrations division can run queries on their own and generate statistical reports about client's statuses: payment, registration, employment. • The new system should be designed in a way that it sends automatic reminders to clients to renew their annual subscriptions. • The new system should be designed in such a manner that certificates, status reports included, can be loaded onto the system and sent automatically once a client is registered and/or paid their annual fee.

Doc #	Change category	Type of change
		<ul style="list-style-type: none"> • The new system should include a new folder where all new applications can be loaded to prevent the database from issuing numbers without checking authenticity of all documents received. • The new system should ensure that a notification is generated automatically. • The database should be integrated (registrations, finance, professional conduct and ETD) to allow better management of clients' information.
D1 D2 D4	Competition	There is no competition since the organisation's existence was promulgated through Social Service Professions Act, No. 110 of 1978. However, the SACSSP has organisations of other professions that are similar in nature that it can benchmark from peers.

Participants were asked about organisational changes for the smooth transition to new ways of working. The question was, "How do you develop and maintain the skills?"

"Whether it is strategic, operational, send everything to them so that they know." (P1)

"If we get what we wanted as per TOR, then can really change how the council change to operate." (P3)

"Fortunately, with the advent of covid-19, the attendance of virtual meetings and quorums has improved. The turnaround time is shorter than when we held face-to-face meetings." (P4)

"He made us aware not to bring external hard drives and not open spam emails." (P5)

Two change categories, namely people and technology, were already implemented due to an IT security breach and covid-19 pandemic. However, the information processing and communication changes were the requirements that were part of the needs of the proposed integrated online system.

4.7.6 IT changes management

IT changes management refers to transition related change management to the IT services being implemented. It was addressed through the development of the terms of reference (ToR) that the organisation drafted for seeking service providers to develop the integrated online system and provide IT capacity support through (D12):

- the development and provision of training materials and an orientation on the use of these materials to the relevant staff members
- training sessions for end-users and staff members on site on the system through multiple sessions.

From the login instructions for council seating as transition it was also evident that changes were implemented during the covid-19 lockdown where invitations to Microsoft (MS) Teams® included a “How to connect to MS Teams” document developed internally to assist internal staff and board members with their functions. Figure 4-29 depicts one of the invites sent (D24).

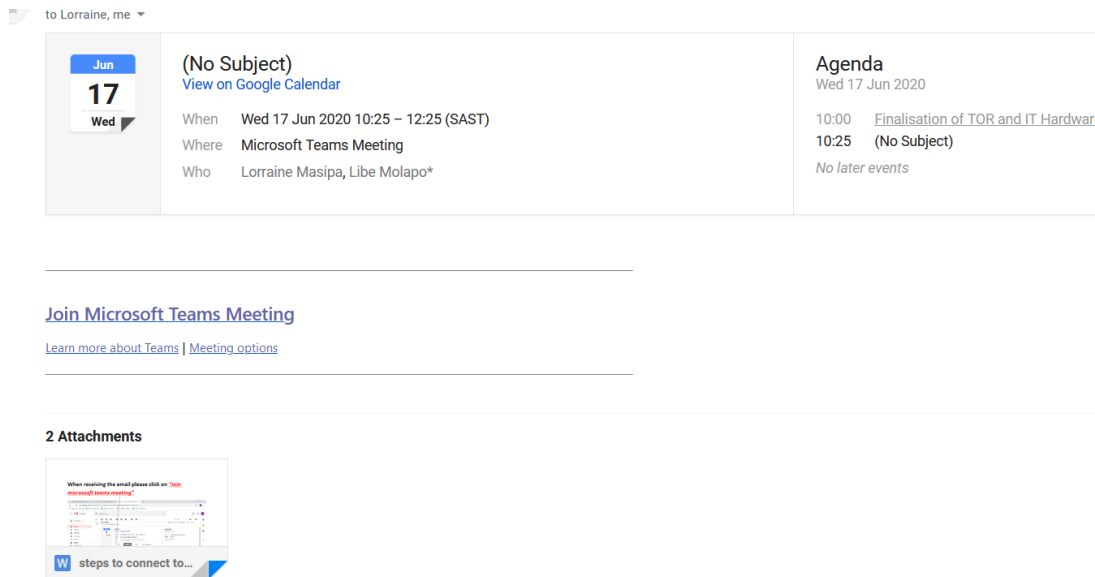


Figure 4-29: How to connect document on MS Teams invite

The implementation of IT changes management led the researcher to include the question “How much of the IT effort goes to fighting fires rather than enabling business improvements?”

“The division is still new and the IT officer supported by an intern. There is a relationship of mentor and mentee. We are slow to improve the system and not responding the quicker way to the market changes.” (P1)

“We are working on capacitating the infrastructure and bringing in house all the data that was stored externally.” (P4)

“They go to training.” (P5)

“We can call using landlines while we are at home for work related issues and we have video conferencing meetings. I have heard that they go to courses. The only thing that I see is skills transfer from companies that installs software in machines.” (P6)

“I don’t recall IT going to training.” (P7)

It became evident that there was some form of skills training in the form of shadowing. Two participants stated contradicting views on going to training. Clear training development programmes should be presented to all staff, so that it does not create confusion.

4.7.7 IT change acceptance and transitioning management

The IT change acceptance and transitioning management processes followed by the organisation are shown in Table 4-6 together with documents utilised. Twelfth deliverables were tabled and highlighted the breakdown of activities, resources required for the successful transition to the system.

Table 4-6: IT change transition activities

Deliverable	Activities to undertake (winning bidder and SACSSP)	Resources required (software / hardware / human) documentation from winning bidder	Doc #
Hosting	List all activities for sustainable hosting <ul style="list-style-type: none"> • Procurement/contract • Licences 	Hardware, software and access to site	D13, D14, D15
Data migration	Data mapping	Database structure	D8, D9, D20
Technical design (URS addendum)	URS analyst and software developer	Process document and workshop attendance	D8, D9
Application Programming Interface (API)	Development of an API	Systems to connect to	D8, D20, D23
Development of registration module	Software development skills	User requirements	D8, D9, D12
Technical staff training	Trainer	Staff to be trained	D11, D13

Deliverable	Activities to undertake (winning bidder and SACSSP)	Resources required (software / hardware / human) documentation from winning bidder	Doc #
Testing	Functional system modules	Testers	D20, D21
User acceptance testing	Provision of testing data	Testing participants	D18, D19
Training	Determine training platforms (virtual or physical training)	Training attendance	D18, D19
Implementation	System backup Daily database functions Daily security functions	Backup solution	D8, D9, D13, D15
Maintenance and support	Technical resource availability	IT staff availability	D12
Change management	Provision of training and resources	Communique	D10

The inputs on the ToR of the proposed system included support for the implementation of the integrated online system over a period of 12 months (D12). It requires highly specialised expertise to develop, run and adjust the system without further outsourcing. The database and different software systems and equipment to be implemented would need staff training in order to have a successful change transition.

4.7.8 Knowledge management

Most of the organisation's explicit knowledge was embedded in documents or repositories and individual computers. Some of the extracts from the documents that were given to the researcher were MS Teams login instruction manual (D24), audit report (D25), ICT policy (D26), draft records management policy (D3), SACSSP Act (D1, D2) and related regulations (D5, D6, D7).

Kindly find council meeting attached.

I have attached a simple step by step guide on how to join the meeting, kindly follow it.

Figure 4-30: Meeting login instruction

The ICT policy explicitly state that “In addition to the requirements of paragraph 5.1.1, the Council ICT official, or in her or his absence, the staff member designated to have sufficient knowledge of ICT standards and requirements, shall review all requests for procurement of ICT equipment and software and make recommendations based on the required standards, compatibility with current systems and this policy.” (D26)

The draft records management policy has not been approved by the council (D3). The SACSSP Act was enacted with the following clauses to address KM initiatives:

Keeping of registers (1) The registrar shall keep separate registers in respect of social workers, student social workers, social auxiliary workers and persons practising other professions in respect of which professional boards have been established registered in terms of this Act and shall, subject to the provisions of this Act, record in the appropriate register the prescribed particulars in the prescribed manner in respect of every such social worker, student social worker, social auxiliary worker and person. (D1, D2)

The SACSSP prescribed how explicit knowledge could be stored. The delay in the approval and use of unapproved policy is not enforceable. The shadowing of permanent employees by interns was a way of acquiring tacit knowledge that is unique to this organisational setting. (D18, D19)

4.7.9 Asset management

The asset management sub-theme presented different asset classes such as hardware analysis, which was performed on the server environment, which revealed that the servers in use were outdated and not able to prepare the integrated online

system and proposed digitisation of all records as stated in Figure 4-31: Assessment and configuration proposal – SACSSP. (D14)

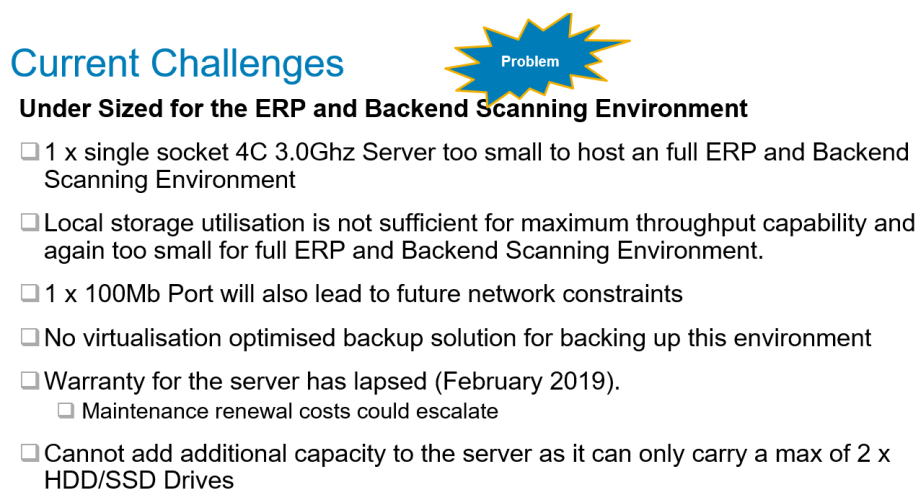


Figure 4-31: Computing hardware analysis results
Source: Hardware analysis (D14, D15)

The organisation indicated the allocation of technology tools (computing equipment, mobile phone and internet router) in order to comply with the ICT policy as per the delegated authority and nature of work. In discussions on hardware, one of the comments related to the topic was replacement of obsolete servers and old laptops that do not meet the current needs. (D26)

4.7.10 Configuration management

No records of warranty were found for the software and hardware assets in use. The configuration management system was not implemented to hold all relevant attributes such as contracts, software licences, suppliers and anything that the organisation deems fit to be stored and maintained in a central location. The researcher could not find any system configurations of the current operational systems (D9, D14). The other challenge discovered was that alterations had been made but the building map did not indicate any. Figure 4-32 shows that a drywall was found while it was thought to be a solid wall. (D17)



Figure 4-32: Dry wall in server room

The plan that was supplied indicated a solid wall that was incorrectly configured (Figure 4-33). (D17)

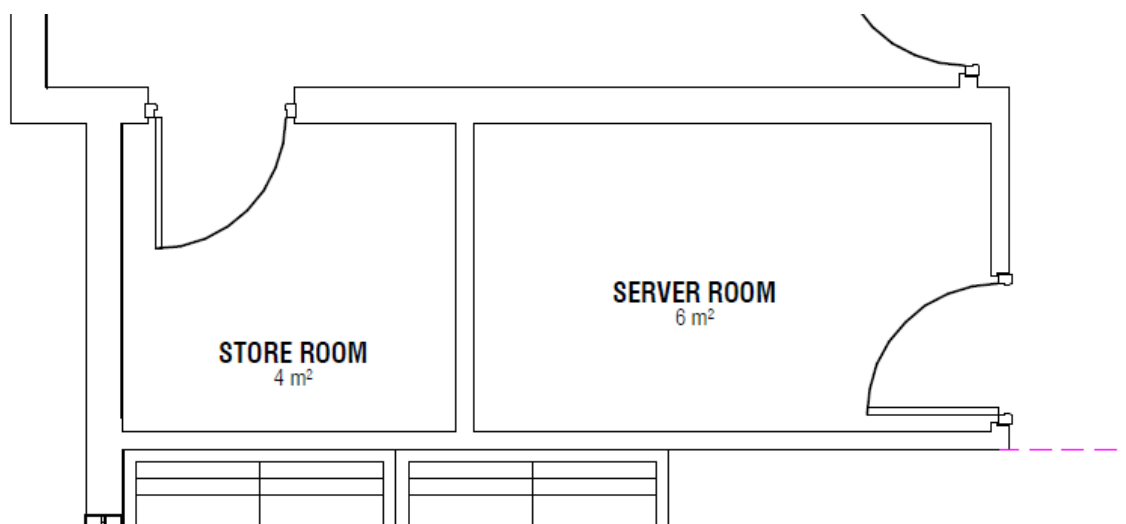


Figure 4-33: Portion of building plan

Based on the challenge, the dry wall, highlighted in Figure 4-33, all the future IT requirements included documentation as part of specifications through the establishing

of SOP. Table 4-7 shows the documents requested per project as part of the specifications issued.

Table 4-7: Configuration documents required

Project type	Document requested
Fibre connectivity from 37 to 33 Annie Botha Avenue	<ul style="list-style-type: none"> • Schematic network layout • Documentation (hard + soft copy)
Appointment of service providers to develop an integrated IT system	18:2 – Documentation on the configuration and deployment of the solution <ul style="list-style-type: none"> • Provision of custom technical and user-friendly manuals in relation to the online system • The development and provision of training materials and an orientation in the use of these materials to the relevant staff members • Source code of the system
Supply and delivery of ICT hardware and software	<ul style="list-style-type: none"> • Licencing portals access with Original Equipment Manufacturers (OEMs) • Hardware warranties • Hardware and software configuration documents

The organisation requires that the following should be submitted to the boards as per the ICT policy:

- Status of all hardware and equipment with recommendations on changes and or upgrades, if required.
- Status of software and programmes used by Council's administration with recommendations on changes and or upgrades, if required.

It should be noted that the SOP for the board of the SACSSP ensures compliance with software licences to prevent and combat computer software piracy in order to give effect to copyright associated with computer software by observing the relevant provisions of international and national laws, including the South African Copyright Act, and applicable licencing restrictions. When updated configurations are made to systems and alterations are made to structures, it must be documented accordingly so that when future changes are planned, AS-IS documents can ensure smooth transition.

4.7.11 Project management

The research project for the thesis was initially about the digitisation of archives and modernisation of the SACSSP’s operations (D27). During the initial assessment, the researcher found that the computing hardware and supporting infrastructure were obsolete (D8, D14). The scope of the project was expanded to assist and empower the organisation to fully implement a digitised I&T environment (D8, D9, D14, D15). The following projects were identified as stated in Table 4-8:

Table 4-8: Projects identification

Projects identified	Scope of work and procurement items
System development	System customisation
Off-the-shelf software	Virtualised software, backup and replication software, server software and licencing costs
ICT hardware	Procurement of servers, installation and configuration
Networking equipment and digital phones	Power over Internet (PoE) Network switches VoIP phones
Digitisation of archived records	Outsourcing or rental of scanning device
Server room upgrade	Procurement of electrical accessories and installation Procurement of floor raising consumables and installation Purchase and installation of cooling units
Data verification	Verification in the population register

Once the projects were identified, participants responded to the question “Do IT projects fail to deliver what they promised and, if so, why?”

“Systems development managed through project plan and does not overspent. Magnitude of projects is huge.” (P1)

“IT does not fail. Despite the impact we have since we developed the department, the assistance is to the business. The only instance where we had overrun, it was unplanned and costly and unbudgeted because we had to buy firewall and anti-virus. Not informed from graduates and had to buy extra computers.” (P2)

“Proper planning and introducing an integrated system linked to all strategic units.” (P4)

“IT is not failing. Most of the projects are in progress and others are to be finalised. This will help the business to deliver on its business.” (P5)

“No, they do not fail. The reason is what they have implemented so far.” (P6)

“When there are projects, they work overtime. They are dedicated.” (P7)

“We have had projects taking place for upgrade and improvising on IT.” (P8)

Identified projects required proper planning, financial resources and buy-in from strategic units that would utilise the IT services. IT staff were seen as committed where they were working beyond the call of duty.

4.8 THEME FOUR: DELIVER, SERVICE AND SUPPORT

The purpose of deliver, service and support (DSS), as indicated by ISACA (2018a), is the delivery of I&T operational and service outcomes as per the plan. The responses were organised into the following sub-themes:

Operations management; Service requests and incidents; Problem management; Continuity management; Security services management; and Business process controls management

4.8.1 Operations management

Operations management consists of performing operational procedures, managing outsourced I&T services, monitoring I&T infrastructure, and managing the environment as indicated in the thematic way.

4.8.1.1 Perform operational procedures

No other standard operating documents were available for inspection. A manual was created and sent together with all MS Teams invitations to all guests (D24). See Figure 4-34.

[Join Microsoft Teams Meeting](#)

[Learn more about Teams](#) | [Meeting options](#)

2 Attachments

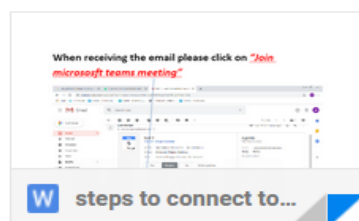


Figure 4-34: Procedure to log into MS Teams

While there were no SOPs in place, there were pockets of procedures that were observed. The staff's computers were updated with anti-virus definitions and software patches weekly in an ad-hoc manner.

4.8.1.2 Managed outsourced I&T services

The outsourced I&T services were conducted on a time and material basis, with no standing contract. The current contract of outsourced services with one of the external service providers hosting a database does not allow SACSSP employees access to their own information. (D18, D19)

4.8.1.3 Monitor I&T infrastructure

While the organisation had video cameras, including outside of the data centre, the researcher discovered the cameras were not monitored, since the display screen was placed inside the data centre, not at security control (D14). Figure 4-36 is a result assessment conducted.

4.8.1.4 Manage the environment

It was found that the network and cooling pipelines to the server room were in a state of disrepair (Figure 4-35). The air conditioning inside the server room was found to be providing adequate cooling to computing devices. The drawback was the old computing devices and boxes that were stored, as depicted in Figure 4-36.



Figure 4-35: Networking and cooling assets
(Photographer: Researcher 2020)

The depiction of an old server room in Figure 4-36 in page 176 was based on an assessment and walkthrough conducted. It was found that the data centre did not meet the minimum standards (Figure 4-36).



Figure 4-36: Old server room
Photographer: Researcher (2020)

Further walkthrough revealed the placement of the fire extinguisher was in line with the minimum standards to be used in case of fire and the signage was visible (Figure 4-37). One striking feature observed about the door to the server room was that it was a conversion of a strong room.

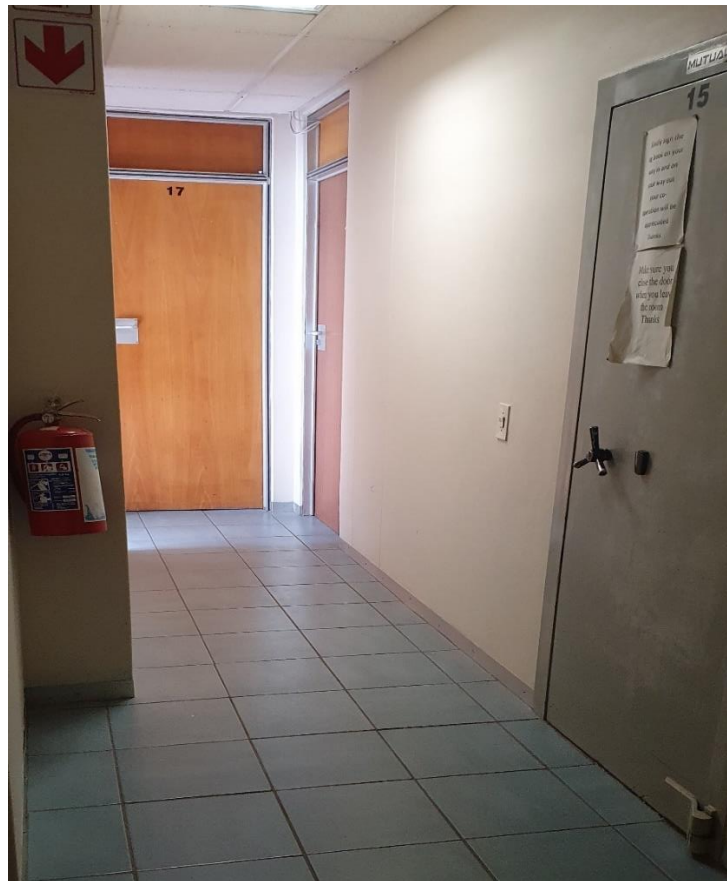


Figure 4-37: Fire extinguisher outside old server room
(Photographer: Researcher 2020)

Figure 4-38 depicts that the server room notice was visibly displayed for auditing purposes. The importance of the notice is to alert anyone who intends to enter the server room to sign the internal logbook so that it correlates with surveillance cameras if an incident occurs.

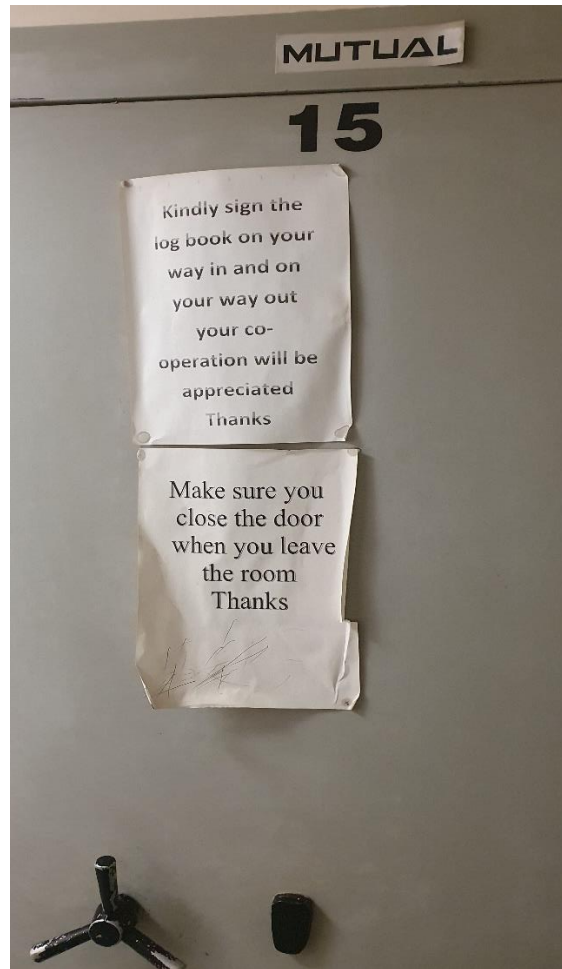


Figure 4-38: Server room notice
(Photographer: Researcher 2020)

Respondents responded as follows to the question “Are you running an efficient and resilient IT operation?”:

“Not at the moment. Looking at the last challenges addressed above, IT is not resilient. IT system is obsolete and not running efficient system. Database is rendering the system inefficient.” (P1)

“Now the place is running smoothly. Council is small and need someone to do IT support.” (P3)

“Yes, because since we have IT, we do not struggle with working tools, and internet connection is fast. They can assist remotely with your machine at home.” (P5)

“We can call using landlines while we are at home for work-related issues and we have video-conferencing meetings. Yes, the database is fast. We have upgraded the internet. They make sure that every morning, they do their round checks and to make sure that systems runs well. When I go to the system, I don’t struggle for sending emails and calls. It makes my job easier.” (P6)

“My system that I access is fast. We have better cabling. Now everything is working fine and you cannot make excuses about the system. There is no fighting now. If you were here last year, it was bad.” (P7)

“We run daily updates and check-ups on the environment from checking on users to resources and communication overall between users and the environment. The internet speed and connection improved. Our job is very transparent; efforts are eye visible, from network improvement, fibre connection, VOIP and Servers.” (P8)

There was an overall satisfaction with the IT services provided. Participants were able to work remotely to provide services.

4.8.2 Service request and incident management

Internally, the requests for IT services are done at ad hoc basis. There was no system to record calls and there were no defined service levels to adhere to. There used to be a call centre system and staff manning the calls; however, the system was replaced by a keyboard system. The old system used to give statistics of calls handled and calls lost. Most calls were lost. No adequate reporting was done on the number of calls received (D9). Email queries were better because payment receipts could be

downloaded and attached to the reply email. The incident response policy and procedure were still being developed (D8). The procedure that has been formulated was for lodging complaints against SSPs by external stakeholders (D10, D27).

Focus group discussions revealed that it took some time for IT incidents to be attended to when calls were logged. There were days when the office could not access their applications if a problem affecting their servers, which made the turn-around time longer. Further discussions were about a retired call centre system that came with the previous telephone system and it used to give them monthly statistics of calls attended and those that were dropped. Ever since the contract ended, there was nothing in place.

4.8.3 Problem management

Problem management was non-existent because of service request and incident management was not implemented. The main concern was the unavailability of systems; however, that problems were addressed through the purchasing of new servers, upgrading of asymmetric digital subscriber line (ADSL) to fiber lines and laptop replacement. The outsourced IT services were a problem and the organisation created a position in order to insource services. (D27)

4.8.4 Continuity management

The thematic network sub-theme illustrated the continuity efforts the organisation has embarked on. Backups were made and transferred to the disk. The archives room, as depicted in Figure 1-1 on page 6, was flooded in February 2020, creating a challenge for the organisation. The fire extinguishers installed in the archives room, as indicated in Figure 4-39, were placed in different locations. (D23)



Figure 4-39: Fire extinguishers in archives room
(Photographer: Researcher 2020)

IT provision was visible in the organisation, even when staff were working remotely due to the covid-19 lockdown through MS Teams video-conferencing (Figure 4-40). (D16, D19)

FW: IT and Business Engineering Committee Inbox x

Libe Molapo LibeM@sacssp.co.za [via sacssp.onmicrosoft.com](mailto:libem@sacssp.onmicrosoft.com) 29 Apr 2020, 10:45
to me

<div style="background-color: #0070c0; color: white; padding: 2px; border-radius: 3px;">Apr</div> <div style="background-color: #e6e6e6; padding: 5px; border-radius: 3px; font-weight: bold; font-size: 1.2em;">29</div> <div style="background-color: #0070c0; color: white; padding: 2px; border-radius: 3px; font-weight: bold; font-size: 0.8em;">Wed</div>	<p>FW: IT and Business Engineering Commi... View on Google Calendar</p> <p>When Wed 29 Apr 2020 10:30 – 13:30 (SAST)</p> <p>Where Cloud 9</p> <p>Who Libe Molapo*</p> <p style="text-align: center;"> <input type="button" value="Yes"/> <input type="button" value="Maybe"/> <input type="button" value="No"/> More options </p>	<p>Agenda <i>Wed 29 Apr 2020</i></p> <p><i>No earlier events</i></p> <p>10:30 FW: IT and Business Engineering Commi...</p> <p><i>No later events</i></p>
--	---	--

-----Original Appointment-----
From: Libe Molapo
Sent: Wednesday, 29 April 2020 10:18
To: Libe Molapo, Andries Viviers; Lorraine Masipa; Langi Malamba; Vincent Hlabangana; Elaine Harrison; Crosby Noko; lucky jacobs
Subject: IT and Business Engineering Committee
When: Wednesday, 29 April 2020 10:30-13:30 (UTC+02:00) Harare, Pretoria.
Where: Cloud 9

Good day,

Kindly find attached meeting request.

Crosby confirmed the meeting can go ahead without him as he doesn't have a laptop and his cell phone is giving issues. He asked we mail him the minutes and he approve/comment

Thank you
Malome Libe

[Join Microsoft Teams Meeting](#)

Figure 4-40: IT and Business Re-engineering Committee MS Teams invitation

Employees were able to connect to the office network with the AnyDesk remote desktop application in order to access their office applications. The ICT policy outlines the pockets of continuity in case of a major disaster, in which case access to key services and data would be needed (D26). Email was one of the key holders of data for the organisation and the organisation could continue with business by accessing the recent emails. The email system was migrated from an on-premise system to Office 365 to ensure the system's continuity. (D22, D23)

Participants were asked: "How critical is IT to sustaining the enterprise?" Four participants responded as follows:

"Financial information – backup system that was stored on cloud." (P1)

"Registration database is critical and council is all it is about." (P3)

"I think IT person works with contractors for skills transfer and information sharing." (P5)

"Yes, regular back-ups. It is essential for IT to sustain the enterprise. The enterprise entirety requires IT, as the database for council runs on cloud and all resources needed for client's services are electronic based." (P8)

Fire extinguishers were deployed in the archives room and in the server room to be used in the event of fire. Continuity was also observed when the council was able to have virtual meetings; one of the benefits of which was that they could quorate as even though there was no physical meeting attendance. Systems backup for finance and registration were important for sustaining the organisation.

4.8.5 Security services management

Security controls were in place, including 24-hour physical security services and surveillance. There were surveillance cameras around the facility, even the server room was under surveillance (Figure 4-41). The entrance to the old server room used a key, as indicated in Figure 4-38. What was not clear was whether there was a register of anyone accessing it and no register could be seen to validate access. The organisation also had physical access measures in place such as a 24-hour security, armed response and electric fencing around the premises.



Figure 4-41: Surveillance camera
(Photographer: Researcher 2020)

The entrance to the organisation involves guests completing and signing the attendance register and receiving a slip that must be handed back when the guest leaves the organisation (Figure 4-42). In the case of this receipt, the information written on the access control receipt was not verified against of the guest's identity document/card.

243 Louis Botha Ave
Orchards
Johannesburg



Tel: 011 551 1600
Fax: (011) 485 2802

MAXI
SECURITY

M
881717

ENTRY CONTROL - VISITORS

DATE: 21/11/2020 TIME IN: 10:53

I.D No.: [REDACTED]

NAME: [REDACTED]

VEH.REG.No.: [REDACTED]

FROM WHICH COMPANY: [REDACTED]

No. OF PEOPLE: [REDACTED]

TEL No.: [REDACTED] PERSON TO SEE:

REASON FOR VISIT: [REDACTED]

I AGREE TO THE FOLLOWING CONDITIONS:

1. The Company reserves the right to inspect and search all vehicles and goods therein on entry to, and on exit from, the premises.
 2. All security and safety notice on these premises must be strictly adhered to.
 - N.B. The Company cannot be held responsible for any injury or loss or damage sustained by the person or persons or vehicle/s admitted to the premises vide this permit.
 3. No Firearms Allowed.
 4. No Smoking Allowed
- SIGNATURE OF VISITOR: [Signature]

PLEASE HAVE THIS PORTION FILLED IN AND RETURN TO SECURITY GUARD BEFORE LEAVING THE PREMISES.

Signature of Person Visited:.....

Print Name:.....

TO BE FILLED IN BY SECURITY GUARD

TIME OUT:.....

SIGNATURE OF SECURITY GUARD:.....

REM 082 486 3456 REF: 000286

Figure 4-42: Access control receipt

In compliance with the occupational health and safety (OHS) regulations and data centre standards, a fire extinguisher was installed as part of a fire suppression system (Figure 4-43).



Figure 4-43: Fire extinguisher
(Photographer: Researcher 2020)

Figure 4-44 depicts that a fire prevention door with security features was installed to protect the new server equipment the organisation invested in.



Figure 4-44: New server room door
(Photographer: Researcher 2020)

A question was asked to participants to investigate the physical security arrangements used to protect organisational data. “Is the information you are processing well secured?” There were diverse responses, as indicated below:

“Those files will be lost in time of a natural disaster.” (P1)

“Files are archived in room stores. It is a control area with restrictions to certain officials.” (P2)

“Make sure that resources are locked in a safe place. We have security cameras. They make sure in following safety standards using CCTV cameras, fire extinguishers, air-conditioning and safety door in server room.” (P6)

“We do have security. IT staff always the lock server room. There is a camera in a server room and fire extinguishers. Server room floor is raised.” (P7)

“All IT resources are secured, from server room being theft and fire secure. Fire extinguishers are at all designated spots. As previously mentioned, the current environment is secure.” (P8)

All the physical security mechanisms such as entrance control, surveillance, cooling and fire suppression systems were implemented to serve as minimum standards for the data centre.

4.8.6 Business process control management

The business process controls management sub-theme ensured that organisational processes were correctly captured to assist with automation. The template for business process mapping was developed to map out the system requirements (D8). Figure 4-45 shows the AS-IS document that was used to develop the process flows for the organisational divisions. (D9)

TEMPLATE FOR BUSINESS PROCESS MAPPING: SACSSP

List the processes for each of the main functions in your department as listed in the diagram below:

REGISTRATION	EDUCATION, TRAINING & DEVELOPMENT	PROFESSIONAL CONDUCT	FINANCE
New application learners	CPD event applications - providers	<p>Complaint process</p> <p>-Complainants access the complaint form from the website or ask the office to email or fax it to him/her. Others access complaints forms through walk-ins in the office.</p> <p>-Complainants complete the form (typed or hand written) and email, fax or hand deliver the form.</p> <p>Stage 1</p> <p>Upon receipt of the complaint, we:</p> <ol style="list-style-type: none"> 1. Verify the registration status of the Respondent (registration database and retrieval of a file from Archive). 2. Assess the complaint to determine if whether we have jurisdiction to process the complaint. 3. If the person is not registered, the matter becomes a criminal matter and the client (complainant) is advised to lay criminal charges. 4. If the person whom a 	Accounts receivable

Figure 4-45: Business process document

The consolidation was developed to ensure all interlinked divisions are catered for as indicated in Figure 4-46, which was completed on 26 October 2018. The consolidated process flow was a combination of processes that were done by different divisions. The following processes were individually workshopped with the affected business units before consolidation between 21 July 2018 and 23 October 2018:

- Professional conduct
- Finance division
- Registration
- CPD logistics
- Assignment marking
- Quality assurance
- Foreign qualifications
- Payment
- Portfolio of evidence marking

The participants were asked “How do you improve business agility through a more flexible IT environment?” Below are some of the responses from respondents:

“We need a capability of issuing certificates digitally and a far more streamlined operation. We really tried to refine business processes and integrate to online system. Registration processes are important. Registering people to licence to practice which is vital to be able to practice their profession. Financial system – procurement and normal financial management and linking with registration. To keep the database up to date.” (P3)

“All divisions of council – registrations, professional conduct, ETD, finance, the office of the registrar and the strategic units require IT.” (P4)

“Registration process is important and the requirement is that the client must register with us.” (P5)

“For the IT system to assist finance with payroll (Sage) and registration using a database.” (P6)

“Finance and registration are vital business processes that are dependent on IT.” (P7)

“The heart and vital departments of SACSSP are finance and registration.” (P8)

All the operations of the council are dependent on IT. The registration system would be linked with the finance system and the bank system through an API. Figure 4-46 depicts a consolidated process flow to improve flexibility of organisational operations.

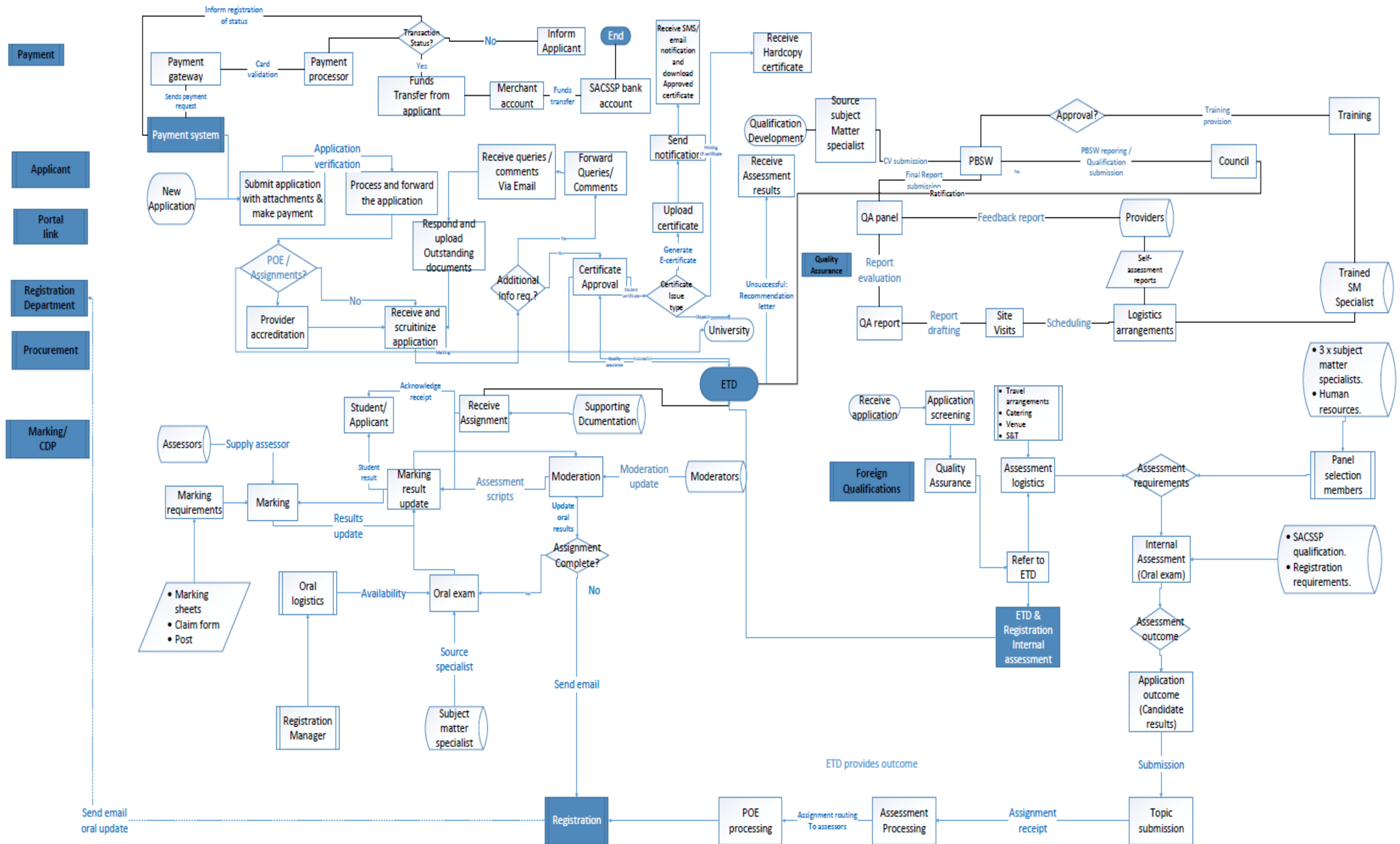


Figure 4-46: Consolidated processes

4.9 THEME FIVE: MONITOR, EVALUATE AND ASSESS

Monitoring of deployed solutions and processes to evaluate transparency of all sub-themes was arranged under the following sub-themes:

Performance and conformance monitoring management; Internal control system; External requirements compliance; and Assurance management.

4.9.1 Performance and conformance monitoring

There were no defined service matrices to be followed when calls were logged on outsourced services. However, the prescripts in the ICT policy state that the utilisation and efficiency of the council's ICT system would be monitored on a regular basis by the Registrar, supported by the ICT officer and the IT and Business Re-engineering Committee, in accordance with its mandate (D16, D18, D19). Furthermore, it states that the Registrar, with the support of the ICT officer, must provide on an annual basis, not later than 31 March, a comprehensive ICT status report in a prescribed format to the council via the IT and Business Re-engineering Committee (D26). This report must provide at least the following information: Status of all hardware and equipment with recommendations on changes and/or upgrades, if required and status of software and programmes used by the council's administration with recommendations on changes and or upgrades, if required (D21, D22, D26).

Participants were asked: "How do you manage performance of IT?" Seven responses were received:

“We have got an annual performance plan (APP) to manage IT performance. IT has its own APP and plan put in place key performance indicators (KPI) measured against the plan. Monitoring system – monthly reporting, quarterly reporting submitted to divisional head.” (P1)

“Every meeting we are supported to have feedback report, there is no good reporting. Investment – It is transparent and comes with financial reports. A board oversees and provide oversight of the performance.” (P3)

“The monthly reports from IT strategic unit and the oversight by the Business Re-engineering Committee and support from external IT resources. I believe so that IT investments are transparent.” (P4)

“I do not have knowledge if they are giving reports. There is performance management conducted annually. For me, there is transparency. We are aware that there was procurement of servers. Two buildings were connected through network cabling.” (P5)

“IT does its work and management looks at their performance. They are transparent because of different committees for approval.” (P6)

“I honestly do not know how their performance is managed. They are transparent because we call all to see.” (P7)

“The internet speed and connection improved. Our job is very transparent; efforts are eye visible, from network improvement, fibre connection, VOIP and Servers.” (P8)

Performance planning includes KPIs that can be measured and monitored accordingly through timeously reporting. Participant 7 did not have knowledge of how performance was managed. It would be beneficial that user education be conducted because the participants seemed not to understand the reports.

4.9.2 Internal control system

There is an internal control system in the organisation, which is under the oversight of the Finance Committee on financial matters, while the IT and Business Re-engineering Committee is playing a similar role for IT matters (D16, D18, D19, D25). The organisation has been empowered by the SACSSP Act to keep records in the prescribed manner of all the moneys received and spent, which include all its assets and liabilities. (D1, D2, D23)

To investigate accountability, the following question was asked: “What are the (control) requirements for information?” Four participants stated that:

“Normally, we keep information onsite, files for members in filing room. Those files will be lost in time of disaster. There will be a loss of files if fire can occur. The financial information is backed up and stored on cloud. Our normal work functions are segregated according divisions and audit trail of what it is happening.” (P1)

“Honestly, they (IT) are transparent. You need to explain everything depending on the amount required.” (P2)

“Yes, efficiency and effectiveness of our internal controls are to a large extent possible. We are still cleaning up some policies; it’s work in progress.” (P4)

“I can’t capture and authorise on the system.” (P7)

While copies of transactional documents were archived, there was a possibility of loss during disaster. Transparency was key in operations. Finance staff were working with segregated functions in order to limit fraud.

4.9.3 External requirements compliance

The SACSSP is able to present their annual reports to the Parliament of South Africa as per the constitutional mandate (Figure 4-47). This process allows scrutiny of SACSSP operations by the parliamentary Portfolio Committee on Social Development through their briefing sessions. In terms of the act, the organisation is required to transmit the records, the statement of account and the balance sheet in the prescribed period, and those documents must be open for inspection by the public at prescribed places during the prescribed periods. (D1, D2)

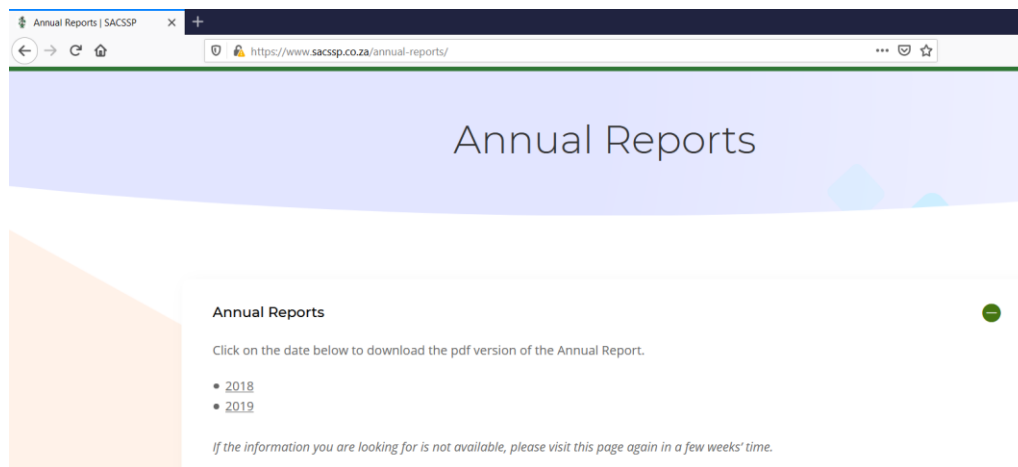


Figure 4-47: SACSSP annual reports
Source: SACSSP (2021)

The presentation to parliament portfolio committee of Social Development on the 31 October 2018 by Department of Social Development and SACSSP, highlighted concerns is that the Department of Social Development did not consider the SACSSP

as one of its entities; rather, it is registered as a non-profit organisation (NPO). It is evident even in reporting to parliamentary presentations that it is not regarded as part of DSD's entities (Figure 4-48). D28 is an extract that indicated the entities reporting to Department of Social Development.

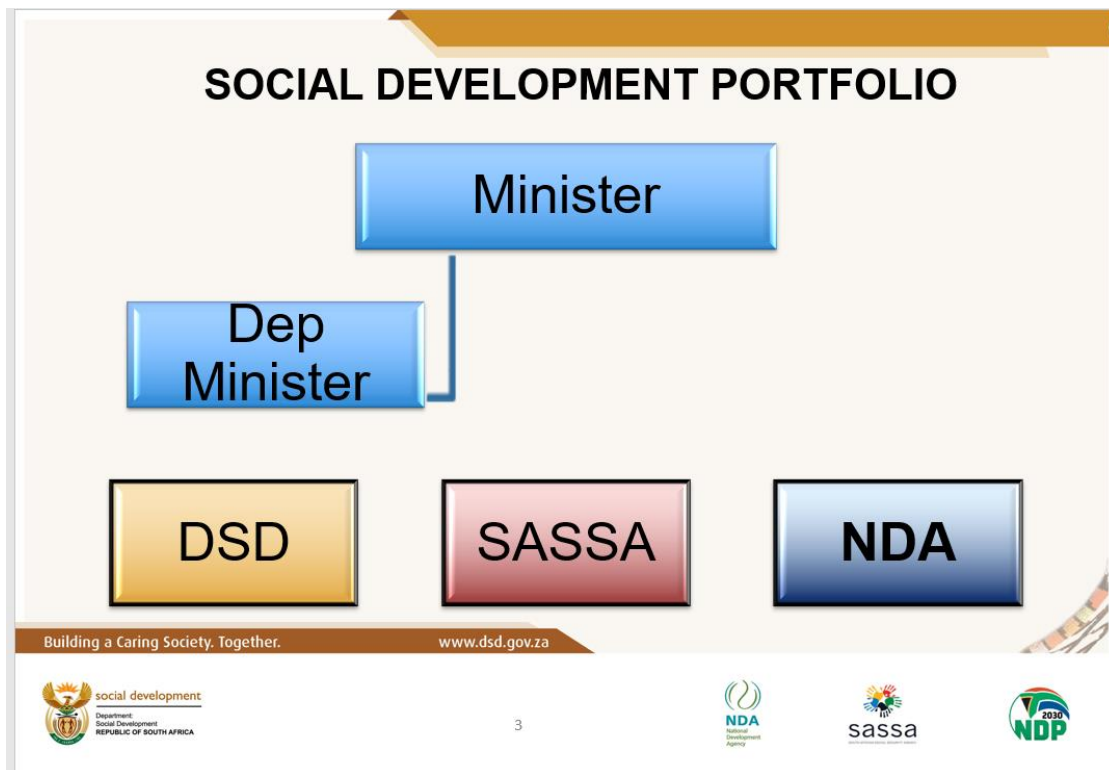


Figure 4-48: DSD Presentation on budget vote

The DSD experienced a challenge in that they struggled to obtain audited financial reports from the SACSSP as presented to Parliament (D28). The ICT policy prescribes a regulatory compliance regarding the storage and retention of documents and email messages to obtain more information on external compliance (D26). The participants were asked regarding the topic. The following are some of the responses to the question: “How do you know whether you are compliant with all applicable regulations?”

“It is difficult to provide assurance and at times you get complains from stakeholders. Yes, very transparent. Number of structures need

to pass through. Bidding process to ensure transparent. Bid Evaluation Committee (BEC), Bid Adjudication Committee (BAC), then Exco and, lastly, the council to do approvals in investments. Lacking to ensure compliance. Having a person ensures that our lives are easy. Revise the policies to be compliant to the rule and regulations of the country.” (P1)

“Honestly, they are transparent. You need to explain everything depending on the amount required.” (P2)

“Designing the system around the regulations, block certain things that are not in regulation. Trust the new system.” (P3)

The next sub-theme presents the assurance management.

4.9.4 Assurance management

The audit report revealed some shortcomings in organisational record keeping. Further to that, section 5 of the finance policy states that the Registrar must ensure that (D25):

- recordings of all invoices and receipts issued to registered professional are kept
- all proper records of all payments and the fees payable are kept
- a report of reconciling of debtors and status of debtors are presented to the Finance Committee and the Executive Committee on a monthly basis
- a report tabling a yearly figure of debtors payable to the council is be included in the audited financial statements.

Some of the audit findings related to the following:

- Inadequate internal control processes in place to maintain adequate supporting information and records by the council.
- Critical positions remained vacant for extended time period, resulting in work overloads and inability to execute all mandates by council.

Based on the audit finding highlighted, it is clear that the SACSSP Act's clause on book-keeping and auditing, which states that "the council shall cause records to be kept in the prescribed manner of all moneys received and spent by it, of all its assets and liabilities and of all financial transactions entered into by it, and shall as soon as possible after the end of every financial year cause statements of account and a balance sheet to be prepared, showing the prescribed particulars in respect of that financial year", is not being complied with. (D1, D2)

To investigate assurance management in the organisation, the following question was asked: "How do you get assurance over IT?" The following were the responses:

"There is segregated on IT systems according to divisions and audit trail of what is happening. They shared with us the service times (standard operating procedure). We now know or are assured that our problems will be worked on or the problem resolved. Their own assessment and changing our passwords. They do not let our password expires and advises on the procurement of IT infrastructure and trust what they are doing. Their performance is reviewed on quarterly basis." (P1)

"Unfortunately, cannot give assurance since they get services from somewhere." (P2)

"Assurance – do not know. Registrar with Finance manager – things signed off and not making sure that deliverables are met." (P3)

“The assurance is that everything is working. Based on the agreements signed, we are able to pay the external providers. Yes, whatever I want to do on the system, I can get to do.” (P7)

Segregation of duties gave assurance regarding transactions performed with checks and balances. The same could not be said about outsourced services, as stated by one participant. The signing of SLAs gave assurance that services would be provided.

4.10 SUMMARY

This chapter presented the results of the participants who were grouped according to five COBIT 2019 constructs. Documents, system, minutes of meetings and focus group notes were thematically analysed and presented according to the research objectives as indicated in section 1.3 of chapter one. The most important results obtained from the study were as follows:

- The organisation has well-established corporate governance structures in place to achieve stated goals.
- While the strategy was cascaded from the board to management, there were challenges with most of the planning elements due to the size of the organisation.
- Management had clear requirements that could be used to support the board in executing its mandate; however, historic challenges and disparaged systems have been an *“Achilles heel”*.
- Most operations were in place, while some were done ad-hoc.
- Proper monitoring and evaluation systems were in place for management to report back to the board as per the regulations.

The following chapter interprets and discusses the research findings.

CHAPTER FIVE

INTERPRETATION AND DISCUSSION OF RESEARCH FINDINGS

5.1 INTRODUCTION

The previous chapter analysed and presented the results obtained from focus groups, hardware and system analysis, benchmarking exercises, and open ended-interviews. Chapter five focuses on the interpretation and discussion of the results. Given (2016: 164) describes this chapter as being used by a researcher to weave the participants' voices, along with published literature, in order to give perspective to the research findings.

The results presented are interpreted and discussed following the research objectives:

- To determine how information governance can ensure that corporate governance can play a role in the evaluation, direction and monitoring of the council's strategy.
- To review how information governance planning can assist in business alignment at the SACSSP.
- To determine how the SACSSP can implement programmes and projects that support business processes.
- To review the outcomes of information governance and related technologies as per the planning.
- To establish how information governance can provide transparency in the monitoring of performance and conformance to drive the achievement of goals.

5.2 EVALUATE, DIRECT AND MONITOR

Evaluate, direct and monitor is a domain in COBIT 2019 that can be used as a catalyst by the board of the SACSSP to implement governance and be able to achieve the

organisational goals. The evaluation of the SACSSP's strategic plan and internal and external environment to:

- identify the SACSSP's stakeholder needs and how it should be realised
- determine the value ICT is expected to create through its enablement of the business
- define the benefits ICT is expected to realise in its enablement of business
- articulate ICT risk appetite and how it should be managed within the risk management regime of the SACSSP
- facilitate the establishment of sufficient ICT organisational structure, resources, capacity and capability
- evaluate and monitor significant ICT expenditure
- determine the monitoring criteria and reporting requirements
- broadly understand the implications of the ICT prescriptive environment
- evaluate the change management requirements for the implementation of governance system.

The recommendation for the organisation should conceptualise and direct business enablement by ICT arrangements:

- Direct the development of the ICT plan, ICT implementation plan and ICT annual performance plan
- Ensure integration of IT governance into the agenda of the Executive Committee.
- Approve ICT governance policy and charter, ICT plan, ICT implementation plan (budget), ICT operational plan (APP) and other related plans and policies
- Approve portfolio of ICT projects and its related expenditure
- Provide direction for the change management requirements for the implementation of CGICT
- Guide implementation of the framework and related policies and strategies

Monitor that implementation conforms to the criteria:

- Conformance, performance and assurance oversight and monitoring.
- Ensure that risk is managed and the ICT audited internally and independently.

The findings of the objective are presented and discussed according to the following sub-themes: governance framework setting and maintenance, benefits delivery, risk optimisation, resource optimisation and stakeholder engagement.

5.2.1 Governance framework setting and maintenance

Zikopoulos et al. (2013: 216) state that a governance framework setting leads to an agreed vision, mission and strategic objectives that can lead the organisation in the right direction. According to Ekpe, Eneh and Inyang (2015: 136), a vision such as the one the SACSSP has adopted (Social service practitioners united in excellence) can be equated to a mental picture that describes an encouraging direction that an organisation can aspire to take. Griffin et al. (2016: 531) advise that leaders should develop a clear sense of mission and values about the intentions of the organisation, while communicating the same to its employees of what key performance areas (KRA) are and how they can be measured. ISACA (2018a: 35) advises that there should be optimisation of digital transformation programmes and internal business process functionality to support the enterprise strategy. It should be noted that the organisation adopted I&T-enabled initiatives that are highlighted in the strategic plan and are anticipated to support business needs through the implementation of cost-effective solutions that bring reliable and accurate data throughout the organisation.

The findings suggested that the SACSSP has properly constituted governance structures as highlighted in the system, document analysis and interviews conducted.

5.2.2 Benefits delivery

The SACSSP board has undertaken certain initiatives to make sure the organisation achieves its strategic mandate through the initiation of I&T-enabled investment programmes based on challenges identified in chapter one. The organisation realised that in order to reap benefits from IT investment, a strategic objective number three had to be formulated to “ensure an efficient registration and process for social service practitioners” through a fully automated application process (SACSSP 2016b: 8). It was found that the SACSSP strategic plan only states that the King III corporate governance framework has been adopted; however, there was no architecture alignment framework to guide the organisation-wide information solutions planning. Solutions identification was conducted and some participants received value from IT services and were in alignment with the business strategic objectives in order to contribute to the service delivery challenges encountered at the SACSSP. The solutions such as digital phones, VPN, virtualised software, backup and replication to the cloud, and the employment of IT resources, are some of the digital transformation initiatives that bring benefits to the organisation.

I&T investments bring with them benefits by optimising the core business so that it achieves its goals. The IT and Business Re-engineering Committee adjudicates the technical elements of IT investments, while the Finance Committee considers the financial risks of such purchase. According to Valacich and Schneider (2018: 84), strategic alignment brings benefits, such as, competitive advantage against other competitors. An integrated online system would add value as it would address the external stakeholders that need to perform transactions such as registration, payment and updating of their details without being present in the office. One more benefit would be VPN access by staff to perform daily tasks. Having an approved organisational strategic plan document would encourage the executive authority to support the I&T-enabled investments (RSA 2012: 16).

5.2.3 Risk optimisation

Having observed that some pockets of information resided outside the organisation, the study raised issues of non-compliance with or violation of the ICT policy (IODSA 2009: 15). Risks included a lack of resources, off-site storage challenges and non-adherence to IT policy. Two of the most important components to corporate governance, namely strategic plan and audit report, highlighted organisational risks that needed to be addressed and mitigated. Five strategic risks and two operational risks were mitigated and reported on during quarterly IT and Business Re-engineering Committee meetings.

During the in-depth interviews conducted, only three participants mentioned risks. A prominent risk mentioned was the BOYD devices. The use of BOYD devices should be included in the organisational risk planning process that would involve conducting of risk management planning, identification, analysis, response planning, response implementation and monitoring risk (PMI 2017: 395). The upgrade of a firewall was initiated and weekly anti-virus checks on all organisational computers were performed by IT resources to mitigate the risks (ISACA 2020: 14).

5.2.4 Resource optimisation

The organisation's human resources department, as highlighted in Table 4-4, indicated some degree of stability, while the registration division had a high turnover even though it is the core of the operations of the council. The resultant process of appointing an IT officer and insourcing IT services has been supported by the board and the management of the organisation (ISACA 2018a: 45). Finance also plays a huge role in filling vacancies. The SACSSP Act indicates that there may not be fewer than 19 and more than 34 board members (RSA 1978: 4). However, the number of board members at the time of the study was 13. The researcher could not ascertain whether the decision to have 13 board members was financially related. Hardware and system

challenges were being addressed through the server hardware refresh, laptop replacement and proposed integrated system development (Reddy et al. 2015: 240).

Most of the interview participants indicated that they had the latest high-end computing equipment after the replacement of the slow and old computers. Financial resources were stated as a limiting factor.

5.2.5 Stakeholder engagement

SACSSP stakeholders include the board members, section 9 and 10 committees, industry partners, government departments, Parliament, social service practitioners and the public, as mentioned in Table 4-1. Some of the roles are not fully exploited. The challenges experienced included data management where SSP details are verified against the population register so that there is a smooth transition to the second phase of verification qualifications. The organisation has been communicating with its stakeholders through the strategic plan, annual meeting calendar published, presentations at governance structure meetings, such as Parliament and the Department of Social Development (ISACA 2018a: 50). The SACSSP Act prescribes submission documents that can be viewed by the public for a prescribed period (RSA 1978: 13). Periodic notices are also published on the SACSSP to inform the SSPs about any information that is relevant to them.

5.3 ALIGN, PLAN AND ORGANISE

Planning involves the strategic alignment of business strategy and I&T enablement to provide a consistent, integrated approach to the planning of the use of I&T in the SACSSP's service delivery mandate to the social service practitioners. This section discusses the results of 14 processes as per the objective.

5.3.1 I&T management framework

The I&T management framework is concerned with the individual accountability and responsibilities with regard to the ICT function and its operations (RSA 2014: 11). One critical aspect is that the records management policy is not approved. This is a limitation to ensure that all service delivery to the business, infrastructure, systems and related activities are focused on fulfilling the ICT plan. This is executed by providing a properly structured and sustainable ICT environment and ensuring that risks are appropriately managed. A management framework is implemented through allocating structures, functions, roles and responsibilities within a governance system, as well as through (ISACA 2018a: 55):

- processes
- principles and policies
- organisational structures
- skills and competencies
- culture and behaviour
- service capabilities
- information management.

Six I&T management framework documents have been approved, as indicated in Table 4-2, while the crucial policy document governing the records is still a draft (The Cabinet Office 2011a: 246). Only two out of eight participants mentioned management framework structures. The organisation operates in a highly regulated environment and the identified documents serve as I&T management components.

5.3.2 Strategic management

Strategic management in organisations is a well-established practice, which is performed to improve the effectiveness and efficiency of SACSSP. Axelos (2020b:

132) states that external and internal audit findings are incorporated into the services roadmap in order to provide independent governance of such service. In this context, the alignment of the SACSSP to the fifth board mandate was achieved and staff were empowered with resources, processes, infrastructure, systems, information and related technology to perform their work (RSA 2010: 1). In line with the responsibility of strategic management of the SACSSP, the strategic plan is articulated in the five-year approved strategic plan, which eventually would result in the operationalisation of the strategy in the annual performance plans (Ansoff, Kipley, Lewis, Helm-Stevens & Ansoff 2019: 12). Strategic management practice ensured that the SACSSP formulated the organisation's goals, together with the development of policies and implementation of plans (Axelos 2020a: 16).

One of the strategic challenges that the document sought to address was system integration to assist with timely receipt of information for decision-making. Five participants responded on strategic managements matters. Of importance was the responses from participants 2 and 3, which placed more emphasis on IT alignment to the organisational strategy.

5.3.3 Enterprise architecture

However, it was established that no common enterprise architecture was adopted that would assist in having business process, information, data, application and technology architecture layers, as well as the development of re-usable building block components (ISACA 2018a: 73). Two participants who responded to the question partially stated the elements related to it. However, their responses did not adequately address the question.

In this construct, the SACSSP would create an enterprise architecture by way of adopting internationally recognised frameworks, such as TOGAF or GWEA and methodologies, which reflect the way in which they deliver services to social service

professionals. Enterprise architecture practice articulates the SACSSP's external and internal environment, defining its service elements, the relationships between the elements and its environment, and the principles guiding its design and evolution. The purpose for the SACSSP to utilise the enterprise architecture practice is to help a department design how to effectively and efficiently deliver on their mandate.

The COBIT 2019 framework provides a domain whose role is to implement a consistent management approach for enterprise governance requirements to be met, covering governance components such as management processes; organisational structures; roles and responsibilities; reliable and repeatable activities; information items; policies and procedures; skills and competencies; culture and behaviour; and services, infrastructure and applications (ISACA 2018a: 65).

The composition of enterprise architecture is as follows (The Open Group 2019):

- Business and information architecture planning articulates the business execution format and its objectives, rules, standards, processes, information, other resources and data requirements to execute the political mandate of the SACSSP, and this is known as the business architecture.
- Information systems architecture describes what major software is required to enable and, in some cases, fully automate the public service delivery in a more effective and efficient way.
- Technology architecture defines the technical infrastructure (such as telecommunication infrastructure, data processing centres, computers and ICT security requirements to enable the information systems to communicate, store and process data at the SACSSP.
- Migration planning allows the department to develop a migration roadmap between the current state of affairs and the ideal future as defined in the business and ICT architectures.
- EA implementation manages of the implementation of the migration roadmap.

The next section interprets the findings for innovation.

5.3.4 Innovation

Information governance, including data governance, usually supports or enables better evidence-based decision making via trustworthy information. Internet of things and artificial intelligence are discussed.

5.3.4.1 Internet of things

The current sources of data that can be used as a basis of IoT, as indicated in Figure 5.1, are an important foundation. There should be synergy or agreement on the standards of data integration for the success of harnessing data from the source. The IoT enabled a more meaningful analysis of data that can be analysed in real time to provide an organisation with business intelligence to better compete in the digital world (Valacich & Schneider 2018: 287). Table 4-3 in page 127 highlights the data sources (sensors) that the organisation can harness to ensure efficient and effective access to relevant data needed for decision-making. These data sources were needed for verification of registration details that were received from SSPs. The proposed IoT connection nodes are prescribed as per regulations and cleaning of organisational data. The external data sources are used for verification of new data that is being captured on the SACSSP databases, namely, the verification of identity numbers with the population register.



Figure 5-1: SACSSP internet of things connection nodes

The next section discusses the artificial intelligence that is needed from IoT nodes that SACSSP already has access to.

5.3.4.2 Artificial intelligence

Figure 5.2 depicts the process of creating an AI that involves the collection of data from some of the information as highlighted in Figure 5.1 about SSPs and other stakeholders. Machine learning looks for data patterns in which insights are realised through the development of algorithms to improve the accuracy of models. Physical intervention brings the ability to write a set of procedures that are specified for the benefit of an organisation by a human being. The creation of a predictive system based on set parameters brings a degree of certainty to future decision-making (Marwala & Hurwitz 2017). Those decisions are made rationally based on the logic of using relevant information and direction to optimally execute the required task (Marwala 2014). Data available streamed back to the organisation from IoT sensors can assist

in building neural networks that recognise underlying relationships in a set of data using a process that imitates the way a human brain functions. Axelos (2020c: 40) points out that the value of solutions, such as predictive analysis, is to project the future situation and enable proactive decision-making. The use of cloud computing is needed to train deep algorithms. The insights that are gained ensures that staff can make informed decisions.

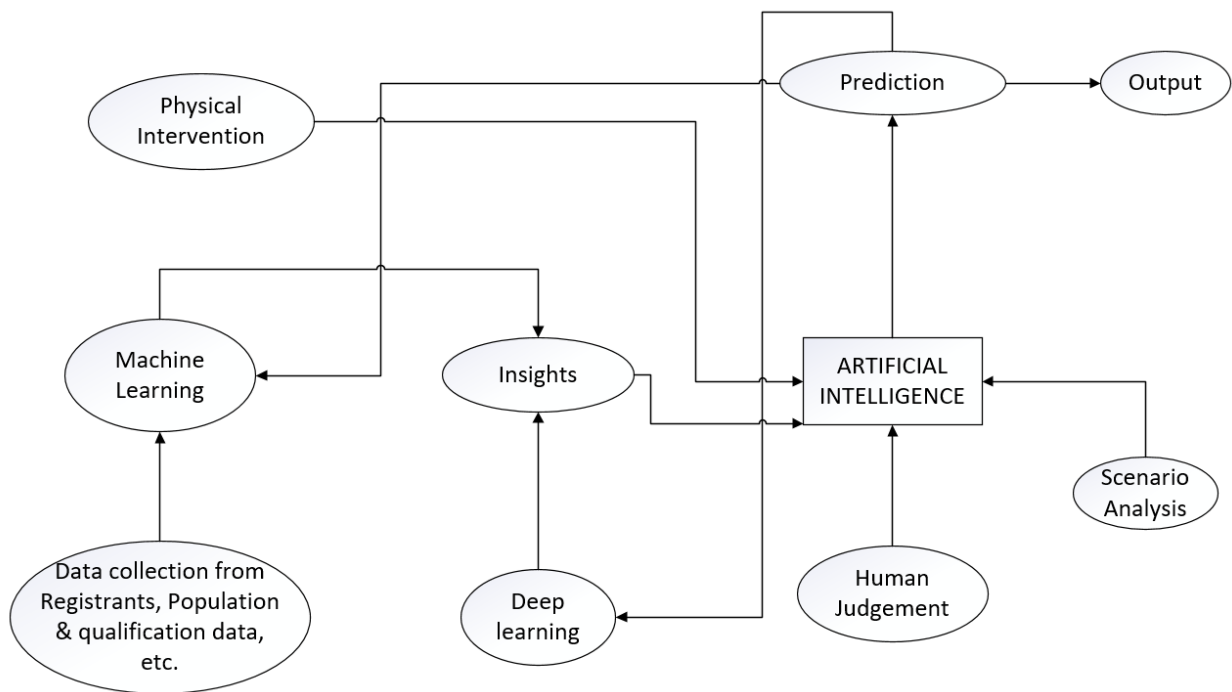


Figure 5-2: Proposed artificial intelligence framework
Source: (Mohapatra & Kumar 2019: 21)

Adopting the AI intelligence framework depicted in Figure 5-2 would ensure that challenges encountered by three participants in section 4.6.4.2 on page 128, are addressed and reporting is accurate and does not rely on guesswork. The main challenges were: staff was not able to present monthly statistics of calls attended; verification personal, qualification and data collected from SSPs.

5.3.5 Portfolio management

This function should be embedded in the organisational portfolio/programme management structure. It explains how the SACSSP can create the necessary capacity to manage ICT-related business programmes/projects. The SACSSP must standardise an internationally accepted methodology. This is informed by the COBIT 2019 process managed portfolio (APO05) and managed programmes (BAI01). Based on the adopted portfolios, the SACSSP would ensure that it has the right mix of programmes, projects, products and services to carry through its strategy within the confines of its funding and resource constraints (Axelos 2020a: 24).

The main public-facing portfolio of service centres on registration services, which include search the register and lodging a complaint to be investigated by the professional conduct division.

5.3.6 Budgeting and costing

With some of the challenges highlighted on the SACSSP's financial reporting by the national Department of Social Development, the PFMA outlines that public entities must: "prepare consolidated financial statements in accordance with generally recognised accounting practice for each financial year" and the minister concerned "must submit the consolidated financial statements and audit report on those statements within one month of receiving the report from Auditor-General, to Parliament for tabling in both houses" (RSA 1999: 15).

The organisation was compliant in the submission of budget planning and approval as depicted in Figures 4-10 in page 132 and 4-11 in page 133. Checks and balances were achieved because the organisation's management, together with the Financial Committee (FinCom), prepares and agrees on the budget that is tabled to the full SACSSP council for approval. The covid-19 pandemic put organisations under

financial pressure and the SACSSP was not immune to this. This was evident when there was an outcry to the Solidarity Social Workers' Guild's proposed subscription increases (Engelbrecht 2021: 8).

The organisational budgets are discussed by management and the IT and Business Re-engineering Committee, while the FinCom plays an oversight role. The discussion on hardware and software procurement illustrates in-depth financial discussions. All eight the interview participants were knowledgeable about the budgeting matters of the organisation. One issue that was raised by various participants was the prioritisation of funds for the IT budget allocation. Funds were requested from the DSD and more funds were shifted from other programmes. However, another issue raised by the auditors was that funds / transactions that were deposited were not traceable. Financial challenges led to some projects having been put on-hold. The main cost drivers for the organisation were the wage bill for staff and all needs related to board members, audits, disciplinary hearings, council operations and catering for emerging professions, and more.

5.3.7 Human resources management

According to the World Economic Forum (WEF) (2018), the following were found to be a good opportunity for a job that represents a desirable transition:

- The target job role is not forecast to decline.
- The role that an employee is transitioning to does not go below the current standard of living.

Table 5.1 represents the current and future target roles that the SACSSP can consider when transitioning from redundant roles when IoT and AI are properly implemented.

Table 5-1: Transition options for roles in the office, administrative job families.

Current role	Target role
Registration clerk	Customer service representative
Secretaries	Meeting, convention and event planners
Archive clerk	Data analyst
Mailroom clerk	Business process automation
Data capturer	Data analytics
Call centre agent	Customer service representative

Source: (World Economic Forum (WEF) 2018: 11)

Organisations should advocate for the continuous learning programmes in their environment in order to adapt to ever-changing business processes (Botha 2019). Section 189 of the Labour Relations Act proposes assistance to employees who might be affected because their roles became redundant due to the organisation's operational requirements (RSA 1995). It is also imperative that management should act sensitively when deciding which roles require automation, and have a discussion with employees concerned (Brandes & Wattenhofer 2016). Human resources are still an integral part of organisations because they can perform tasks such as negotiating, persuading and caring while being complemented by AI (Frey & Osborne 2017). It is on that note AI and IoT, which are proposed for implementation, will disrupt the status quo (McKinsey Global Institute (MGI) 2013). The study's intention is not to replace human resources, but rather to upskill them to be competitive in the digitised environment while being supported by such technologies (Nedelkoska & Quintini 2018).

Finally, there should be definition and management of the skills and competencies required of personnel. Regular verification should be done that personnel have the competencies to fulfil their roles on the basis of their education, training and/or experience, and it should be ensured that these competencies are being maintained,

using qualification and certification programmes, where appropriate (ISACA 2018a: 100).

5.3.8 Relationships management

ISACA (2018a: 36) supports the creation of governance structure, such as relationship managers within IT to enable greater business insight for the SACSSP, with the Business Re-engineering Committee currently playing that integral role. Axelos (2020d: 62) states that the service providers and customers need to build and manage a transparent relationship that focuses on the achievement of agreed service outcomes that are supported by mutual trust and optimises the costs and mitigation of risks. Having a single point of contact in the form of a relationship manager would ensure that whoever is identified at the SACSSP has sufficient technology awareness and have the appropriate level of authority to make decisions (ISACA 2018a: 108).

Out of the six participants who were involved in the interviews, participant 1 provided more insights into the relationship management at the SACSSP. Relations that were entered into with external suppliers were for service requirements such as, upgrades from ADSL to Fiber, as depicted in Figure 4-13 in page 137. Participant 2 clarified the different decision-making structures.

5.3.9 Service level agreements

The outsourced I&T services with third parties were not linked to any contracts and SLAs for hosting or providing such services. A lack of agreed SLAs had repercussions for the organisation when the service provider locked out the administrator access to the Microsoft Office® 365 admin portal. Security incidents occurred in section 4.6.13 in page 144, but because no signed SLA existed, it was not enforceable to give penalties to the external service providers.

According to Axelos (2020d: 118), SLAs are used to drive and track stakeholder value, including the expectations that must be aligned to it, with value co-creation mapped and planned, and service scope and quality to assist the SACSSP. The SACSSP would be able to measure the availability, reliability and security as part of SLA contracts that cover the specific service levels that must be provided and must be usable as a vehicle to resolve conflicts when problems arise (Valacich & Schneider 2018: 151). ISACA (2018c: 26) clarifies that when external service providers are consistently failing to deliver services according to agreed service levels, the cause may be to governance issues where services were not defined and tailored to fulfil business IT service needs. In fulfilling the business needs, the SLA should rely on a sound measurement and reporting that can assist the organisation in ensuring that improvements are initiated when targets are not met (Axelos 2020a: 42). All the eight participants have a better understanding of SLA processes.

The COBIT 2019 framework SLA process proposes that new or changed service level options should include service time, user satisfaction, availability, performance, capacity, security, continuity, compliance and usability, to ensure that the IT services are fit for use.

5.3.10 Vendors management

As the SACSSP does not have access to the CSD of the National Treasury, it has taken the correct path to advertise bids in order to attract more prospective bidders. Figures 4-14 in page 139 and 4-15 in page 140 are proof that IT service requests were sent out. The process of managing vendors from the time that bids are received includes quality assurance of received bids (proposal evaluation) in accordance with the advertised tender until award (vendor selection) (Valacich & Schneider 2018: 404). Axelos (2020d: 73) sees vendor management as a single point of a vendor's visibility

in the involvement of service delivery that is consistent and can enable realisation of value to the SACSSP.

The SACSSP should request access to the CSD system in the process of verification of suppliers. Having systems that are interoperable brings consistency through improved information sharing on suppliers that are not performing. It is of concern that services are requested through a website, while the State Information Technology Agency (SITA) is tasked with certifying companies that do business with state entities. The repercussion would be that unaccredited service providers would be doing business with the organisation with no means of recourse if something goes wrong.

5.3.11 Quality management

The process of sending notices and bulk SMSs to all social service professionals to update their records has not yielded the desired results. Authentication methods such as username and password, and linkage of the handset used must be implemented to ensure that the person updating the records is the person authorised to do so. A two-factor authentication can be employed if a user is using either web-enabled computing equipment or the fingerprint reader of any smartphone. These are represented by a facial image that is then compared to a stored image of a social professional with facial recognition software or scanning of such fingerprint, and the comparison is done. Sending documents to third parties creates problems relating to the POPI Act since data are exposed. The organisation should put in place mechanisms to mitigate data privacy issues that might arise. Systems proposed will have an API to send data for printing without human interaction. Section 107 of the POPI Act details punitive actions that would apply to organisations, such as a maximum penalty of R10 million or imprisonment for a period not exceeding ten years, or both, for guilty offenses (RSA 2013). ISACA (2018c: 28) warns organisations that issues of data quality or data integration can have a serious impact on the success of such an organisation and that

it is very important to establish correct processes, roles and responsibilities, among other requirements, in order to furnish the organisation with value from information.

It was found that the current system of sending letters by registered post had a high rate of returns. The cost of postage and storage of returned items was about R32.00 for a hardcopy certificate and R18.00 for other documents. All undelivered post is considered a loss because the organisation incurred the costs of posting. Authors such as Ngulube et al. (2017) echo the need for an archives repository to contain relevant records that can be consulted to fulfil people's requests. However, having analysed the records that were managed in a group, the researcher could not ascertain which organisation dealt with the preservation period of returned post and the disposal thereof.

This problem was also identified by Maluleke, Ngoepe and Marutha (2020) when they stated that university libraries also express the problem of losing materials in transit due to document delivery services by SAPO. This places significant financial burdens on academic libraries, as the costs cannot be recovered. However, the SACSSP has mitigating strategies to deal with the anticipated loss of certificates by sending them by registered post. This process involves documents being tracked from source to collection point and SAPO sending a slip to the recipient to be collected at the relevant SAPO branch.

5.3.12 Risk management

One of the challenges as raised by IODSA (2009: 15) was that organisations must address concerns of integrity and availability of systems in their care and not forget about other concerns such as unauthorised use, access, disclosure, disruption or changes to their systems.

The enterprise risk management policy must include how business-related ICT risks

would be managed and how capacity would be created in the risk management function to address ICT-related risks. This is informed by the ISACA risk IT framework and COBIT 2019 process on risk management (APO12). ISACA (2020: 33) advises that management should have proper understanding of risk inputs (Table 5-2).

Table 5-2: Risk matrix

Risks inputs	Risks workflow
Risk profile	<ul style="list-style-type: none"> • Identification of relevant risk scenarios. • The assessment of impact and likelihood of the scenario materialising, considering the current state of risk mitigating controls. • Overall rating of the risk based on the preceding inputs.
Current I&T-related Issues	<p>All IT issues can be reported through risk management, audit, senior management or external stakeholders.</p> <p>A clear differentiation must be made to rate the I&T issues so as to provide the adequate inputs to decide on the governance priorities.</p>

All organisations face uncertainty and the challenge for management is to determine how much uncertainty it is prepared to accept as it strives to grow stakeholder value. Enterprise risk management is the process that will enable management to identify, assess and manage risks in the face of uncertainty and, therefore, is integral to stakeholder value creation and preservation.

The objective of the risk assessment is to enable the SACSSP to take care of its risk management responsibilities, as set out in section 38(a) of the PFMA, and further expanded on in section 3.2.1 of the National Treasury Regulations published in terms of the PFMA. Four participants stated that risks were being addressed and monitored. The evidence of the risks is documented in the audit report, ICT policy and risk register.

5.3.13 Security management

The information plan and ICT security policy must ensure that classified information,

intellectual property and personnel information are protected in ICT systems. This is informed by the Minimum Information System Security (MISS) document and COBIT 2019 processes, managed security (APO13) and managed security service (DSS05). The scope of security management in organisations must address the following (ISACA 2018c: 76):

- Defining I&T security policies, plans and procedures and monitoring, detecting, reporting and resolving security vulnerabilities and incidents.
- Understanding security requirements, including privacy and cybersecurity, vulnerabilities and threats, in line with business requirements and impact.
- Managing user identities and authorisations in a standardised manner
- Testing security regularly.

The security breaches of ransomware attack would have been mitigated had the information security management system been implemented and maintained to provide a standardised, formal and continuous approach to information security management in order to ensure that a security technology and related business processes were aligned with organisational requirements (ISACA 2018a: 139). With threats from ransomware attacks, organisations are required to be vigilant and increase security awareness to circumvent future infections and attacks through the implementation of disaster recovery and backup strategies (Valacich & Schneider 2018: 52). Alternatively, the use of a VPN assisted the organisation to maintain confidentiality of organisational data that are encrypted to unreadable form and decrypted back to original data for the recipient to consume using a decryption key (Yaokumah & Dawson 2019: 6). Implementation of e-commerce and online transactions would require the SACSSP to prevent unauthorised disclosure, alterations, and fraud (ISO 2006: 21).

The organisation adopted the consistent use of a computer network that requires a unique password and regular changing of passwords. Furthermore, in the ICT policy,

users were given the responsibility to protect their passwords. The organisation managed to submit a request to the Department of Home Affairs of South Africa and there were issues that were identified for proposed data access on 26 June 2019:

- Yearly vulnerability assessment and penetration testing were not done by a third party.
- There was no approved and implemented incident response process.
- Data to be shared through MS Excel® were not encrypted.

Management of data results are discussed in detail in the following section.

5.3.14 Managed data

The current system of filing the returned mail is unsustainable because of space limitations in the organisation. It would benefit the organisation to implement data management strategies to achieve effective management of the enterprise data assets across the data life cycle from creation to delivery, maintenance and archiving (ISACA 2018a). In future, this will assist the organisation in overcoming cost-related problems experienced with returned mail such as information technology, data collection and information sharing (Badenhorst 2013). The study uncovered that the organisation has been communicating with its stakeholders. Implementation of innovative solutions would complement and enhance the strategies already in place.

The implementation of digital certificates – electronic certification service – would dramatically speed up the documentation process, helping social service professionals to avoid the costs and delays associated with the issuing and transportation of hard copy certificates. The certificates can be verified by scanning a QR code, which would contain information that is cross-referenced with an organisation's database containing the social professional's details, such as full name, practice number and validity of the certificate (Narayanan 2012). The practice card, as depicted in Figure 4-43 in page

185, will be imprinted with a QR code to assist with verification. This can happen if data are cleansed when it is transferred between systems before any processing can take place, and the reliability of the destination system has been controlled and secured (ISO 2016). In addition, organisations have to create agile structures that would support automation and enhanced customer experiences, while supporting digital transformation initiatives are highlighted (Verhoef et al. 2021).

The social service professionals will be able to change details about their address, cell phone number and other details from a predetermined menu item (Figure 5-3).

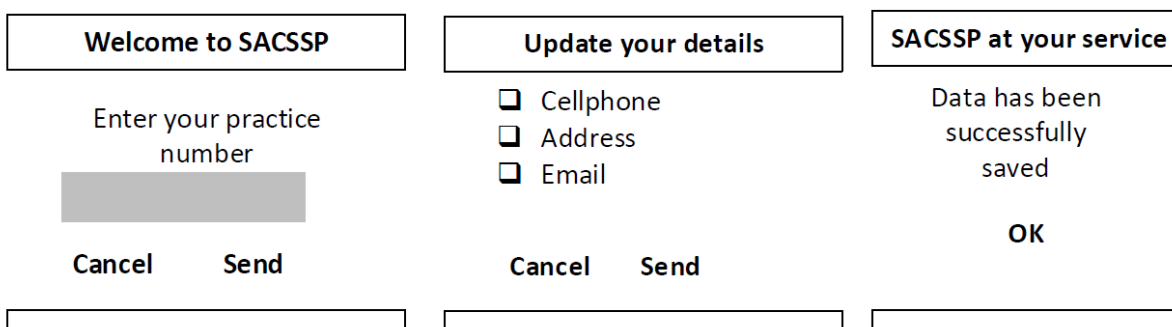


Figure 5-3: Sample of proposed phone USSD-based contacts

The implementation of USSD technology proved successful for rural health practitioners in Uganda when they migrated from paper-based reporting to USSD-based reporting, because it was possible even on entry level handsets (Nakibuuka, Semwanga & Were 2019: 164). The advantage of adopting USSD technology is that it creates a real-time connectivity to the server, which allows a two-way exchange of data for a limited time (Robertson & Jeffreys-Leach 2017: 12).

Sending of personalised QR codes to social service professionals can help to verify their credentials when needed. QR code implementation has the advantage that it is easily created and can be utilised by mobile subscribers with smartphones to update their records (Ozkaya, Ozkaya, Roxas, Bryant & Whitson 2015: 211). According to Valacich and Schneider (2018: 189), the use of QR coding can digitally transform the

organisation by enabling social service practitioners to update their contact details or verify their membership status.

5.4 BUILD ACQUIRE AND IMPLEMENT

This domain discusses 11 components of build, acquire and implement.

5.4.1 Programme management

Six participants highlighted programme management in their interview responses. COBIT 2019 advises that programme management (BAI01) should “manage all programmes for the investment portfolio in alignment with enterprise strategy and in coordinated way, based on a standard programme management approach” (ISACA 2018a: 153). Participant 4 outlined the programme management approach as per the standard BAI01 guidelines. The cost overruns were mentioned by two participants (participants 2 and 8) in managing the programmes. The portfolio of proposed service options should be documented to indicate the pipeline services in Table 5-3, catalogue services and the retired services.

Table 5-3: Proposed pipeline services

Solution identification	I&T capabilities sought
System development	System redevelopment to integrate and automate information through organisation-wide data points such as: Registration, Finance (sage ERP), ETD and Professional Conduct divisions. Information should be available to management and stakeholders through online technologies such as tablets and smartphones.
ICT server hardware	Refresh hardware in order to receive hardware maintenance from OEMs and warranty on purchased ICT hardware equipment.

Solution identification	I&T capabilities sought
Virtualised software	Technology to assist in running more than one server operating system, while sharing hardware resources. It saves hardware space, cooling and electricity.
Backup and replication solution	Creation of copies of data and transferring the copy off site to serve as insurance in the event that data in the primary site are lost or corrupted.
Server licences	Assists in bringing a technology where user computers send requests to applications that are processed in a server and displays the results on the user's computing device when the server response.
Digital phones	Upgrading of normal phones to digital phones assists users to enjoy features such as VOIP, presence (following me service routing system) and unified messaging (UM), among others.
Networking equipment	Assist in linking two or more IT hardware devices or buildings either through Ethernet wiring or wireless technology.
Employment of an IT resource	Capacity building internally
A DR site (cloud) if there is no alternative site	It offers reduced downtime in the event of disaster by giving the organisation high availability (HA).

When proposed solutions are identified, the organisational requirements need to be defined as it is a case in the succeeding section.

5.4.2 Requirements definition

The organisation embarked on defining their requirements, refining them through a benchmarking process and building a holistic process flow that was presented to the management and the board for noting and approval (ISACA 2018a: 163). Figure 4-46 on page 190, was a final integrated process plan after the inputs from all consulted

stakeholders. The benchmarking process embarked on as highlighted in section 4.7.2 on page 148, should be a regular exercise that would inform a continual improvement process that would ensure that the organisation can surpass or match its peers or competitors (Axelos 2020a: 42). Focus groups discussions were held to discuss different organisational needs, as depicted in Figures 4-18 on page 150; 4-19 on page 150; 4-20 on page 151; 4-21 on page 152; 4-22 on page 153; 4-23 on page 154; 4-24 on page 155; 4-25 on page 155; and 4-26 on page 156. Seven participants engaged in the requirements definition for the SACSSP. The COBIT 2019 framework advises the gradual design of the business process activities and workflow that need to be performed, in conjunction with the new application systems to meet the enterprise objectives, including the design of the manual control activities.

5.4.3 Solutions identification and build

The business processes and workflows were developed to be in line with the organisational needs. Due to the size of the organisation, the procurement / sourcing was done through partnering with vendors for the proposed development of the system, based on the defined development methodology (ISACA 2018a: 169). Organisations adopt different sourcing strategies based on needs, using outsourcing as part of that strategy that results in obtaining continuous specialised and technological advancement at a fraction of the price of internal skills, which can be expensive to maintain (Wild & Wild 2016: 410). Figure 4-27 in page 158 presents the server hardware solution that was ultimately procured, configured and brought into service. Other solutions that were proposed were VOIP, backup server hardware and fiber upgrade.

5.4.4 Availability and capacity management

Based on section 4.7.4 in page 159, the backup process in use did not provide a guarantee during times of disaster. The external hard drives were susceptible to

damage or loss of data. Even during the *Ink-Horse-Deal* ransomware attack, no data were recovered. COBIT BAO04, which manages availability and capacity advises that organisations need to “maintain service availability, efficiently management of resources and optimisation of system performance through prediction of future performance and capacity requirements” (ISACA 2018a: 181). The organisational backup system was operational; however, it was not adequate. System analysis reflected failed backups due to poor planning for capacity. Seven interview participants’ inputs were captured.

5.4.5 Organisational change management

The success of any change must ensure that it does not cause conflict, poor communication about the pending change, task independence on another resource or information and structural conflict caused by organisational structure, and that it gives attention to differing views based on the values or worldviews (Griffin et al. 2016: 378). Axelos (2020b: 38) advises that improvements on the OCM in which the SACSSP can be involved are:

- ensuring that people’s involvement in implementing improvement initiatives can be done effectively and efficiently
- people who are impacted by the changes that result from improvement initiatives, accept and adopt such changes.

It is further confirmed by ISACA (2018b: 34) that there should be preparation, and the organisation should commit stakeholders for business change in order to reduce the risk of failure resulting from a change.

5.4.6 IT changes management

Due to the size of the SACSSP, change management can be regarded as successful

implementation of the governance system. The board and management provided a structured and proactive approach and buy-in that was cascaded down to the operational staff of the SACSSP. This ensured that the organisation achieved success with change that was managed through the initiation of information governance champions for the implementation future systems (RSA 2014). The SACSSP included provision of training and ongoing maintenance to staff to manage changes for a period of 24 months (Valacich & Schneider 2018: 396).

5.4.7 IT change acceptance and transitioning management

Table 4-6 in page 166, outlines the preparedness of the SACSSP to safely transition from the current system in use, while anticipating the needs of the staff. One of the conditions for the winning bidder for system development was that support of the implemented integrated online system should be transitioned over a period of 24 months. The range of documentation required as part of IT changes included (Valacich & Schneider 2018: 396):

- Documentation on the configuration and deployment of the solution.
- Documenting and indexing of content in an approved format.

5.4.8 Knowledge management

The study indicated that knowledge is an expensive commodity since it captures explicit knowledge on registration information of social service professionals (Folorunso & Ogunde 2005: 34). Organisational registrations databases, manuals, staff computer files, proposals, committee meeting minutes and physical files stored are considered knowledge assets (Valacich & Schneider 2018: 282). ISACA (2018c: 39) advises on the enforcement of knowledge transfer from external experts to process owners.

5.4.9 Asset management

According to the results presented in section 4.7.9 of on page 168, assets can be managed through four lifecycle approaches:

- Planning for definition of assets;
- Procurement of assets,
- Asset maintenance, upgrade and depreciation
- Asset disposal.

Figure 5-4 depicts the asset management lifecycle.

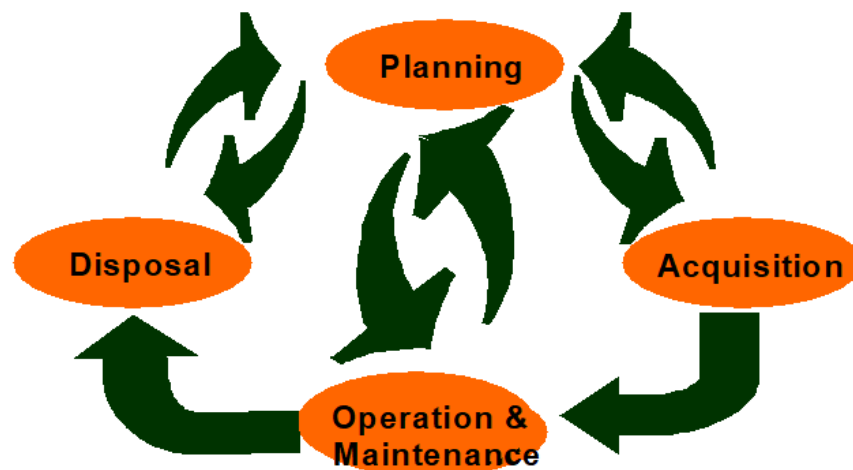


Figure 5-4: Asset lifecycle management
Source: RSA (2004: 15)

The next section, configuration management, elaborates the results as presented about the configuration of service assets in the organisation.

5.4.10 Configuration management

According to Axelos (2020c: 72), a lack of configuration of services and CIs that are reliable and available when needed, was evident when building plans were not updated to alterations done. Based on prior challenges encountered with non-documented processes, systems configurations and building plans, a new process was adopted as outlined in Table 4-7 in page 171, where the deployment, configurations and access to software licencing portals and warranties are accessible to the organisation. One document that was found to be addressing this was the ICT policy through reporting on all hardware equipment and the status of software owned by the board. “Configuration management knowledge repositories containing the versions of software and hardware components and baselines of all performing organisation standards, policies, procedures, and any project documents” (PMI 2017: 41).

Hardware server and desktop specifications were considered important in ensuring that staff have faster access to IT services. The organisation should consider the utilisation of SITA-approved specifications, as stated in transversal tender number 2003 in order to ensure uniformity and receive certified computing products. Participant 4 brings to the fore the important aspect of having SOPs that can be useful to the organisation to have consistent application processes and services.

5.4.11 Project management

The SACSSP had initiated seven projects to digitise the ICT environment and ensure that management received support to account to the board. Among these projects, cost overruns were mentioned by participants as being out of their control. Participant 1 lamented that the magnitude of these projects was huge. Participants further indicated that the implementation of these projects was progressing according to plan. The increase in scope was due to additional requirements that were required to digitise

the I&T environment and these scope changes were realised due to configuration management problems. The staff of the organisation were knowledgeable.

5.5 Deliver, service and support

This section discusses six domains: operations management, perform operational procedures, service request and incident management, problem management, continuity management, security services management and business process control management.

5.5.1 Operations management

Five operations management sub-processes perform operational procedures, manage outsourced I&T services, monitor I&T infrastructure, manage the environment, and managed facilities are discussed.

5.5.1.1 Perform operational procedures

The importance of documenting operating procedures and maintaining and performing operational procedures and operational tasks reliably and consistently was evident when the building plans of the organisation were changed through a deviation that was done without following due processes (ISACA 2018a: 232) (Figure 4-32 and Figure 4-33 in page 170). While RSA (2015c: 84) points out the limitations of an SOP, such as more restrictions, too much paperwork to go through and bureaucratic processes, properly approved operational procedures ensure quality of work for future expansions, protection of knowledge and cost-saving initiatives (QuickBooks Canada 2020). Most of the IT-related skills, knowledge and expertise of operating and drawing reports for management were outsourced, which was costly for the organisation. Such reports were charged on a time and material basis. With the advent of covid-19, internal IT

resources developed a manual to ensure that staff and board members were able to attend virtual meetings.

5.5.1.2 Managed outsourced I&T services

Outsourced services involve the management of contracts. According to Nieman (2018: 5), procurement of goods and services is regulated by:

- section 217 of Constitution of South Africa
- the Public Finance Management Act, No. 1 of 1996
- the Preferential Procurement policy Framework Act, No. 5 of 2000, and the regulations,

Purchase order issuance becomes a form of contract. The terms of a contract dictate which goods and services will be supplied over a specified period. Figure 5-5 illustrates the contract management process that the organisation intends to follow for outsourced services.

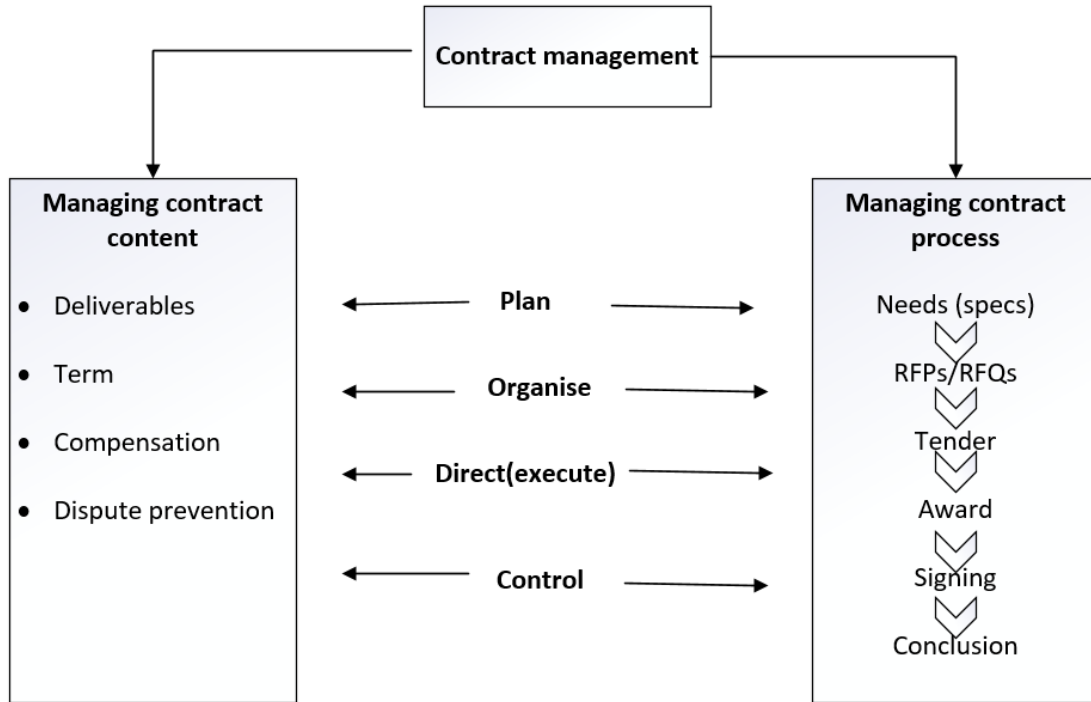


Figure 5-5: Contract management process
 Source from: (Nieman 2018: 28)

Contracted services at SACSSP had provision to be monitored and the process is discussed in the following section.

5.5.1.3 Monitor I&T infrastructure

The Telecommunication Infrastructure Standard for Data Centres (TIA-942-A) states that the data centre owner/investor and supporting team will use the TIA to ensure that the actual design of the standards is customised, approved and aligned with the expectations and requirements specified for the environment (DiMinico & Jew 2017: 5). The analysis of surveillance system revealed that there was no active monitoring of cameras. The organisation should implement a central monitoring application that helps to ensure that there are predictable performance and availability of essential applications (Tang & Todo 2013: 195). Once performance and capacity gaps are

identified based on the monitoring of current and forecasted performance, proactive plans can be made.

5.5.1.4 Manage the environment

Measures for protection against environmental factors should be maintained and the organisation should have specialised equipment and devices to monitor and control the environment (ISO 2016b: 2). Organisations should recruit experienced technical experts to carefully monitor systems and equipment, which would ensure optimal performance in the protection against downtime (Sawhney et al. 2018: 447–7). The observation by this research was that the signage was properly placed and met the minimum standards in Figure 4.36 in page 176, that is reflected by improvements to the new server room (ISACA 2018a: 232).

5.5.1.5 Manage facilities

The following measures were put in place in agreement with the organisational staff (participants):

- There must be an uninterrupted power supply (UPS) that is used to support the servers when the power goes off. The batteries for the UPS should to be replaced because they reached their lifetime.
- An air-conditioning unit supplying cold air in the server room must be set to alert the IT technicians of any problems about the temperature in the server room.
- Cables should be properly laid in the server room to correct what was observed in Figure 4-35, shows the results of the PAR from the researcher, staff, management and the board.

Figures 4-36 in page 176 and 4-37 in page 177 are a depiction of an old server room from when the researcher commenced with the study in 2018.

5.5.2 Service request and incident management

The organisation's objective is to be able to minimise disruptions while having quick resolutions to queries from users and to achieve increased productivity (ISACA 2018b: 35). The SACSSP currently does not have an IT service desk to record incidents. Valacich and Schneider (2018: 357) propose that organisations should investigate the deployment of customer engagement centres that use a variety of communication channels, such as web, face-to-face contact, video-conferencing, telephony, and virtual technology with which staff can choose to stay on the line or be called back.

5.5.3 Problem management

If an organisation has a clearly defined problem management process, it would warrant that a root cause analysis or investigation be conducted for further investigation to eliminate the occurrence of an incident and find a permanent solution for the SACSSP's IT-related calls (Kush 2013: 98). Root cause analysis ensures that workarounds being reviewed are followed by proposed fixes for the errors in order to increase quality of service provision for the benefit of the SACSSP (Axelos 2020b: 137). ISACA (2018b: 35) outlines that the process objectives involve "Increase availability, improve service levels, reduce costs, improve customer convenience and satisfaction by reducing the number of operational problems and identify root causes as part of problem resolution". In the interviews, three participants highlighted the challenges they had been suffering for an extended period.

5.5.4 Continuity management

The operational, information and data requirements of the business should inform the business continuity plan (BCP). The COBIT 2019 process manages continuity and must inform the ICT continuity policy and plan. The organisation's ICT policy clearly outlined what needed to be done during activation of a disaster that has to be applied in accordance with the "Emergency Response and Business Resumption Policy" that the organisation has adopted. Challenges identified in section 4.6.13 in page 144, brought the organisation's activities to a halt. It is important for an organisation to have complete up to date systems that can help to minimise recovery time for mission critical systems where all data are mirrored on separate servers (Valacich & Schneider 2018: 446). According to ISACA (2018b: 35), to manage continuity, the organisation needs to "adapt rapidly, continue business operations, and maintain availability of resources and information at a level acceptable to the enterprise in the event of a significant disruption..." This would require organisations to understand the impact of new implementations and integrate them into continuity and disaster recovery plans (Axelos 2020b: 119). Continuity can be achieved by housing mission critical systems in data centres equipped with high availability systems to allow continuous availability of services (Sawhney et al. 2018: 447-457).

The COBIT 2019 framework states the following on continuity management:

- Provision of infrastructure that can be an enabler for innovation, such as collaboration tools for enhancing work between geographic locations and divisions.
- Definition of business continuity policy and scope alignment with enterprise and stakeholder objectives.
- Identification of key stakeholders and roles and responsibilities for defining and agreeing on continuity policy and scope.

- Development of a business continuity plan based on the strategy that documents the procedures and information in readiness for use in an incident to enable the enterprise to continue its critical activities.

5.5.5 Security service management

The SACSSP would benefit from applying the security services management function in order to minimise the impact of operational information security vulnerabilities and incidents (ISACA 2018b: 35). The design of the data centre should have an access control system to be interfaced with the security services access system (ISACA 2018a: 257). Figure 4-44 shows the implementation of the security system that was extended to the server room. While the entry control receipt mitigated entry control, a verification process should be implemented to confirm what is written on the receipt (Sawhney et al. 2018: 447–2). Another server room layer of protection was included, as outlined in Figure 4-44, as well as the installation of a fire door to protect the new computing investment. Five participants indicated the assurance of the applied security measures employed. The only concern was raised by participant 1, who indicated that losses would occur in case of a disaster because the physical files were not secured (Zikopoulos et al. 2013: 232).

5.5.6 Business process control management

The organisation has matured business processes that were thoroughly workshopped and clarified. The streamlining of the internal processes eliminated the redundancies of various departments (Bakar et al. 2015: 132). The COBIT 2019 framework ensures that essential business processes are captured to support the related IT services (ISACA 2018a: 265). Focus groups were crucial in seeking clarity that culminated in the development of a consolidated organisational process (Figure 4-46). From the seven participants who responded to interview questions, two mentioned that the

Finance and Registration divisions' vital business processes depended on IT, while others stated that all processes were relied on to ensure an integrated online system.

5.6 MONITOR, EVALUATE AND ASSESS

The monitor domain discusses performance and conformance monitoring, internal control system, external requirements compliance and assurance management.

5.6.1 Performance and conformance monitoring

Performance and conformance monitoring included organisational auditing, including ICT audits (ISACA 2018a: 273). The internal audit is an outsourced function. What is imperative to note is that the assured conformance objective must ensure that accountable people can ascertain that service provision and service consumption comply with corporate and regulatory directives with respect to governance, risk and compliance (Axelos 2020b: 130). However, professional conduct has a defined format for complains lodged. The performance and conformance monitoring process is prescribed in the SACSSP Act and IT operations are accountable to the IT and Business Re-engineering Committee. Seven participants mentioned a wide range performance reporting, including monthly and quarterly reporting, transparency with financial reports and computer checks for suspicious activities (Aerts & Walton 2018: 439).

5.6.2 Internal control system

The SACSSP must develop the procedures for monitoring the use of information processing facilities, which would lead to the periodical review of the monitoring of organisational activities (RSA 1999: 44). Transparency is not assured to key stakeholders on the inadequacy of the internal control system in use due to the non-

submission or quality of reports (Aerts & Walton 2018: 447). Five participants communicated about internal control system challenges at the SACSSP.

5.6.3 External requirements compliance

The SACSSP was able to present and publish annual reports as prescribed ISACA (2018a: 285). Certainty is needed on the status of the SACSSP and confusion needs to be cleared. The SACSSP needs to be accountable to the DSD and report accordingly (IODSA 2016). This requirement would ensure that their activities are financially supported. Agreements between the SACSSP and the DSD need to be finalised before being presented in Parliament. It was reassuring to the SACSSP procurement processes transparency had to go through multiple levels of scrutiny before an application could move to the next level (RSA 2018:5). The initial hardware tender was re-advertised due to non-compliance in the initial bid. One interesting response was from participant 3, who highlighted that system development design happens through regulations and matters that are not in the regulations are blocked.

5.6.4 Assurance management

The SACSSP implemented the assurance management initiative even though they are not regularly conducted. IODSA (2016: 9) indicated that assurance is “the diligent application of mind to evidence, resulting in a statement or declaration concerning an identified subject matter or subject matter information, and that is made for the purpose of enhancing confidence in that subject matter or subject matter information.”

Due to the size of the organisation, audit assurance is done externally and the last audit was conducted in the 2016/17 financial year. The SACSSP Act prescribes that the organisation should “... be audited by a person registered as an accountant and auditor under the Public Accounts’ Act, 1991 (Act No. 80 of 1991), and appointed by the council”.

It was found that section 5 of the finance policy was not complied with. The root cause of audits being done was the unintegrated systems. Most of the participants raised the matter of untraceable receipts, documents and vacancies. Accountability of funds from the DSD was also a burning issue. The SACSSP understood auditing guidelines and reporting to all stakeholders (ISACA 2012: 289). The participants provided mixed responses when asked if they could obtain assurance from the SACSSP.

5.7 SUMMARY

The chapter discussed the following:

- The information governance systems at the SACSSP played an important role in the evaluation, direction and monitoring of the council's approved five-year strategy.
- Information governance planning minimally assisted in the business alignment at the SACSSP as it was done on ad hoc basis.
- The implementation of programmes and projects that support business processes was done by service providers due to limited internal ICT capabilities.
- The implemented technologies did not respond to organisational needs.
- The information governance in place provided transparency in the monitoring of performance and conformance of I&T through reporting to the management, the IT and Business Re-engineering Committee, Exco and the board.

The next chapter provides the conclusions, summaries and recommendations on how the SACSSP could implement a governance system with a view for entrenching a culture of good corporate governance.

CHAPTER SIX

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

6.1 INTRODUCTION

The previous chapter analysed and presented the results obtained from focus groups, hardware and system analysis, benchmarking exercises and open ended-interviews. Chapter five focuses on the interpretation and discussion of the results. Given (2016: 164) describes this chapter as being used by a researcher to weave the participants' voices, along with published literature, in order to give perspective to the researcher's voice. The presentation of summary of findings is based on the research objectives. Furthermore, conclusions of the study are stated and recommendations are drawn from them. The chapter will propose an information governance framework for SACSSP. This chapter covers the overall conclusions.

The results from the study indicated that information governance drove the organisational information needs and better decision-making. Planning was done in accordance with strategic objectives that assist in business alignment.

The conclusions of the research are based on the objectives of the study that were addressed in chapter 4 in sections 4.5; 4.6; 4,7; 4,8 and 4,9:

- To determine how information governance can ensure that corporate governance can play a role in the evaluation, direction and monitoring of the council's strategy.
- To review how the information governance planning can assist in business alignment at the SACSSP.
- To determine how the SACSSP can implement programmes and projects that support business processes.

- To review the outcomes of information governance and related technologies as per the planning.
- To establish how information governance can provide transparency in the monitoring of performance and conformance to drive achievement of goals.

The next section discusses the findings of the study.

6.2 SUMMARY OF FINDINGS

The summary of findings is presented in the section in alignment with research objectives. The purpose of the current research was to develop an information governance system at SACSSP, with a view to develop an information governance system with a view for entrenching a culture of good corporate governance. The IG system framework will be beneficial to other professional councils.

The critical emancipatory study involved qualitative data collected through interviews with eight participants, organisational documents, meetings and observations. The study discussed participatory action research project that involved collaboration between researchers and study participants in defining and solving the problem through needs assessment exercise that is alignment with the research methodology roadmap.

6.2.1 Evaluation, direction and monitor

The success of a governance system is through the adoption of principles, related accountability structures and practices indicated in Table 6.1. This is further demonstrated by the adoption of a mission and vision that give a clear strategic direction that is supported organisational operations.

Table 6-1: Governance system accountability, principles and practices

Structure	Principles	Practice
The board	Must ensure that a governance system achieves the political mandate	<ul style="list-style-type: none"> • Provide political leadership and strategic direction • Determine policy and provide oversight • Ensure that ICT service delivery enables the attainment of the strategic plan • Ensure that the department's organisational structure makes provision for the corporate governance of ICT • Where applicable, ensure that governance arrangements are in place for cross-sector responsibility
Head of SACSSP	<ul style="list-style-type: none"> • Must ensure that the governance system supports the department to achieve its strategic plan. • Must create an enabling environment for a governance system within prescriptive and secure context. 	<ul style="list-style-type: none"> • Provide strategic leadership and ensure alignment • Place a governance system on strategic agenda • Ensure an IT governance policy is developed and implemented • Ensure roles and responsibilities are defined and delegate authority, responsibility and accountability. • Ensure realisation of value through use of ICT • Ensure that governance and ICT capacity and capability is provided • Ensure monitoring of governance and alignment effectiveness

The governance system accountability, principles and practices would be a success if the initiatives are targeted, coordinated and executed fast enough to make an organisational vision a reality (Kotter 2014: 9).

According to ISACA (2018c: 73), the COBIT goals are cascaded to determine which governance and management objectives are relevant to achieve the priority organisations goals. The translation allows setting specific goals at every level and in every area of the organisation to support overall goals and stakeholders' requirements (ISACA 2012: 18). Strategic organisational goals and translated into actionable items that are concluded the next domain.

6.2.2 Align, plan and organise

Figure 6-1 shows a process flow of all information governance components that could assist in the alignment of ICT and business goals.

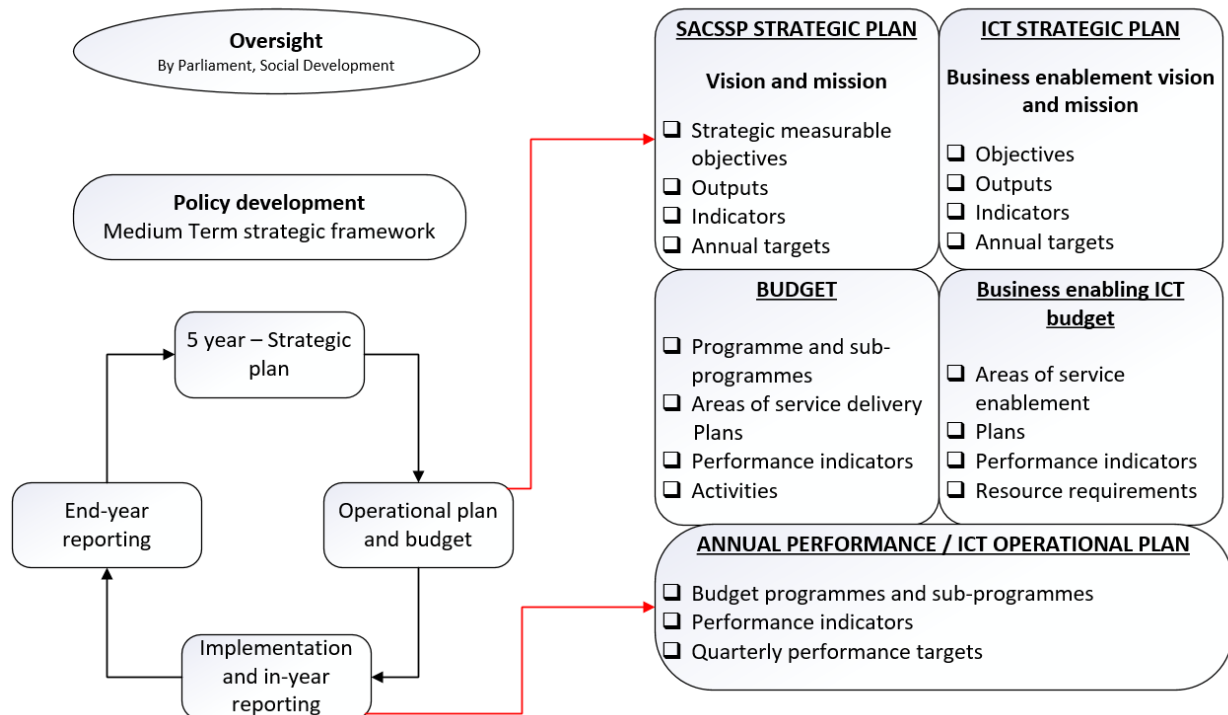


Figure 6-1: SACSSP Alignment of business and ICT
Source: (RSA 2014: 14)

Once an organisational strategic plan, operational plan and budget is approved, specific plans are designed to operationalise what needs to be achieved. The following domain brings the plans into reality.

6.2.3 Build, acquire and implement

According to Selig (2016: 62), the following factors will ensure an effective programme management culture:

- The publication of a formal governance calendar which identifies different meetings with the required status reports (weekly, bi-weekly, monthly and quarterly).
- Key roles and responsibilities should be formally agreed and communicated to all stakeholders using RACI.
- Programme / project scope, requirements and deliverables should be approved by the sponsors beforehand and the sourcing, testing, training and implementation phases should be monitored.
- Consistent programme and project metrics should be initiated based on time, cost, resources, quality and customer satisfaction. Tools can be used to quantify resource utilisation and cost estimation, among other components.
- Risk management should be used in the development of contingency plans for a high probability of occurrence and high impact.
- The establishment of the programme management office (PMO) in order to lead the project management processes, staff coordination, development and certification, management of large projects and facilitation of project plan, status reporting and reviews.

The succeeding domain brings to life the organisational plans and organisational strategy.

6.2.4 Deliver, service and support

The conclusion is based on ISACA's (2018a: 231) statement that the organisation should coordinate and execute operational procedures required to deliver internal and outsourced I&T services should include the following:

- Development and maintenance of procedures and related activities to support all organisational services
- Maintenance of a schedule of operational activities and perform such activities.
- The verification of all data expected for processing are processes completely and timeously
- Performance management of the scheduled activities
- Monitoring of incidents and problems when handling operational procedures and appropriate actions should be done to improve reliability of operational tasks performed.

Consideration of internal and external policies is concluded in the successive domain.

6.2.5 Monitor, evaluate and assess

The adoption of performance management and reporting framework (PMRF) consists of the following legislation applicable to performance planning, management and reporting:

- Public Finance Management Act, 1 of 1999 (PFMA)
- Treasury Regulations, 2005, issued in terms of the PFMA
- National Treasury practice note 4 of 2009-10
- Public Service Act, 1994 (PSA)
- Public Service Regulations, 2016 issued in terms of the PSA

- Financial Management of Parliament and Provincial Legislatures Act, 10 of 2009 (FMPPL)
- The Framework for Managing Programme Performance Information (FMPPI), issued by the National Treasury. This framework is applicable to all spheres of government.
- The Revised Framework for Strategic Plans and Annual Performance Plans (Revised FSAPP), issued in terms of the National Treasury instruction No. 10 of 2020. This framework is applicable to all national and provincial departments, constitutional institutions and those public entities listed in parts A and C of schedule 3 of the PFMA.
- Circulars and guidance issued by the National Treasury and the Department of Public Service and Administration (DPSA), Department of Cooperative Governance and Traditional Affairs (COGTA and supported by the Department of Planning Monitoring and Evaluation (DPME) regarding the planning, management, monitoring and reporting of performance against predetermined objectives.

The study presents the recommendation for the South African Council for Social Service Professions.

6.3 RECOMMENDATIONS

The following recommendations were made for a framework for information governance to support corporate governance at the South African Council for Social Service Professions.

6.3.1 Evaluation, direction and monitor

Organisations need to emphasise a holistic approach to IG that would translate into empowering a formal decision body, such as a board that would coordinate and integrate IT decision-making across the organisation and IT (De Haes, Van Grembergen, Anant & Huygh 2020: 2). The King IV code on Corporate Governance recommends to organisations to do the following (IODSA 2016: 43):

- Steer and set strategic direction
- Approve policy and planning
- Oversee and monitors
- Ensures accountability

King IV includes governance principles, each consisting of several practices such as:

“The application of governance practices would lead to governance outcomes, such as ethical culture, good performance, effective control and legitimacy.”

6.3.2 Align, plan and organise

The following are the recommendations for planning:

The organisation should manage the definition, acquisition and implementation of I&T solutions and their integration in organisational processes (ISACA 2018b: 11).

The study recommends that the revised planning, monitoring and reporting guidelines should be in place each financial year and the annual performance plan of the organisation should detail the performance indicators and targets that the organisation seeks to achieve in the upcoming financial year and during the following two years of the MTEF period. The strategic objectives, performance indicators and targets should

be aligned to each budget programme and sub-programme, where relevant, and include a quarterly breakdown of performance targets for the upcoming financial year. It is important that these performance indicators and targets should be aligned across the organisation's annual plans, budgets, and in-year and annual reports (RSA 2020d: 35).

6.3.3 Build, acquire and implement

The organisation should manage all programmes from the investment portfolio in alignment with the organisational strategy in a coordinated way (ISACA 2018a: 151). Organisations should adopt the governance framework of portfolio, programmes and projects, which should be tailored to the organisational culture, types of projects and the needs of the organisation (PMI 2017: 44).

6.3.4 Deliver, service and support

The outcome, deliver and support domain recommends the following practices (Axelos 2020c: 74):

- Incident management – provision of skills, tools and resources needed for early life support (ELS) to update support scripts and knowledge articles and to enable transition from ELS to live support.
- Problem management – documentation of all known errors and workarounds utilised.
- Service desk – the skills, tools and supporting resources needed to capture customers' details and issues when new service is released.

This domain assist in the early diagnosis of incidents and problems ensures that the performance if IT services are available to the consumers (Gërvalla, Preniqi & Kopacek 2018: 184). Furthermore, this domain ensures the problems are classified and root

causes analysed in order to effect permanent resolutions (Safwandi, Muthmainnah, Jannah & Lubis 2022: 43).

The recommendation for monitor, evaluate and assess is presented in the next section.

6.3.5 Monitor, evaluate and assess

The information governance components, such as annual report, are used to report on the financial position of the organisation, their performance against predetermined objectives and their overall governance. One of the important oversight functions of Parliament is to consider the SACSSP's annual reports. To perform this oversight function, they need assurance that the information in the annual report is credible. To this end, the annual report includes our auditor's report, which provides assurance on the credibility of the financial statements and the annual performance report, as well as on the organisation's compliance with legislation.

Such reporting and the oversight processes reflect on past events, as it takes place after the end of the financial year. However, management, the board and those charged with governance contribute throughout the year to the credibility of financial and performance information and compliance with legislation by ensuring that adequate internal controls are implemented.

6.4 PROPOSED INFORMATION GOVERNANCE SYSTEM FRAMEWORK AT THE SACSSP

The last objective was to develop an information governance framework at the SACSSP based on results and conclusions of the qualitative findings. The framework, as depicted in Figure 6.2, is a culmination of the findings presented in chapters four and five, together with the literature that was reviewed in chapter two. An IG system is

concerned with the handling of information, sourced, captured, utilised and shared either electronically or on paper.

The proposed information governance framework will assist professional organisations and board members to adopt a tailored governance system that would be designed according to their needs. The study found that there was no architectural alignment framework guiding an information governance system.

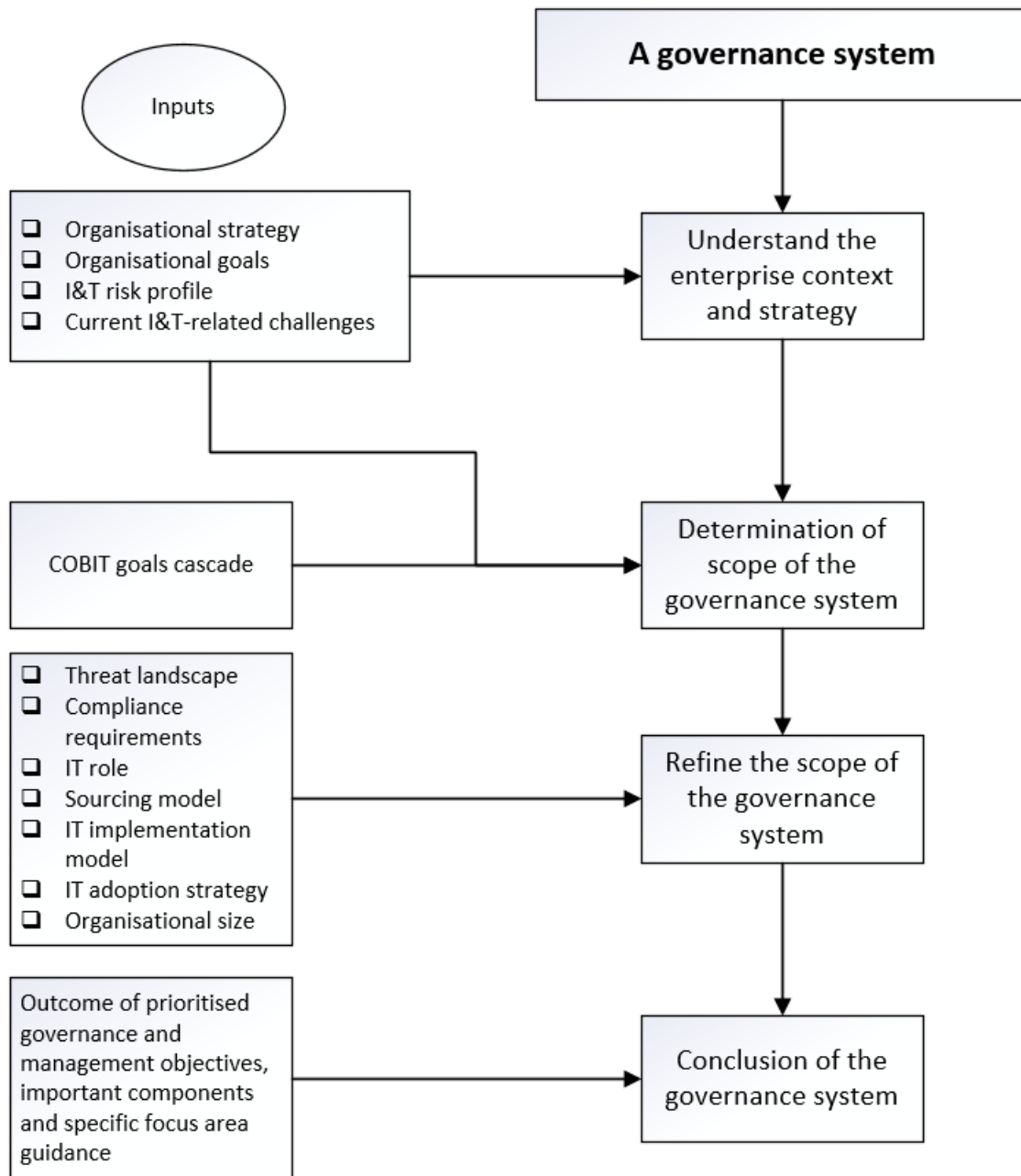


Figure 6-2: Information governance system framework

Having presented the governance framework, the next section is a description of the same framework.

6.4.1 Description of the information governance system framework

The information governance framework was based on the findings from the board and staff at the SACSSP in South Africa. The formulation of a governance system follows four design workflow stages, namely understand the enterprise strategy, determine the scope of the governance system, refine the scope of the governance system and conclude the governance system. The above results in recommendations for prioritising governance and management objectives or related governance system components, or for the adoption of specific variants of a governance system component. Other important aspects of a governance system would be the inclusion of an integrated IG framework into the corporate governance system.

6.4.1.1 Understand the enterprise context and strategy

The organisation evaluates its context, strategy and operating environment to achieve a clear understanding across four partially overlapping, interdependent and complementary domains, which are organisational strategy, organisational goals, IT risk profile and existing I&T issues.

6.4.1.2 Determination of scope of the governance system

The output of understanding the enterprise strategy provides values that are translated into a set of prioritised governance components to produce a tailored governance system for the organisation. The successful conclusion of this state will give the organisation a clear and consistent view of the organisational strategy, organisational goals, IT risk profile and current I&T issues.

6.4.1.3 Refine the scope of the governance system

This stage involves a governance system designer involved in:

- doing a walkthrough on the design factors mentioned in Table 6.2
- determining the applicability of each design factor
- determining the potential values applicable to the organisation.

Table 6-2: Design factors and explanations

Design factor	Explanation
Threat landscape	An organisation operating under either normal or high-threat environment
Compliance requirements	An organisation being subjected to either minimal, common or higher compliance requirements that are related to the industry or geopolitical conditions
Role of IT	<p>The role of IT can be classified as:</p> <ul style="list-style-type: none"> • Support – not crucial to the business • Factory – not seen as a driver for innovation • Turnaround – seen as a driver for innovation on business processes and services • Strategic – critical for running and innovation to organisation's business processes and services
Sourcing model	<p>The following sourcing model that an organisation can chose to adopt:</p> <ul style="list-style-type: none"> • Outsourcing – third party providing services to an organisation • Cloud – an organisation making use of cloud services to provide services to its cloud • Insourcing – an organisation providing resources in terms of staff and services • Hybrid – a combination of services from three sourcing models adopted
IT implementation methods	<p>IT implementation methods that the organisation can adopt:</p> <ul style="list-style-type: none"> • Agile – usage of agile development methods for the development of software

Design factor	Explanation
	<ul style="list-style-type: none"> • DevOps – it is used for software building, deployment and operations • Traditional – uses the waterfall model and separates software development and operations • Hybrid – the organisation uses a combination of traditional and modern IT implementation
Technology adoption strategy	<p>The organisation has a choice of adoption strategy to consider:</p> <ul style="list-style-type: none"> • First mover – an organisation becomes the first to adopt a new technology in order to gain advantage • Follower – the organisation waits for new technology to become mainstream before adoption • Slower adopter – an organisation delays adopting new technologies
Enterprise size	<p>An organisation with at least 50 to 250 full-time employees is considered small and medium enterprise (SME), while larger organisations have more than 250 employees</p>

The refinement of the governance scope leads to the conclusion of the governance system that is concluded in the next section.

6.4.1.4 Conclusion of the governance system

The final stage connects all inputs from the previous steps to conclude the governance system design.

6.4.2 Application of the information governance system

The application of a governance system should ensure that the implementation plan at SACSSP:

- defines standards and metrics by which success will be measured
- maps governance requirements to organisational functions and business requirements
- allocates resources to implement according to priorities and over periods of time as requirements and resources permit
- defines the schedule and components of the review process (Baret, Sandford, Hida, Vazirani & Hatfield 2013: 12).

The recommendations for future research are presented.

6.5 RECOMMENDATIONS FOR FUTURE RESEARCH

The study dealt with one of the key issues relating to the facets of information governance system. The following are possible studies to be pursued identified from the main findings of this research:

- Future studies should include social service practitioners as part of the study participants.
- Future studies could be conducted in a longitudinal study to test and account for the time-lag effects on organisational governance practices since the implementation of current interventions.
- The use of large organisations in the public and private sectors to evaluate whether the results from the current study could be extended to other settings.
- Future studies could expand the research to other African countries to evaluate the structural relationships across the professional councils, and whether the differences in organisational cultures influence the perceptions of the holistic application of information governance to support corporate governance.

Implications on the theory and practice are relayed in the next section.

6.6 IMPLICATIONS ON THEORY AND PRACTICE

The proposed framework is generic and is likely to be applicable to both theory and practice because it is not depended to prescribed technologies due to usage of open standards that can be utilised by industry and researchers. The study proposes a consideration of a theoretical support of information governance framework as opposed to incomplete frameworks. The COBIT framework should be tailored according to the organisation-specific context in order to implement the enterprise governance of I&T to support corporate governance (De Haes et al. 2020: 154). This was the case with the implementation of the COBIT 2019 framework at the SACSSP through PAR.

6.7 FINAL CONCLUSION

The study was arranged into six chapters. Chapter one gave a brief overview of the study to be undertaken. Chapter two gave the literature review of a holistic oversight over governance; planning; acquiring and implementation, system operation (run); and monitoring of tools that support corporate governance. The research methodology was presented in chapter three. The results of the study collected through observations, interviews, focus groups, systems and hardware analysis were presented in chapter four and analysed using thematic analysis. These methods were used to extract key themes in qualitative data using generally agreed principles for defining core themes in data. Atlas Ti 9 qualitative data analysis software was used because it supports a wide range of disparaged data sources.

The discussion and interpretation of the findings from the study were presented in chapter five. Chapter six presented the conclusions of all the objectives as stated in chapter one and to show that all objectives of the study have been satisfactorily responded to.

It was established in the study that having properly implemented an information governance system plays a significant role in bringing information as a valuable commodity to assist in organisations' decision-making. The I&T systems would need to include the basic building blocks, which include standards that are agreed upon to facilitate future data exchange and interoperability between the SACSSP's systems, qualification verification and population register. Governance structures (council management) from all affected stakeholders need to be set up to deal with a more holistic business, information, systems and technology architecture for the South African Council of Social Service Professions and other professional councils.

All these initiatives must be driven through the board and management buy-in in order to enforce compliance with the implementation of an IG system that creates an ability for the organisation to advance in making crucial decisions to be implemented speedily before the window of opportunity closes.

REFERENCES

- Aas, TH, Breunig, KJ & Hydle, KM. 2017. Exploring New Service Portfolio Management. *International Journal of Innovation Management*. 21(6):1–41. doi.org/10.1142/S136391961750044X.
- Abedian, I, Strachan, B & Ajam, T. 1998. *Transformation in action: Budgeting for health service delivery*. Juta and Company Ltd.
- Aerts, W & Walton, P. 2018. *Global financial accounting and reporting: principles and analysis*. Forth ed. Hampshire, UK: Cengage Learning EMEA.
- Agnew, C. 2019. *Information governance management framework*. Available from: <https://www.nottinghamshire.gov.uk/policy-library/49347/information-governance-framework> [Accessed 15 May 2019].
- Al-hawari, F & Barham, H. 2019. A machine learning based help desk system for IT service management. *Journal of King Saud University - Computer and Information Sciences*. (xxxx). doi.org/10.1016/j.jksuci.2019.04.001.
- Ali, A. 2017. Ransomware: A Research and a Personal Case Study of Dealing with this Nasty Malware. *Issues in Informing Science and Information Technology*. 14:087–099. doi.org/10.28945/3707.
- Amadi-Echendu, AP. 2016. Towards a Framework for the Intergration of Data and Data sources in the automation and dematerialisation of land administration system. *Statistical Field Theor*. 53(9):1689–1699. doi.org/10.1017/CBO9781107415324.004.
- Amin, MEK, Nørgaard, LS, Cavaco, AM, Witry, MJ, Hillman, L, Cernasev, A & Desselle, SP. 2020. doi.org/10.1016/j.sapharm.2020.02.005.
- Andrejevic, M & Selwyn, N. 2020. Facial recognition technology in schools: critical questions and concerns. *Learning, Media and Technology*. 45(2). doi.org/10.1080/17439884.2020.1686014.
- Andrew, S. 2020. *CNN: This map tracks the coronavirus in real time*. Available from:

- <https://edition.cnn.com/2020/01/29/health/coronavirus-map-real-time-tracking-trnd/index.html> [Accessed 30 January 2020].
- Ansoff, HI, Kiple, D, Lewis, AO, Helm-Stevens, R & Ansoff, R. 2019. *Implanting Strategic Management*. doi.org/10.1007/978-3-319-99599-1.
- Arolsen Archives. 2019. *Holdings concerning Nazi persecution in the online archive*. Available from: <https://arolsen-archives.org/en/search-explore/search-online-archive/> [Accessed 27 August 2019].
- Associated Press. 2020. *Photo cropping mistake leads to AP soul-searching on race*. Available from: <https://apnews.com/article/us-news-sally-buzbee-race-and-ethnicity-greta-thunberg-business-6a853a81f34164ab85713e68a889976d> [Accessed 31 March 2020].
- Australia Public Service Commission. 2019. *What is Building Digital Capability?* Available from: <https://www.apsc.gov.au/building-digital-capability> [Accessed 27 December 2019].
- Axelos. 2019. *ITIL Foundation ITIL 4 edition*. 4th ed. Norwich: The Stationary Office. Available from: <https://www.axelos.com>.
- Axelos. 2020a. *ITIL 4: Direct, Plan and Improve*. Norwich: The Stationary Office. Available from: <https://www.axelos.com>.
- Axelos. 2020b. *ITIL 4: High-velocity IT*. Norwich: The Stationary Office. Available from: <https://www.axelos.com>.
- Axelos. 2020c. *ITIL 4: Create, Deliver and Support*. Norwich: The Stationary Office. Available from: <https://www.axelos.com>.
- Axelos. 2020d. *ITIL: Drive Stakeholder Value*. Norwich: The Stationary Office. Available from: <https://www.axelos.com>.
- Badenhorst, A. 2013. A framework for prioritising practices to overcome cost-related problems in reverse logistics. *Journal of Transport and Supply Chain Management*. 7(1). doi.org/10.4102/jtscm.v7i1.113.

- Bakar, ZA, Yaacob, NA & Udin, ZM. 2015. The effect of business continuity management factors on organizational performance: A conceptual framework. *International Journal of Economics and Financial Issues*. 5.
- Baret, S, Sandford, N, Hida, E, Vazirani, J & Hatfield, S. 2013. *Developing an effective governance operating model: A guide for financial services boards and management teams*. Available from:
<https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/dttl-fsi-US-FSI-Developinganeffectivegovernance-031913.pdf>.
- Baskerville, R & Dulipovici, A. 2006. The theoretical foundations of knowledge management. *Knowledge Management Research and Practice*. 4(2).
doi.org/10.1057/palgrave.kmrp.8500090.
- Baucherel, K. 2018. *Let the Blockchain take the strain*. Available from:
https://digileaders.com/let-blockchain-take-strain/?utm_source=ActiveCampaign&utm_medium=Blog_Promo&utm_campaign=Comms&utm_content=Smart_Contracts&utm_source=Newsletter&utm_medium=email&utm_content=Is+Blockchain+a+game+changer+for+business%3F&utm_campaign [Accessed 26 December 2019].
- Becerra-Fernandez, I & Sabherwal, R. 2014. *Knowledge management: Systems and processes: Second edition*. doi.org/10.4324/9781315715117.
- Bettoni, M, Andenmatten, S & Mathieu, R. 2006. Knowledge cooperation in online communities: A duality of participation and cultivation. *Proceedings of the European Conference on Knowledge Management, ECKM*.
- Boisot, MH. 1999. *Knowledge Assets Securing Competitive Advantage in the Information Economy*. Oxford: Oxford University Press. Available from:
<http://www.oup.com>.
- Borgman, CL. 2003. *From Gutenberg to the Global Information Infrastructure: Access to Information in the Networked World*. Digital Libraries & Electronic Publishing.
- Botha, LM. 2019. Relevant internal audit skills for the future: An evaluation of current

- curricula. In: *Proceedings of the 5th International Conference on Business and Management Dynamics 2019: Pragmatic business solutions by Africa for Africa, IFRD, UAE*. M. Twum-Darko, Ed. Swakopmund. 10–23.
- Brandes, P & Wattenhofer, R. 2016. Opening the Frey/Osborne Black Box: Which Tasks of a Job are Susceptible to Computerization? Available from: <http://arxiv.org/abs/1604.08823>.
- Brown, DCG & Toze, S. 2017. Information governance in digitized public administration. *Canadian Public Administration*. 60(4):581–604. doi.org/10.1111/capa.12227.
- De Bruyn, M. 2014. The Protection Of Personal Information (POPI) Act - Impact On South Africa. *International Business & Economics Research Journal (IBER)*. 13(6):1315. doi.org/10.19030/iber.v13i6.8922.
- Bryman, A. 2016. *Social Research Methods*. Fifth ed. Oxford: Oxford University Press. Available from: <http://www.oup.com>.
- Buckl, S & Schweda, CM. 2013. A systemic view on enterprise architecture management: State-of-the-art and outline of a building block-based approach to design organization-specific enterprise architecture management functions. In: *A Systemic Perspective to Managing Complexity with Enterprise Architecture*. doi.org/10.4018/978-1-4666-4518-9.ch007.
- Caravaca, MM. 2016. Spanish legislation on records management and digital preservation. *Intepares Trust*. Available from: https://interparestrust.org/assets/public/.../EU04_20160811_FinalReport.pdf.
- Carrol, AB & Buchholtz, AK. 2015. *Business & Society Ethics, Sustainability, and Stakeholder Management*. Ninth ed. Stamford: Cengage Learning. Available from: www.cengage.com.
- Chauke, KR. 2018a. Corporate Governance Failures: Is it the End of Governance as we Know it? *The 3rd Annual International Conference on Public Administration and Development Alternatives*. (July).
- Chauke, TA. 2018b. Integration of Information Management Systems to enhance

- Business INtelligence at the Department of Transport in South Africa. University of South Africa. Available from: <https://uir.unisa.ac.za/handle/10500/25110>.
- Cohen, D. 2019. *Obama's presidential library is already digital*. Available from: <https://www.theatlantic.com/ideas/archive/2019/04/obamas-presidential-library-should-be-digital-first/586693/> [Accessed 13 June 2019].
- Commonwealth of Australia. 2013. *Digitising accumulated physical records: A guide to initiating and planning digitisation projects*. Available from: <http://www.naa.gov.au/information-management/managing-information-and-records/capturing/digitising-accumulated-records/index.aspx> [Accessed 9 October 2018].
- Creswell, JW. 2014. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. . Research design Qualitative quantitative and mixed methods approaches. *Research design Qualitative quantitative and mixed methods approaches*.
- Creswell, JW & Creswell, JD. 2018. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Fifth ed. California: SAGE Publications, Inc.
- Culot, G, Nassimbeni, G, Podrecca, M & Sartor, M. 2021. doi.org/10.1108/TQM-09-2020-0202.
- Dahir, I. 2020. *BuzzFeed News: A Ugandan Climate Activist Was Cropped Out Of A News Agency Photo of Greta Thunberg At Davos*. Available from: <https://www.buzzfeednews.com/article/ikrd/vanessa-nakate-greta-thunberg-davos> [Accessed 25 January 2020].
- DataDesign Technology Partners. 2019. *Risks Dropbox poses to your corporate data*. Available from: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&CD=20&ved=2ahUKEwixo7yivlvkAhVD6KQKHVwEAJ0QFjATegQIBRAC&url=http%253A%252F%252Fdesigndatacorp.com%252Fwp-content%252Fuploads%252F2016%252F03%252FPipeLine-Sync-7-Risks-Dropbox-Poses-to-Your-Corpo> [Accessed 17 August 2019].
- Denscombe, M. 2010. *The Good Research Guide for small-scale social research*

- projects*. forth ed. Berkshire: McGraw Hill Education. Available from:
www.openup.co.uk.
- DiMinico, C & Jew, J. 2017.
- Dube, B & Hlalele, D. 2018. Engaging critical emancipatory research as an alternative to mitigate school violence in South Africa. *Educational Research for Social Change*. 7(2):74–86. doi.org/10.17159/2221-4070/2018/v7i2a5.
- Duranti, L. 2016. InterPARES Project. 1–2.
- Ekpe, EO, Eneh, SI & Inyang, BJ. 2015. Leveraging Organizational Performance through Effective Mission Statement. *International Business Research*. 8(9). doi.org/10.5539/ibr.v8n9p135.
- Engelbrecht, M. 2021. *Social Workers' Guild declares SACSSP fee increases unfair*.
- European Union - EU. 2016. *General Data Protection Regulation*. Available from:
<https://gdpr-info.eu/>.
- Fill, H-G & Haerer, F. 2018. Knowledge Blockchains: Applying Blockchain Technologies to Enterprise Modeling. *Proceedings of the 51st Hawaii International Conference on System Sciences*. 9:4045–4054. doi.org/10.24251/hicss.2018.509.
- Fitroh, Siregar, S & Rustamaji, E. 2017. Determining evaluated domain process through problem identification using COBIT 5 framework. *2017 5th International Conference on Cyber and IT Service Management, CITSM 2017*. (August). doi.org/10.1109/CITSM.2017.8089281.
- Folorunso, O & Ogunde, AO. 2005. Data mining as a technique for knowledge management in business process redesign. *Information Management and Computer Security*. 13(4):274–280. doi.org/10.1108/09685220510614407.
- Frey, CB & Osborne, MA. 2017. The future of employment: How susceptible are jobs to computerisation? *Technological Forecasting and Social Change*. 114:254–280. doi.org/10.1016/j.techfore.2016.08.019.
- Galiev, A, Prokopyev, N, Ishmukhametov, S, Stolov, E, Latypov, R & Vlasov, I. 2019.

- Archain: A Novel Blockchain Based Archival System. In: *Proceedings of the 2nd World Conference on Smart Trends in Systems, Security and Sustainability, WorldS4 2018*. doi.org/10.1109/WorldS4.2018.8611607.
- Gallagher. 2020. *ARS Technica: London to deploy live facial recognition to find wanted faces in a crowd*. Available from: <https://arstechnica.com/information-technology/2020/01/london-to-deploy-live-facial-recognition-to-find-wanted-faces-in-crowd/> [Accessed 30 January 2020].
- Gamble, JE, Peteraf, MA & Thompson, AA. 2017. *Essentials of Strategic Management The quest for competitive advantage*. Fifth ed. New York: McGraw Hill Education. Available from: <http://www.mhhe.com>.
- Gartner. 2012. *The Importance of 'Big Data': A Definition*. Available from: <http://www.gartner.com/id=2057415> [Accessed 17 December 2019].
- Gartner, Pezzini, M, Natis, Y V, Malinverno, P, Iijima, K, Thompson, J, Thoo, E & Guttridge, K. 2017. *Magic Quadrant for Enterprise Integration Platform as a Service*.
- Georges, S. 2020. National Archives exhibit blurs images critical of President Trump. *Washington Post* (Washington). 17 January. Available from: [exhibit-blurs-images-critical-of-president-trump/2020/01/17/71d8e80c-37e3-11ea-9541-9107303481a4_story.html](https://www.washingtonpost.com/news/technology/wp/2020/01/17/71d8e80c-37e3-11ea-9541-9107303481a4_story.html).
- Gërvalla, M, Preniqi, N & Kopacek, P. 2018. IT infrastructure library (ITIL) framework approach to IT governance. *IFAC-PapersOnLine*. 51(30):181–185. doi.org/10.1016/j.ifacol.2018.11.283.
- Gill, P & Dolan, G. 2015. Originality and the PhD: What is it and how can it be demonstrated? *Nurse Researcher*. 22(6). doi.org/10.7748/nr.22.6.11.e1335.
- Given, L. 2016. *100 Questions (and Answers) About Qualitative Research*. California: SAGE Publications, Inc.
- Griffin, RW, Phillips, JM & Gully, SM. 2016. *Organizational Behavior Managing People and Organizations*. Twelfth ed. Boston: Cengage Learning. Available from:

<http://www.cengage.com>.

- Grillitsch, W, Müller-Stingl, A & Neumann, R. 2006. Sharing project knowledge: Initiation, implementation and institutionalisation. *Proceedings of the European Conference on Knowledge Management, ECKM*. (January 2007):184–191.
- Grother, P, Ngan, M & Hanaoka, K. 2019. Face Recognition Vendor Test (FVRT): Part 3, Demographic Effects. [doi.org/https://doi.org/10.6028/NIST.IR.8280](https://doi.org/10.6028/NIST.IR.8280).
- Guercio, M. 2015. EU04 – policies for recordkeeping and digital preservation: recommendations for analysis and assessment services. *InterPARES Trust*.
- Guetat, SBA & Dakhli, SBD. 2015. The Architecture Facet of Information Governance: The Case of Urbanized Information Systems. *Procedia Computer Science*. 64:1088–1098. doi.org/10.1016/j.procs.2015.08.564.
- Gwala, S. 2016. Barriers to Implementation of the (SA) National Cybersecurity Policy Framework. University of Witwatersrand. Available from: <http://wiredspace.wits.ac.za/handle/10539/23802>.
- Gwanyanya, MG. 2015. The south african companies act and the realisation of corporate human rights responsibilities. *Potchefstroom Electronic Law Journal*. 18(1). doi.org/10.4314/pelj.v18i1.05.
- De Haes, Steven; Van Grembergen, W. 2013.
- De Haes, S, Van Grembergen, W, Anant, J & Huygh, T. 2020. *Enterprise Governance of Information Technology. Achieving Alignment and Value in Digital Organizations*. Third ed. Cham: Springer.
- Hafeez, K & Alghatas, F. 2007. Knowledge management in a virtual community of practice using discourse analysis. *Electronic Journal of Knowledge Management*. 5(1):29–42.
- Han, J, Kamber, M & Pei, J. 2012. *Data Mining: Concepts and Techniques*. doi.org/10.1016/C2009-0-61819-5.
- Heim, J. 2020. *The Washington Post: National Archives exhibit blurs images critical of*

- President Trump*. Available from: https://www.washingtonpost.com/local/national-archives-exhibit-blurs-images-critical-of-president-trump/2020/01/17/71d8e80c-37e3-11ea-9541-9107303481a4_story.htm [Accessed 20 January 2020].
- Heng, GM. 2015. Business Continuity Management Planning Methodology. *International Journal of Disaster Recovery and Business Continuity*. 6. doi.org/10.14257/ijdrbc.2015.6.02.
- Hoofnagle, CJ, Sloot, B van der & Borgesius, FZ. 2019. The European Union general data protection regulation: What it is and what it means. *Information and Communications Technology Law*. 28(1). doi.org/10.1080/13600834.2019.1573501.
- Hou, CK. 2013. Measuring the impacts of the integrating information systems on decision-making performance and organisational performance: An empirical study of the Taiwan semiconductor industry. *International Journal of Technology, Policy and Management*. 13(1). doi.org/10.1504/IJTPM.2013.051007.
- Huygh, T & De Haes, S. 2018. Using the Viable System Model to Study IT Governance Dynamics: Evidence from a Single Case Study. *Proceedings of the 51st Hawaii International Conference on System Sciences*. 9. doi.org/10.24251/hicss.2018.612.
- Huzzard, T. 2021. Achieving impact: exploring the challenge of stakeholder engagement. *European Journal of Work and Organizational Psychology*. 30(3). doi.org/10.1080/1359432X.2020.1761875.
- Iles, H. 2013. Information Governance: A Brief Introduction – New Zealand Focus. (August):1–7. doi.org/10.13140/2.1.2069.1847.
- Information Governance Initiative. 2018. IGI State of the Industry Report Volume III. III:1–63. Available from: <https://iginitiative.com/download-the-state-of-information-governance-report-volume-iii-6/>.
- Information System Audit and Control Association – ISACA. 2011. *Integrating COBIT into the IT Audit Lifecycle*.

- Information System Audit and Control Association – ISACA. 2012. *A Business Framework for the Governance and Management of Enterprise IT*. Available from: <http://linkd.in/ISACAOOfficial>.
- Information System Audit and Control Association – ISACA. 2018a. *COBIT 2019 Framework: Governance and Management Objectives*. Available from: <https://www.isaca.org/resources/cobit>.
- Information System Audit and Control Association – ISACA. 2018b. *COBIT 2019 Framework: Introduction and Methodology*. doi.org/10.1007/978-981-15-7650-8_1.
- Information System Audit and Control Association – ISACA. 2018c. A Historical Timeline The COBIT Framework. 1. doi.org/10.1201/b19194-14.
- Information System Audit and Control Association – ISACA. 2018d. *COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution*.
- Information System Audit and Control Association – ISACA. 2018e. *COBIT® 2019 Designing an Information and Technology Governance Solution*.
- Information System Audit and Control Association – ISACA. 2020. *Risk IT Framework*. Second ed. Schaumburg, IL. Available from: <http://isaca.org>.
- Institute of Directors in Southern Africa - IODSA. 2009. King Code of Governance for South Africa 2009. *King Report on Governance for South Africa 2009*. 66. Available from: http://www.ngopulse.org/sites/default/files/king_code_of_governance_for_sa_2009_updated_june_2012.pdf.
- Institute of Directors in Southern Africa - IODSA. 2016. Report on corporate governance for South Africa 2016. *King IV Report on Corporate Governance for South Africa*. 71 and 87–94.
- International Standard Organization - ISO. 2006. *ISO 27001*. Geneva.
- International Standard Organization - ISO. 2013. *International Organization for*

- Standardisation and International Electrotechnical Commission, ISO/IEC, 27001.*
Geneva, Switzerland.
- International Standard Organization - ISO. 2015. ISO_IEC_11179-7_First_Draft_WD_Metadata_for_Datasets. 1–29.
- International Standard Organization - ISO. 2016a. ISO 15489-1:2016(en) Information and documentation — Records management — Part 1: Concepts and principles. 2016:15–20.
- International Standard Organization - ISO. 2016b. *Benefits of ISO 14001:2015.*
Available from: <https://www.iso.org/iso-14001-environmental-management.html>
[Accessed 29 January 2020].
- International Standard Organization - ISO. 2019. *ISO 22301:2019(en) Security and resilience — Business continuity management systems — Requirements.*
Geneva, Switzerland.
- Jalaldeen, R, Karim, NSA & Mohamed, N. 2009. Organizational readiness and its contributing factors to adopt KM processes: A conceptual model. In: *Innovation and Knowledge Management in Twin Track Economies Challenges and Solutions - Proceedings of the 11th International Business Information Management Association Conference, IBIMA 2009.* V. 1–3.
- Jansen, A & Duranti, L. 2013. The InterPARES Trust Project – Trust and digital records in an increasingly networked society. *InFuture2013: “Information Governance”.* 63–68.
- Jedynak, P. 2013. Business Continuity Management - the Perspective of Management Science. *Współczesne Zarządzanie.* 12(nr 4).
- Jingyao, S, Chandel, S, Yunnan, Y & Jingji, Z. 2020. Securing a Network : How Effective Using Firewalls and VPNs Are ? Securing a Network : How Effective Using Firewalls and VPNs Are ? (March 2019). doi.org/10.1007/978-3-030-12385-7.
- John Hopkins University. 2020. *Center for Systems Science and Engineering: 2019-nCoV Global Cases.* Available from: <https://coronavirus.jhu.edu/map.html>

[Accessed 19 July 2020].

- Kak, SF, Mustafa, FM & Valente, P. 2018. A Review of Person Recognition Based on Face Model. *Eurasian Journal of Science and Engineering*. 4(1). doi.org/10.23918/eajse.v4i1sip157.
- Karaman, E & Kurt, M. 2015. Comparison of project management methodologies: prince 2 versus PMBOK for it projects. *International Journal of Applied Sciences and Engineering Research*. 4(5). doi.org/10.6088/ijaser.04068.
- Keely, L, Walters, H, Pikkell, R & Quinn, B. 2014. *Ten Types of Innovation: The Discipline of Building Breakthroughs*. V. 57. New Jersey: John Wiley & Sons.
- Khumalo, S & Mearns, M. 2019. SharePoint as enabler for collaboration and efficient project knowledge sharing. *SA Journal of Information Management*. 21(1):1–9. doi.org/10.4102/sajim.v21i1.1044.
- von Kinsky, BR, Miller, C & Jones, A. 2016. The skills framework for the information age: Engaging stakeholders in curriculum design. *Journal of Information Systems Education*. 27(1).
- Kooper, MN, Maes, R & Lindgreen, EEOR. 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):195–200. doi.org/10.1016/j.ijinfomgt.2010.05.009.
- Kotter, JP. 2014. *8 Steps: To Accelerate change in 2015*. Available from: <http://go.kotterinc.com/get-the-8steps-ebook.htm> [Accessed 9 September 2021].
- Kotusev, S. 2019. INTRODUCTION TO THE COURSE The Practice of Enterprise Architecture : A Modern Approach to Business and IT Alignment Svyatoslav Kotusev , PhD. (June).
- Kush, P. 2013. Difficulties in Implementing Effective Problem Management. 4(8):98–100.
- Laney, C. 2020. *The Observer: Emily Roderick, Evie Price and Anna Hart, founders of the Dazzle Club, wearing makeup designed to confuse facial recognition*

- cameras. Available from:
<https://www.theguardian.com/world/2020/feb/01/privacy-campaigners-dazzle-camouflage-met-police-surveillance> [Accessed 7 March 2020].
- Lantsoght, EOL. 2018. *The A-Z of the PhD Trajectory*. Cham: Springer International Publishing AG. doi.org/10.1007/978-3-319-77425-1.
- Leedy, PD & Ormrod, JE. 2015. *Practical Research: Planning and Design*. Eleventh ed. Pearson Education Limited.
- Leedy, PD, Ormrod, JE & Johnson, LR. 2019. *Practical Research Planning and Design*. Twelfth ed. New York: Pearson Education, Inc. Available from:
<http://www.pearsoned.com>.
- Maluleka, JR. 2017. Acquisition, transfer and preservation of indigenous knowledge by traditional Healers in the limpopo province of South Africa. University of South Africa.
- Maluleka, JR & Ngoepe, M. 2018. Turning mirrors into windows: Knowledge transfer among indigenous healers in Limpopo province of South Africa. *SA Journal of Information Management*. 20(1):1–7. doi.org/10.4102/sajim.v20i1.918.
- Maluleke, S, Ngoepe, M & Marutha, NS. 2020. A Framework for Document Delivery Services in an Open Distance e-Learning Environment Library. *Journal of Interlibrary Loan, Document Delivery and Electronic Reserve*. 29(1–2). doi.org/10.1080/1072303X.2020.1850598.
- Maney, K, Hamm, S & O'Brien, J. 2011. *Making the world work better: the ideas that shaped a century and a company*. Pearson Education, Inc.
- Martincic, A & Dovey, K. 2011. Action research as a knowledge generating change methodology. *International Journal of Learning and Intellectual Capital*. 8(1). doi.org/10.1504/IJLIC.2011.037362.
- Marwala, T. 2014. *Artificial Intelligence Techniques for Rational Decision Making*.
- Marwala, T & Hurwitz, E. 2017. Efficient market hypothesis. In: *Advanced Information and Knowledge Processing*. doi.org/10.1007/978-3-319-66104-9_9.

- Matsiliza, NS. 2017. Corporate governance of the state-owned enterprises in an emerging country: Risk management and related issues. *Risk Governance and Control: Financial Markets and Institutions*. 7(3). doi.org/10.22495/rgcv7i3p4.
- McKinsey Global Institute (MGI). 2013. Disruptive technologies: Advances that will transform life, business, and the global economy. 114(1):1–176. doi.org/10.4337/9781786438256.00014.
- Mclaughlin, J. 2017. Understanding Organizational Culture Defining Organizational Culture Characteristics of Organizational Culture. Available from: [https://irp-cdn.multiscreensite.com/6e5efd05/files/uploaded/Understanding Organizational Culture %281%29.pdf](https://irp-cdn.multiscreensite.com/6e5efd05/files/uploaded/Understanding%20Organizational%20Culture%281%29.pdf).
- Mendes, C & Mira, M. 2010. Implementing the Service Catalogue Management. (November). doi.org/10.1109/QUATIC.2010.31.
- Merkus, J, Helms, R & Kusters, R. 2019. Data Governance and Information Governance : Set of Definitions in Relation to Data and Information as Part of DIKW. *In proceedings of the 21st International Conference on Enterprise Information Systems (ICES 2019)*. 2(Iceis):143–154. doi.org/10.5220/0007411901430154.
- Mhlongu, NSM, Chen, JYJ & Alkema, P. 2019. The underlying factors of a successful organisational digital transformation. *SA Journal of Information Management*. 21(1):1–10. doi.org/10.4102/sajim.v21i1.995.
- Mikalef, P, Boura, M, Lekakos, G & Krogstie, J. 2020. The role of information governance in big data analytics driven innovation. *Information and Management*. 57(7). doi.org/10.1016/j.im.2020.103361.
- Mládková, L. 2011. Knowledge Management for Knowledge Workers. *The Electronic Journal of Knowledge Management*. 9(3):248–258. Available from: <http://www.ejkm.com>.
- Moeller, RR. 2013. *Executive's guide to IT governance: improving systems processes with service management, COBIT, and ITIL*. New Jersey: John Wiley & Sons Inc.

- Mohapatra, S & Kumar, A. 2019. Developing a Framework for Adopting Artificial Intelligence. *International Journal of Computer Theory and Engineering*. 11(2):19–22. doi.org/10.7763/ijcte.2019.v11.1234.
- Mojapelo, MG. 2017. Contribution of selected chapter nine institutions to records management in the public sector in South Africa. University of South Africa.
- Morland-Austin. 2020. *Manage Business Process Controls*. Available from: <https://www.morland-austin.com/it-grc-knowledge-base/3.4.6/manage-business-process-controls> [Accessed 18 May 2020].
- Mosweu, O, Bwalya, K & Mutshewa, A. 2016. *Examining factors affecting the adoption and usage of document workflow management system (DWMS) using the UTAUT model: Case of Botswana*. V. 26. doi.org/10.1108/RMJ-03-2015-0012.
- Mosweu, T, Luthuli, L & Mosweu, O. 2019. Implications of cloud-computing services in records management in Africa: Achilles heels of the digital era? *SA Journal of Information Management*. 21(1):1–12. doi.org/10.4102/sajim.v21i1.1069.
- Motii, M & Semma, A. 2017. Towards a new approach to pooling COBIT 5 and ITIL V3 with ISO/IEC 27002 for better use of ITG in the Moroccan parliament. *International Journal of Computer Science Issues*. 14(3):49–58. doi.org/10.20943/01201703.4958.
- Motii, M & Semma, A. 2019. Esarbica journal. *SA Journal of Information Management*. 21(1):1–12. doi.org/10.1016/j.jclepro.2018.07.047.
- Mourad, EB, Malik, M, Anong, AC & Mustappa, B. 2017. Combination between Cobit 5 and ITIL V3 2011. *International Journal of Advanced Engineering Research and Science*. 1(5):41–47. doi.org/10.22161/ijaers.4.5.8.
- Mui, C. 2012. *How Kodak Failed*. Available from: <https://www.forbes.com/sites/chunkamui/2012/01/18/how-kodak-failed/#198012696f27> [Accessed 16 December 2019].
- Mullon, PA & Ngoepe, M. 2019. An integrated framework to elevate information governance to a national level in South Africa. *Records Management Journal*.

- 29(1–2):103–116. doi.org/10.1108/RMJ-09-2018-0030.
- Muro, M, Whiton, J & Maxim, R. 2019. *What jobs are affected by AI? Better-paid, better-educated workers face the most exposure.*
- Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *Artificial Life*. 23(4):552–557. doi.org/10.1162/ARTL_a_00247.
- Nakate, V. 2020. [Twitter] 24 January. Available from: https://twitter.com/vanessa_vash/status/1220936740665511936 [Accessed 25 January 2020].
- Nakibuuka, J, Semwanga, AR & Were, MC. 2019. Implementation of USSD Technology to Improve Quality of Routinely Reported Health Data in a Resource-Limited Setting. In: *Studies in Health Technology and Informatics*. V. 262. doi.org/10.3233/SHTI190042.
- Narayanan, AS. 2012. QR Codes and Security Solutions. *International Journal of Computer Science and Telecommunications*. 3(7).
- National Archives and Records Administration. 2019. *Obama Presidential digital library*. Available from: <https://www.obamalibrary.gov> [Accessed 13 June 2019].
- Nedelkoska, L & Quintini, G. 2018. Automation, skills use and training (OECD Working Paper). (202):1–125. Available from: <https://doi.org/10.1787/2e2f4eea-en>.
- Neuman, WL. 2014. *Social Research Methods: Qualitative and Quantitative Approaches*. Seventh ed. V. 30. Harlow: Pearson Education Limited. doi.org/10.2307/3211488.
- Newman, D & Logan, D. 2006. *Achieving agility: How enterprise information management overcomes information silos*. Stamford, CT: Gartner Research.
- Ngoepe, M & Ngulube, P. 2014. The need for records management in the auditing process in the public sector in south africa. *African Journal of Library Archives and Information Science*. 24(2).
- Ngulube, P. 2020. *Handbook of Research on Connecting Research Methods for*

- Ngulube, P, Ngoepe, M, Saurombe, N & Chaterera, F. 2017. TOWARDS A UNIFORM STRATEGY FOR TAKING ARCHIVES TO THE PEOPLE IN SOUTH AFRICA. 36:21.
- Nguyen, C, Sargent, J, Stockdale, R & Scheepers, H. 2014. Towards a unified framework for governance and management of information. *Proceedings of the 25th Australasian Conference on Information Systems, ACIS 2014*.
- Nicho, M. 2013. *An Information Governance Model for Information Security Management*. doi.org/10.4018/978-1-4666-2083-4.ch007.
- Nieman, G. 2018. *Contract Management An introduction*. Second ed. Pretoria: Van Schaik. Available from: www.dalro.co.za.
- Nkoane, MM. 2012. Critical emancipatory research for social justice and democratic citizenship. *Perspectives in Education*. 30(4):98–104.
- Nonaka, I & Takeuchi, H. 1995. *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. Oxford University Press.
- Omari, LA. 2016. IT Governance Evaluation: Adapting and Adopting the COBIT Framework for Public Sector Organisations. Queensland University of Technology. Available from: https://eprints.qut.edu.au/cgi/search/archive/thesis/?screen=Search&dataset=archive&title_merge=ALL&title=&creators_name_merge=ALL&creators_name=Omari&supervisors_name_merge=ALL&supervisors_name=&documents%2Fkeywords_merge=ALL&documents%2Fkeywords=&satisf.
- Osipov, VS. 2019. The rise of unemployment in the cyber economy. *Contributions to Economics*. PartF2. doi.org/10.1007/978-3-030-31566-5_11.
- Ozkaya, E, Ozkaya, HE, Roxas, J, Bryant, F & Whitson, D. 2015. Factors affecting consumer usage of QR codes. *Journal of Direct, Data and Digital Marketing Practice*. 16(3). doi.org/10.1057/dddmp.2015.18.
- Panian, Z. 2010. Some practical experiences in data governance. *World Academy of*

Science, Engineering and Technology. 38.

Patino, R. 2009. Intellectual property rights and research disclosure in the university environment: Preserving the commercialization option and optimizing market interest. *Journal of the American Association for Laboratory Animal Science*. 48(2):138–143.

Pickard, AJ. 2013. *Research Methods in Information*. Second ed. London: Facet Publishing.

Du Plessis, T & Mabunda, TT. 2016. Change management in an academic library in the knowledge economy. *SOUTH AFRICAN JOURNAL OF LIBRARIES AND INFORMATION SCIENCE*. doi.org/10.7553/82-1-1596.

Polzonetti, A & Sagratella, M. 2018. Towards a data-driven enterprise: Effects on information, governance, infrastructures and security. *IEEE International Conference on Industrial Engineering and Engineering Management*. 2017-Decem:1480–1484. doi.org/10.1109/IEEM.2017.8290139.

Poole, AH. 2016. The conceptual landscape of digital curation. *Journal of Documentation*. 72(5). doi.org/10.1108/JD-10-2015-0123.

Project Management Institute - PMI. 2017. *A guide to the project management body of knowledge (PMBOK Guide)*. Sixth ed. Newtown Square, Pennsylvania: Project Management Institute, Inc. Available from: <http://www.pmi.org>.

QuickBooks Canada. 2020. *Importance and Benefits of Standard Operating Procedures*. Available from: <https://quickbooks.intuit.com/ca/resources/business/importance-and-benefits-of-standard-operating-procedures/> [Accessed 18 May 2020].

Randolph, JJ. 2009. A Guide to Writing the Dissertation Literature Review. Practical Assessment, Research & Evaluation. *Practical Assessment, Research & Evaluation*. Vol. 14(13).

Reddy, BS., Nagaraju, SK & Salman, M. 2015. A study on optimisation of resources for multiple projects by using primavera. *Journal of Engineering Science and*

- Technology*. (February):235–248.
- Republic of South Africa - RSA. 1978. *Social Service Professions Act 110 of 1978*. V. 1978.
- Republic of South Africa - RSA. 1995. Labour Relations Act No. 66 of 1995. *Republic of South Africa Government Gazette*. 8(2–3):1–222.
doi.org/10.1017/s0047160700504181.
- Republic of South Africa - RSA. 1998. *Social Work Amendment Act No. 102 of 1998*.
- Republic of South Africa - RSA. 1999. *Public Finance Management Act No. 1 of 1999*. V. 32. South Africa.
- Republic of South Africa - RSA. 2001. National Archives and Records Service of South Africa Act. *Government Gazette*. 13(No 36 of 2001):10.
- Republic of South Africa - RSA. 2004. *Asset Management Framework*.
- Republic of South Africa - RSA. 2005. *Co-Operatives Act, 2005*. V. 482. South Africa.
- Republic of South Africa - RSA. 2006. *Children’s Act, 2005*. V. 492. Republic of South Africa.
- Republic of South Africa - RSA. 2007. *Chapter 5 of the Treasury Regulations for departments, trading entities, constitutional institutions and public entities*. V. 1999.
- Republic of South Africa - RSA. 2009.
- Republic of South Africa - RSA. 2010. *National Treasury Framework for Strategic Plans and Annual Performance Plans*. Pretoria. Available from:
<https://www.treasury.gov.za>.
- Republic of South Africa - RSA. 2011. *REGULATIONS REGARDING THE REGISTRATION OF SOCIAL AUXILIARY*. V. 19.
- Republic of South Africa - RSA. 2012. *Public Service Corporate Governance of Information and Communication Technology Policy Framework*. Pretoria. Available from: http://www.dpsa.gov.za/dpsa2g/psictm_documents.asp.

Republic of South Africa - RSA. 2013. *Protection of Personal Information Act 2013*.

South Africa. Available from:

<http://www.gov.za/documents/download.php?f=204368>

[%5Cnhttp://www.greengazette.co.za/notices/act-no-4-of-2013-protection-personal-information-act-2013_20131126-GGN-37067-00912](http://www.greengazette.co.za/notices/act-no-4-of-2013-protection-personal-information-act-2013_20131126-GGN-37067-00912).

Republic of South Africa - RSA. 2014. IMPLEMENTATION GUIDELINE FOR CORPORATE GOVERNANCE OF INFORMATION AND COMMUNICATION TECHNOLOGY Version 1. (January):1–29. Available from: www.dpsa.gov.za.

Republic of South Africa - RSA. 2015a. *Public Sector Supply chain management review*. Pretoria. Available from:

[http://www.treasury.gov.za/publications/other/SCMR REPORT 2015.pdf](http://www.treasury.gov.za/publications/other/SCMR%20REPORT%202015.pdf).

Republic of South Africa - RSA. 2015b. The National Cybersecurity Policy Framework (NCPF) For South Africa - 2015. *Government Gazette*. (39475):1–30. Available from: http://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf.

Republic of South Africa - RSA. 2015c. *Public Service Operations Management*.

Republic of South Africa - RSA. 2018. Public Audit Amendment Act 5 of 2018. 641(5). Available from:

http://www.nsw.gov.au/sites/default/files/Government_Gazette_2_December.pdf#page=15.

Republic of South Africa - RSA. 2019a. *Data governance framework*. Pretoria.

Republic of South Africa - RSA. 2019b. *Principles of good governance for co-operatives*. Available from:

https://www.gov.za/sites/default/files/gcis_document/201508/39029gon647s.pdf.

Republic of South Africa - RSA. 2019c. *2019 Estimates of National Expenditure Guidelines*.

Republic of South Africa - RSA. 2019d. *Auditor-General of South Africa: Investigation and Special Audits Regulations*. V. 110. South Africa.

Republic of South Africa - RSA. 2020a. *National Treasury: Central Supplier Database*

- for Government. Available from: <https://secure.csd.gov.za/> [Accessed 14 May 2020].
- Republic of South Africa - RSA. 2020b. *Department of Postal and Telecommunications: National Cybersecurity Hub*. Available from: <https://www.cybersecurityhub.gov.za/> [Accessed 27 February 2020].
- Republic of South Africa - RSA. 2020c. *Strategic Plan 2020-2025*.
- Republic of South Africa - RSA. 2020d. Department of planning, monitoring & evaluation: The Annexure to the revised APP 2020/21.
- Robertson, G & Jeffreys-Leach, S. 2017. *Sustainable data collection: Mobile Modes. FinMark Trust insight2impact facility*. Available from: <https://www.i2ifacility.org> [Accessed 31 July 2020].
- Safwandi, S, Muthmainnah, M, Jannah, M & Lubis, HA. 2022. Information Technology Governance Audit Using COBIT 5 of DSS Domain (Deliver , Service , And Support) Framework at Malikussaleh University Lhokseumawe. *Journal of Renewable Energy, and Computer Engineering*. 2(1):38–46. Available from: <https://doi.org/10.29103/jreece.v2i1.6633>.
- Samiotakis, M. 2013. Integrating ITIL and COBIT 5 to Optimize IT Process and Service Delivery. *6th itSMF South East Europe Conference*. 14. Available from: http://www.itsmc.gr/pdf/Michalis_Samiotakis.pdf.
- Sarno, R & Herdiyanti, A. 2010. A Service Portfolio for an Enterprise Resource Planning. *International Journal of Computer Science and Network Security*. 10(3).
- Sawhney, J, Raisinghani, M. & Idemudia, EC. 2018. Quality management in a data center: A critical perspective. *In: 49th Annual Meeting of the Decision Sciences, Chicago*.
- Selig, GJ. 2016. IT Governance-An Integrated Framework and Roadmap : How to Plan , Deploy and Sustain for Improved Effectiveness University of Bridgeport. 55–77.
- Serumaga-Zake, PAE. 2017. The role of user satisfaction in implementing a Business

- Intelligence System. *SA Journal of Information Management*. 19(1). doi.org/10.4102/sajim.v19i1.736.
- SFIA Foundation. 2019. *SFIA – What is it?* Available from: <https://www.sfia-online.org/en/framework/sfia-7/about-sfia-7#section-3> [Accessed 27 December 2019].
- Shabalala, PM. 2005. BUDGET ALLOCATION AND EXPENDITURE PATTERNS OF GOVERNMENT WITH SPECIFIC REFERENCE TO GOVERNMENT COMMUNICATION AND INFORMATION SYSTEM (GCIS) FOR THE PERIOD 1998 - 2001.
- Shibambu, A & Ngoepe, M. 2020. When rain clouds gather: Digital curation of South African public records in the cloud. *SA Journal of Information Management*. 22(1). doi.org/10.4102/sajim.v22i1.1205.
- Simoiu, C, Gates, C, Bonneau, J & Goel, S. 2019. A Study of Ransomware. *USENIX Symposium on Usable Privacy and Security (SOUPS)*. 1–16.
- Smallwood, RF. 2014. *Information Governance: Concepts, Strategies, and Best Practices*. V. 61. Hoboken, New Jersey: John Wiley and Sons.
- Soma, K, MacDonald, BH, Termeer, CJAM & Opdam, P. 2016. Introduction article: Informational governance and environmental sustainability. *Current Opinion in Environmental Sustainability*. 18:131–139. doi.org/10.1016/j.cosust.2015.09.005.
- South African Council for Social Service Professions - SACSSP. 2016a. *Audit Report*. Pretoria.
- South African Council for Social Service Professions - SACSSP. 2016b. *SACSSP Strategic Plan 2016 - 2020*.
- South African Council for Social Service Professions - SACSSP. 2018a. *About us – Mandate*. Available from: <https://www.sacssp.co.za/About> [Accessed 9 September 2018].
- South African Council for Social Service Professions - SACSSP. 2018b. *SACSSP – UNISA Partnership Exploration Meeting*. Pretoria.

- South African Council for Social Service Professions - SACSSP. 2018c.
- South African Council for Social Service Professions - SACSSP. 2019a. *Information Technology risk register*. Pretoria.
- South African Council for Social Service Professions - SACSSP. 2019b. *Policy on Continuing Professional Development (CPD) for social workers and social auxiliary workers*. Pretoria.
- Stevens, F. 2010. Frameworks for IT governance implementation. *Enterprise IT Governance, Business Value and Performance Measurement*. 1–18. doi.org/10.4018/978-1-60566-346-3.ch001.
- Stevens Institute of Technology. 2020. Guide to the Systems Engineering Body of Knowledge SEBoK 2.2. *Guide to the Systems Engineering Body of Knowledge (SEBoK)*. (May):945. Available from: <http://g2sebok.incose.org/app/mss/menu/index.cfm>.
- Stockemer, D. 2019. *Quantitative Methods for the Social Sciences*. Cham: Springer. doi.org/10.1007/978-3-319-99118-4.
- Stringer, ET. 2014. *Action research*. Forth ed. Thousand Oaks, California: SAGE Publications, Inc.
- Sun, J, Yan, J & Zhang, KZK. 2016. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*. 2(1). doi.org/10.1186/s40854-016-0040-y.
- Sunassee, NN & Sewry, DA. 2002. A Theoretical Framework for Knowledge Management Implementation. In: *SAICSIT - South African institute of computer scientists and information technologists*.
- Takeuchi, H. 1996. The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation. *Journal of International Business Studies*. 27(1):196–201. doi.org/10.1057/jibs.1996.13.
- Tama, M. 2017. 2 487 Washington D.c. Photo Mario Tama Premium High Res Photos. Available from: <https://www.gettyimages.com/photos/washington-d.c.-photo->

- mario-tama [Accessed 31 March 2020].
- Tang, X & Todo, Y. 2013. A Study of Service Desk Setup in Implementing IT Service Management in Enterprises. 2013(August):190–196.
- Tapper, J. 2020. *The Guardian: Hiding in plain sight: activists don camouflage to beat Met surveillance*. London. Available from: <https://www.theguardian.com/world/2020/feb/01/privacy-campaigners-dazzle-camouflage-met-police-surveillance> [Accessed 7 March 2020].
- Taylor, C. 2017. NetIKX July 2017 seminar on blockchain and information management. (July):1–9.
- Telesca, L, Rana, J & Ion, M. 2007. Challenges of Interoperability Issues for Enterprise Software and Applications. Available from: https://cordis.europa.eu/pub/ist/docs/ict-ent-net/eivp-create_en.pdf.
- Thabane, T & Snyman-Van Deventer, E. 2018. Pathological corporate governance deficiencies in South Africa's state-owned companies: A critical reflection. *Potchefstroom Electronic Law Journal*. 21. doi.org/10.17159/1727-3781/2018/v21i0a2345.
- The Cabinet Office. 2011a. *01 ITIL 2011 - Service Strategy.pdf*. Norwich: The Stationary Office.
- The Cabinet Office. 2011b. *02 ITIL 2011 - Service Design.pdf*. Norwich: The Stationary Office. Available from: <http://www.cabinetoffice.gov.uk>.
- The Cabinet Office. 2011c. *04 ITIL 2011 - Service Operation.pdf*. Second ed. Norwich: The Stationary Office. Available from: <http://www.cabinetoffice.co.uk>.
- The Cabinet Office. 2011d. *03 ITIL 2011 - Service Transition.pdf*. Second ed. Norwich: The Stationary Office. Available from: <http://www.cabinetoffice.co.uk>.
- The Cabinet Office. 2011e. *Continual service improvement*. Second ed. V. 0. Norwich: The Stationary Office. doi.org/10.1007/978-1-4614-3897-7_7.
- The Ohio State University. 2020. *Center For Clinical And Translational Science: Writing*

- Standard Operating Procedures*. Available from:
<https://ccts.osu.edu/content/writing-standard-operating-procedures-sops>
[Accessed 18 May 2020].
- The Open Group. 2009. *TOGAF Version 9 The Open Group Architecture Framework (TOGAF)*. V. 37. Berkshire: The Open Group.
- The Open Group. 2018. The TOGAF® Standard, Version 9.2. *The Open Group*.
- The Open Group. 2019. *Open Group Standard Open Data Format (O-DF), an Open Group Internet of Things (IoT) Standard*. Berkshire: The Open Group.
- The Star Newspaper. 2019. *Archives with data on Holocaust victims digitised and posted online*. Available from: <https://www.thestar.com.my/tech/tech-news/2019/08/25/archives-with-data-on-holocaust-victims-digitised-and-posted-online> [Accessed 27 August 2019].
- Thomas, A. 2012. Governance at South African state-owned enterprises: What do annual reports and the print media tell us? *Social Responsibility Journal*. 8(4). doi.org/10.1108/17471111211272057.
- Thompson, AA, Peteraf, MA, Gamble, JE & Strickland III, AJ. 2020. *Crafting & Executing Strategy: Concepts and Cases The quest for Competitive Advantage*. 22nd ed. New York: McGraw Hill Education.
- United States of America. 2016. *FOIA Improvement Act of 2016*. United States of America.
- University of South Africa - Unisa. 2013. Policy on research ethics. *Research Department, University of South Africa*. 1:1–26.
- Valacich, J & Schneider, C. 2018. *Information Systems Today Managing in the Digital World*. Eighth ed. Harlow: Pearson Education, Inc. Available from: <http://www.pearsonglobaleditions.com>.
- Verhoef, PC, Broekhuizen, T, Bart, Y, Bhattacharya, A, Qi Dong, J, Fabian, N & Haenlein, M. 2021. Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*. 122.

- doi.org/10.1016/j.jbusres.2019.09.022.
- Walker, PO. 2019. Chapter 8 Indigenous paradigm research. (September 2015).
doi.org/10.1007/978-3-319-18395-4.
- Walker, RS & Brown, I. 2019. Big data analytics adoption: A case study in a large South African telecommunications organisation. *SA Journal of Information Management*. 21(1):1–10. doi.org/10.4102/sajim.v21i1.1079.
- Warwickshire County Council. 2018. *Information Management Governance Framework*.
- White, GRT & Brown, K. 2016. Future Applications of Blockchain: toward a value-based society. In *INCITE Conference*. 10.
- Wild, JJ & Wild, KL. 2016. *International Business The Challenges of Globalization*. Eighth ed. Harlow: Pearson Education Limited. Available from:
<http://www.personglobaleditions.com>.
- World Economic Forum (WEF). 2018. *Towards a reskilling revolution: a future of jobs for all*. Available from: <https://www.weforum.org/reports/towards-a-reskilling-revolution>.
- Wowczko, I. 2016. Business Intelligence in Government Driven Environment. *International Journal for Infonomics*. 9(1).
doi.org/10.20533/iji.1742.4712.2016.0134.
- Yaokumah, W & Dawson, AA. 2019. Network and Data Transfer Security Management in Higher Educational Institutions. doi.org/10.4018/978-1-5225-8455-1.ch001.
- Yiua, M, Sankatb, C & Punc, K. 2013. In search of the knowledge management practices in organisations: A review. *West Indian Journal of Engineering*. 35(2).
- Zhang, D & Zhou, C. 2014. Adoption of COBIT 5 and ITIL in Small and Medium Size Enterprises in China. 00(vx):27.
- Zikopoulos, PC, DeRoos, D, Parasuraman, K, Deutsch, T, Corrigan, D & Giles, J. 2013. *Harness the Power of Big Data: The IBM Big Data Platform*. New York:

McGraw Hill.

ANNEXURE A: QUESTIONNAIRE

1. How do you get value from the use of IT? Are end users satisfied with the quality of IT service?

2. How do you manage performance of IT?

3. How can you best exploit new technology for new strategic opportunities?

4. How do you best build and structure the IT department?

5. How dependent are you on external providers? How well are outsourcing agreements being managed? How do you obtain assurance over external providers?

6. What are the (control) requirements for information?

7. Did you address all IT-related risk?

8. Are you running an efficient and resilient IT operation?

9. How do you control the cost of IT? How do you use IT resources in the most effective and efficient sourcing options?

10. Do you have enough people for IT? How do you develop and maintain the skills, and how do you manage their performance?

11. How do you get assurance over IT?

12. Is the information that you are processing well secured?

13. How do you improve business agility through a more flexible IT environment?

14. Do IT projects fail to deliver what they promised and, if so, why? Is IT standing in the way of executing the business strategy?

15. How critical is IT to sustaining the enterprise? What do you do if IT is not available?

16. What concrete vital primary business processes are dependent on IT, and what are the requirements of business processes?

17. What has been an overrun of the IT operational budgets? How often and how much do IT projects go over budget?

18. How much of the IT effort goes into fighting fires rather than into enabling business improvements?

19. Are sufficient IT resources and infrastructure available to meet required enterprise strategic objectives?

20. How long does it take to make major IT decisions?

21. Are the total IT effort and investments transparent?

22. Does IT support the enterprise in complying with regulations and service levels?
How do you know whether you are compliant with all applicable regulations?

Annexure B: Documents analysed

Doc #	Document
D1	Social Service Professions Act 110 of 1978
D2	Social Welfare Act 102 of 1998
D3	SACSSP records management policy
D4	SACSSP Strategic Plan 2016 to 2021
D5	Regulations Specialties in Social Work
D6	PBSW – CPD standards & guidelines
D7	Regulations regarding the registration of social auxiliary workers and the holding of disciplinary inquiries
D8	SACSSP departments processes
D9	AS-IS Architecture document
D10	SACSSP general notices
D11	SACSSP organogram
D12	Terms of reference of system development (part of bid document)

Doc #	Document
D13	Budget 2021
D14	Assessment and configuration proposal
D15	Hardware solution proposed
D16	2021 Annual Meeting calendar
D17	Floor plan
D18	Minutes - 9 th IT Business Reengineering Committee meeting – 17 June 2019
D19	Minutes – 12 th IT Business Reengineering Committee meeting – 29 April 2020
D20	Data verification
D21	Operational IT risk register
D22	IT and business reengineering strategy 2016 to 2021
D23	Data Protection measures
D24	Steps to connect to MS Teams

Doc #	Document
D25	Audit report
D26	IT Policy
D27	Exploratory meeting minutes
D28	Department of Social Development presentation to portfolio committee
D29	Public Finance Management Act
D30	Department of Social Development Strategic plan
D31	Privacy of Personal Information Act

Annexure C: Ethical clearance

DEPARTMENT OF INFORMATION SCIENCE ETHICS REVIEW COMMITTEE

20 May 2020

Dear Mr Tshepo Arnold Chauke

Decision:

**Ethics Approval from 20 May
2020 to 20 May 2024**

DIS Registration #: Rec-20200520

References #: 2020-DIS-0013

Name: TA Chauke

Student #: 38569043

Researcher(s): Mr Tshepo Arnold Chauke

38569043@mylife.unisa.ac.za
0732050974

Supervisor(s): Prof MS Ngoepe

nqoepms@unisa.ac.za

**A framework for information governance to support corporate
governance at the South African Council for Social Service
Professions**

Qualifications: Doctoral Study



The *low risk application* was reviewed and expedited by the Department of Information Science Research Ethics Committee on 20 May 2020 in compliance with the Unisa Policy on Research Ethics and the Standards Operating Procedure on Research Ethics Risk Assessment. The proposed research may now commence with the provisions that:

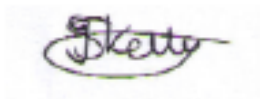
1. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy of Research Ethics.
2. Any adverse circumstances arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the Department of Information Science Ethics Review Committee.
3. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
4. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards the protection of participants' privacy and the confidentiality of the data should be reported to the Committee in writing, accompanied by a progress report.
5. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no. 4 of 2013; Children's Act no. 38 of 2005 and the National Health Act, no. 61 of 2003.
6. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
7. Research must consider rules for engagement that are in line with observing COVID 19 regulations.
8. No field work activities may continue after the expiry date of **20 May 2024**. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:

The reference number 2020-DIS-0013 should be clearly indicated on all forms of communication with the intended research participants, as well as the Committee.



Yours sincerely

A handwritten signature in black ink, appearing to read "Isabel Schellnack-Kelly". The signature is written in a cursive style with a large initial 'I' and a long horizontal stroke at the end.

Dr Isabel Schellnack-Kelly
Department of Information Science: Ethics Committee

ANNEXURE D: LETTER OF PERMISSION



SOUTH AFRICAN COUNCIL FOR SOCIAL SERVICE PROFESSIONS

Private Bag X12, Gezina, Pretoria, 0031
Tel: (012) 356 8301/21
Email: support1@sacssp.co.za
Enq: Mrs. L Malamba

37 Annie Botha Ave, Riviera, Pretoria, 0084
Fax: (086) 645 2913
Website: www.sacssp.co.za
Ref : 14/12

14 December 2020

Dr Isabel Schellnack-Kelly
Department of Information Science Ethics Review Committee
UNISA

Dear Dr. Schellnack-Kelly

RE: ENDORSEMENT OF RESEARCH PROJECT: "A FRAMEWORK FOR INFORMATION GOVERNANCE TO SUPPORT CORPORATE GOVERNANCE AT THE SOUTH AFRICAN COUNCIL FOR SOCIAL SERVICE PROFESSIONS" MR TSHEPO ARNOLD CHAUKE

Kindly note that the IT and Business Reengineering committee approved the initiation of the research project within SACSSP at a meeting held on 9 July 2018. Further support and endorsement of the research project championed by Mr Chauke was given at the meeting of Council held on the 29 and 30th November 2018. Council's administration is already reaping benefits from his involvement since 2018.

We welcome his involvement for the entire duration of his study period and look forward to having him on board until 2024.

Yours faithfully

A handwritten signature in black ink, appearing to be 'LM', is written over a horizontal line.

Ms. L Malamba
REGISTRAR

Cc: Prof Mpho Ngoepe – Study supervisor

NON NOBIS – Not for ourselves

Annexure E: Informed consent

PARTICIPANT INFORMATION SHEET

09 March 2021

Title: A holistic Information Governance system for SACSSP

Dear Participant,

My name is Tshepo Arnold Chauke and I am doing research with Prof. Mpho Ngoepe, a professor in the Department of Information Science towards a Doctor of Philosophy at the University of South Africa. We are inviting you to participate in a study entitled A holistic Information Governance system for SACSSP.

WHAT IS THE PURPOSE OF THE STUDY?

The purpose of this study is to investigate the A holistic Information Governance system for SACSSP. To ensure that this purpose is achievable, the following research objectives will be investigated:

- determine how information governance can be used for evaluation, direction and monitoring of the SACSSP's strategy by the board.
- review how the information governance planning can assist in business alignment at SACSSP.
- determine how the SACSSP can build, acquire and implement programmes and projects that support business processes.
- review the outcomes of information governance and related technologies as per the planning.

- establish how information governance can provide transparency in the monitoring of performance and conformance to drive achievement of goals by management.
- suggest an information governance framework for the SACSSP.

WHY AM I BEING INVITED TO PARTICIPATE?

Your contact details were received from the Council and you fall under the category of participants that is relevant to the study, including staff, managers and select Council members at SACSSP.

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?

The study involves open ended questions. The questions to be asked would be under the following themes outlined on the purpose of the study. The expected duration of participation will take 15 - 30 minutes and the time needed to complete specific research activities like open ended interviews would be 30 minutes.

CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?

Participating in this study is voluntary and you are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason.

WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?

The possible benefits for the participant, the organization and the scientific community would be to get better understanding on how could the integration of systems assist in enhancing business intelligence to improve decision making processes within the Department of Transport in South Africa.

ARE THERE ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?

There will not be any potential level of inconvenience and/or discomfort to the participant since they will be interviewed in their workplaces. There will not be any possible or reasonably foreseeable risks of harm or side-effects to the potential participants. There will be minimal risk that may come from others identifying the person's participation in the research since the researcher.

There is no need for indemnity or insurance coverage for participants since there will not be any harm arising from participating in the research.

WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?

Your name will not be recorded anywhere and no one will be able to connect you to the answers you give. Your answers will be given a code number or a pseudonym and you will be referred to in this way in the data, any publications, or other research reporting methods such as conference proceedings.

Your answers may be reviewed by people responsible for making sure that research is done properly, including the transcriber, external coder, and members of the Research Ethics Review Committee. Otherwise, records that identify you will be available only to

people working on the study, unless you give permission for other people to see the records.

Your anonymous data may be used for other purposes, such as a research report, journal articles and/or conference proceedings. A report of the study may be submitted for publication, but individual participants will not be identifiable in such a report.

HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?

Hard copies of your answers will be scanned and stored on a password protected computer by the researcher for a period of five years in an electronic format which will be stored for future research or academic purposes. Future use of the stored data will be subject to further Research Ethics Review and approval if applicable. The hard copies will be shredded and/or electronic copies will be permanently deleted from the hard drive of the computer through the use of Active@ KillDisk software programme.

WILL I RECEIVE PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?

The participant will not incur any costs arising from the participation of this study.

HAS THE STUDY RECEIVED ETHICS APPROVAL

This study has received written approval from the Research Ethics Review Committee of the Research Ethics Review committee, Unisa. A copy of the approval letter can be obtained from the researcher if you so wish.

HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?

If you would like to be informed of the final research findings, please contact Tshepo Arnold Chauke on +27 82 450 2673 or tel: +27 12 309 3022 or email: tshepo.chauke@gmail.com . Should you require any further information or want to contact the researcher about any aspect of this study.

Should you have concerns about the way in which the research has been conducted, you may contact Prof. Ngoepe, email: ngoepms@unisa.ac.za , phone number +27 12 429 6360 and Fax +27 12 429 3199. Alternatively, contact the research ethics chairperson of the Research Ethics Review committee, Dr. Isabel Schellnack-Kelly and contact details +27 12 429 6936, including email: schelis@unisa.ac.za

Thank you for taking time to read this information sheet and for participating in this study.
Thank you.

Tshepo Arnold Chauke

CONSENT TO PARTICIPATE IN THIS STUDY

I, _____ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname..... (please print)

Participant Signature.....Date.....

Researcher's Name & Surname **Tshepo Chauke**

Researcher's signature.....Date.....

Annexure F: Proof of qualitative analysis activities

System	Evidence of practical application
SACSSP hardware & software audit	Figure 4-31: Computing hardware analysis results
System benchmarking exercise (Two organisations visited)	Figure 4-20: Benchmarking exercise - Similar sized organisation Figure 4-21: Benchmarking notes (similar sized council one) Figure 4-22: Benchmarking – similar sized council two
Telephone and internet connectivity	Figure 4-12: Bid evaluation – networking Figure 4-13: Fiber requirements meeting
Hardware refresh	Figure 4-27: Proposed server hardware solution
SACSSP website portal	Figure 4-6: Search a register Figure 4-7: Complaints management Figure 4-9: Registration services

Annexure G: Data source verification

Data source	Type of information	Verification type
Police clearance	Fitness verification	This is to verify that an applicant does not have a criminal record under their name.
National child protection Register	Verification on suitability to work with children	This is used to check if an applicant has not been convicted for child abuse related offenses
Population register	Identity verification	This is used to verify with the population register if the identity card presented is in existence.
Training institution	Academic records	Confirmation that the academic records present at registration as a true copy
Finance system	Confirmation that all due amounts have been paid	Verification of financial details are up to date and are in sync with banking partner of Council.
Banking	Payment confirmation from social service professionals	Confirmation of amounts paid by applicants and allocation of such amounts.
Qualification accreditation	Foreign qualifications, national learner records verification, tertiary qualifications verifications	<p>An original document providing proof from the provider where the applicant received the education and training, of the content, nature and duration of the theoretical and experiential learning that were received.</p> <p>A certified copy documentary proof that the provider where the applicant received the education and training in Social Auxiliary Work is accredited, specifying the body of accreditation, or if the provider was not accredited, proof of any other form of recognition that the training provider has; and</p> <p>In the case of a provider that is accredited, a certified copy of documentary proof from the accrediting body that the qualification is or was the accepted education and training for social auxiliary work in the country concerned;</p>
Application forms	Registration details	<p>A certified copy of documentary proof of applicant's name, identity or residence permit and date of birth or age;</p> <p>A certified copy proof of the qualification on the basis of which application is being made for registration;</p> <p>An original copy of documentary proof of the provider in which an indication is given of the nature, duration and content of the course and the subjects passed or the competency of the applicant pertaining to achievement of exit level outcomes of the qualification approved by the council.</p>