CYBER GOVERNANCE IN THE WATER SECTOR

Volume 2 – Guidelines for the development of a water sector cybersecurity governance framework in South Africa

Report to the

WATER RESEARCH COMMISSION

by

WIKUS ERASMUS, MASIKE MALATJI, ANNLIZÉ L. MARNEWICK, SUNÉ VON SOLMS

University of Johannesburg

WRC Report No. 3060/2/22

ISBN 978-0-6392-0364-5

March 2023

Obtainable from
Water Research Commission
Bloukrans Building
Lynnwood Bridge Office Park
4 Daventry Road
Lynnwood Manor
PRETORIA

orders@wrc.org.za or download from www.wrc.org.za

This report forms part of a set of four reports as part of WRC project no. C2021/23-00354.

The other reports are:

Cyber Governance in the Water Sector. Volume 1: Water and sanitation cybersecurity legislative and policy environment (3060/1/22)
Cyber Governance in the Water Sector. Volume 3: Water sector cybersecurity resilience strategy and assessment (WRC Report No. 3060/3/22)
Cyber Governance in the Water Sector. Volume 4: Education and awareness guidelines (WRC Report No. 3060/4/22)

EXECUTIVE SUMMARY

BACKGROUND

A wide range of corporate information technology (IT) and operational technology cybersecurity threats and vulnerabilities in the water sector have been identified by both industry and academia. Some are associated with municipal water distribution systems that can easily be sabotaged or even damaged by means of contamination injection, cyberattack or physical destruction (Janke, Tryby & Clark, 2014). In many countries, as in South Africa, critical infrastructure (CI) owners and operators have focused largely on physical security. However, with the increased connectivity through digital technologies and communication networks, cybersecurity has become an area of increasing concern. This is also true of the water sector as utilities are increasingly using smart or connected industrial control systems (ICS) for their operational technologies.

Even though networked, and in more connected environments, smart ICS are necessary for the remote and real-time monitoring and control of physical processes essential to water treatment plants and distribution systems, cybersecurity risks are introduced. This, inevitably, increases the cyberthreat level in the utilities as also highlighted in the WRC project report TT 757/18. Thus, a cybersecurity governance framework to help mitigate and protect sector-specific cybersecurity threats is required.

RATIONALE

Cybersecurity governance refers to a structure put in place for collective steering and controlling of human interactions and cybersecurity operational procedures (Heinimann & Hatfield, 2017; Mueller, 2017; Von Solms & Von Solms, 2018). The enablers and components of a good governance system include: (i) organisational structures; (ii) people, skills, and competencies; (iii) information flows; (iv) processes; (v) policies and procedures; (vi) culture, ethics and behaviours; and (vii) services, infrastructure and applications (Information Systems Audit and Control Association, 2018). Therefore, a good cybersecurity governance structure will also comprise similar basic attributes. Moreover, it helps achieve cybersecurity resilience of CI which is essential for addressing human-made and natural adverse conditions (Jackson, 2015).

It is with this in mind that a best practice cybersecurity governance framework for South Africa's water infrastructure needs to be developed. Generally, a cybersecurity governance structure for collective steering and controlling of cybersecurity practices is put in place at strategic and tactical levels. According to Singh, Gupta and Ojha (2014), the strategic level is

policy driven, tactical level guidelines driven and operational level measures driven. In this regard, the water resources infrastructure cybersecurity governance framework needed to be developed as a strategic/tactical management guideline on how best to govern the CI cybersecurity responsibilities of the water sector of South Africa.

AIM AND OBJECTIVES

The aim of the study was to develop a CI cybersecurity governance framework for South Africa's water sector. The expected impact of the governance framework is that it should provide guidelines for the sector to effectively monitor, measure, manage and continuously improve on cyber resilience. The objectives of the study were as follows:

- Establish the cybersecurity requirements of the water sector of South Africa.
- Develop a suitable CI cybersecurity governance framework with a clear governing body, governance structure and mode.

METHODOLOGY

The methodology involved evaluating relevant knowledge sources of governance and identifying those aspects relating to cybersecurity. This resulted in governance practices being identified. These governance practices were then condensed and summarised to identify overlapping areas and categorised to develop a framework. This framework was validated against existing criteria from literature.

RESULTS AND DISCUSSION

The ultimate outcome of this report is a framework for the governance of cybersecurity within the water and sanitation sector. This framework combines best practices and guidelines from national policy as well as established governance guidelines for cybersecurity. A major contribution is further support for the recommendation of the establishment of a specific water and sanitation governing body to oversee these governance arrangements and how it will be seated within the governance realm for this sector. A possible structure is proposed in this regard.

CONCLUSIONS

It is the recommendation of this work package that the current arrangements for the governance of cybersecurity at sectoral level be formalised and updated to include the latest best practices while still adhering to national guidelines. To that end, the proposed framework for the governance of cybersecurity at sectoral level should be evaluated for adoption.

RECOMMENDATIONS FOR FUTURE RESEARCH

This work package focuses on providing a sectoral framework for the governance of cybersecurity. What could be addressed in future is how cybersecurity strategy is aligned with organisational level considerations and then at implementation level on an operational basis. This may require a sample of cybersecurity audits to be completed at various bodies to determine how well the current or proposed cybersecurity frameworks have been implemented and what the specific needs at this level appear to be for cybersecurity implementation and maintenance.

ACKNOWLEDGEMENTS

The authors would like to thank the following individuals for their input during WRC Project C2021-2023-00354.

Name	Title	Affiliation
Dr Nonhlanhla Kalebaila	Research Manager	Water Research Commission
Ms Charmaine Khanyile	Project Co-ordinator	Water Research Commission
Mr Dumisani Gubuza	Reference group member	City of Tshwane
Ms Kgaogelo Kubyana	Reference group member	eMalahleni municipality
Mr Vusi Kubheka	Reference group member	RandWater
Ms Nomazwi Mhloma	Reference group member	eThekwini Metro municipality
Mr Mluleki Mnguni	Reference group member	Umgeni Water
Mr Moloko Monyepao	Reference group member	Ekurhuleni municipality
Mr Dan Naidoo	Reference group member	Umgeni Water
Dr Kiru Pillay	Reference group member	Department of Communication and Digital Technologies
Dr Renier van Heerden	Reference group member	SANREN
Dr Brett Van Niekerk	Reference group member	Durban University of Technology

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

AG	Alignment goal
APO	Align, Plan, Organise
BAI	Build, Acquire, Implement
CAF	Cyber Assessment Framework
CGICT	Corporate Governance of Information and Communication Technology
CGICTPF	Corporate Governance of Information and Communication Technology Policy Framework
CI	Critical infrastructure
CIS	Centre for Internet Security
CMA	Catchment management agencies
COBIT	Control Objectives for Information and Related Technology
CRC	Cybersecurity Response Committee
CSIRT	Cyber Security Incidents Response Team
DSS	Deliver, Service, Support
DWS	Department of Water and Sanitation
EDM	Evaluate, Direct, Monitor
EG	Enterprise goal
EU	European Union
GDPR	General Data Protection Regulations
HR	Human resources
ICS	Industrial control systems
ICT	Information and communication technology
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Standardisation Organisation
IT	Information technology
JCPS	Justice, Crime Prevention and Security
MEA	Monitor, Evaluate, Assess
NCPF	National Cybersecurity Policy Framework
NIS	Network and Information Systems Security
NIST	National Institute of Standards and Technology
NWRIA	National Water Resources Infrastructure Agency
SA	South Africa

SALGA	South African Local Government Association
TCTA	Trans-Caledon Tunnel Authority
USA	United States of America
WP	Work package
WRC	Water Research Commission
WSA	Water services authority
WSP	Water services provider
WUA	Water user associations
WWFSA	World Wide Fund for Nature South Africa

This page was intentionally left blank

1. INTRODUCTION AND OBJECTIVES

1.1 Introduction

Governance is defined as a structure put in place to direct and control operational procedures and human interactions (Heinimann & Hatfield, 2017). The directing and controlling of operational procedures and human interactions (Heinimann & Hatfield, 2017) can be within an enterprise, among critical infrastructure (CI) sector utilities and agencies, private sector organisations, civil society and interest groups, regionally and/or globally (Amsler, 2016). Thus, cybersecurity governance refers to a structured process of collective steering and controlling of cybersecurity operational procedures and human interactions (Heinimann & Hatfield, 2017; Mueller, 2017; Von Solms & Von Solms, 2018). According to Control Objectives for Information and Related Technologies (COBIT) (Information Systems Audit and Control Association, 2018), components or enablers of a good governance system include: (i) organisational structures; (ii) people, skills and competencies; (iii) information flows; (iv) processes; (v) policies and procedures; (vi) culture, ethics and behaviours; and (vii) services, infrastructure and applications. It was the aim and objective of this study to establish best practice cybersecurity governance guidelines for the protection of South Africa's water resources cyberinfrastructure.

1.2 Project aim and objectives

The aim of the WP3 study was to develop a cybersecurity governance framework for South Africa's water resources CI. The goal was to provide CI governance processes of collective steering and controlling of tactical cybersecurity activities and human interactions in the water sector of South Africa. The study was not intended to provide the day-to-day operational cybersecurity procedures in detail, as cybersecurity controls are more business-specific and depend on factors such as the enterprise risk, industrial applications and plant operational scenarios (Ani, Daniel, Oladipo & Adewumi, 2018; Spathoulas & Katsikas, 2019; Weiss, 2014). The objectives of the study were as follows:

- Establish the cybersecurity requirements of the water sector of South Africa.
- Develop a suitable cybersecurity governance framework with a clear governing body, governance structure and mode.

1.3 Governance

What was of central importance to this work package was arriving at a working definition of governance. Governance at its foundational level serves as a steering mechanism to allow the organisation to arrive at a desired and specified outcome (Muller, 2009). This is achieved

by the implementation of various guiding practices, processes, procedures and actions that have the ability to influence the behaviour of people and systems (Bevir, 2013).

There are numerous theories of governance in literature and most can be categorised according to four dimensions (Erasmus, 2020):

- Power dimension: Power, which may or may not be vested in authority, influences the interaction of the various stakeholders in a governance system. Power can be centralised or decentralised. It is assumed in CI organisations such as water and sanitation that authority is delegated but power remains centralised in government.
- Ability to direct behaviour: Various theories state the benefits and disadvantages of behaviour being overtly directed or covertly influenced. It is assumed in this context that behaviour is more explicitly directed than influenced. This may occur on a continuum between these two points.
- Source of influence: The various governance theories establish that a governance arrangement can emerge automatically among stakeholders interacting, or be established and created by stakeholders in a system who experience an explicit need for governance arrangements. For this context it is assumed that governance arrangements are explicitly established.
- Method of steering: As needs and strategies change, so must governance arrangements. Depending on how these arrangements are implemented, these changes can be implemented via self-steering mechanisms, or can be directed. In this context, governance arrangements are assumed to be directed to change in formal forums and decision-making processes. This is, of course, influenced by the power of the stakeholders affected.

Given the assumptions above, this sector could be described by institutional governance theory.

Institutional theory states that various organisations of possibly unequal power, with their own governance arrangements, are required for decision making (Guy Peters, 2013). This would require strong policy setting and oversight to ensure that implemented polices have the desired outcome. Where the desired outcome is envisaged to be missed, corrective action ought to be taken by implementing more “correct” policy. The advantage of this view is that because institutions and stakeholders influence one another, there is a strong feedback loop that would provide greater clarity on improved policy (Alker & Biersteker, 2011).

Governance can be applied through establishing policies, practices, processes and procedures. These tools are used to influence and guide the behaviour of individuals and to

establish parameters in which organisational processes autonomously or manually perform their tasks. The types of governance practices a body wishes to implement are influenced by internal needs and external pressures. The external pressures influence the governance regime in that the body must comply with existing sectoral legislation and the sectoral environment presents strategic opportunities and threats that must be dealt with. The internal needs are defined by the governance appetite of the body and the extent to which there is a culture of compliance with governance regimes.

It is prudent to differentiate between “governance” and “management”. While management forms part of a subset of governance activities, management is not governance. Management is concerned with the allocation and coordination of resources in order to achieve specific objectives in the medium and short term (Ferreira, Mueller & Papa, 2018). Essentially, management answers the “how” question while being guided by the “what” of governance. It must also be noted that governance can be applied at multiple levels, namely a sector and an organisation.

1.4 Cybersecurity background

With the recent numerous attacks on South African cyberspace in recent months, the need for coherent response, mitigation and prevention plans is critical, especially as they relate to CI. A cybersecurity governance system is put in place usually at strategic and tactical levels. These correspond to the policy-driven and guidelines-driven levels of a system, respectively (Singh, Gupta & Ojha, 2014). The operational level, which is not the focus of this study, is usually measures/controls driven and, as stated earlier, these are unique to each organisation.

A coherent cybersecurity strategy for the sector depends primarily on the formulation of a coherent IT strategy which is based on and aligned with the overall strategy of the sector. Without this alignment, gaps will inevitably form that would only be addressed at implementation level. What is evident is that cybersecurity activities would be very similar across all sectors. What would differ from sector to sector is how these are implemented at operational level and how they would be overseen. Some of these considerations that need to be addressed are (Bruggemann, Koppatz, Scholl & Schuktomow, 2021):

- Confidentiality of user data and institutional information in line with relevant legislation
- Integrity of decision-making data
- Availability of systems for continuous service provision
- Verification of the authenticity of transmitted information and the identification of those receiving or transmitting information

- Non-repudiation assurance of the validity of the communication process to ensure that receivers and senders of information are aware of the status of communication between each other

Any cybersecurity implementation plan and strategy must address these aspects to provide sufficient and reasonable coverage as required by the sector's needs and external pressures.

1.5 Water sector context

To understand the application of the water sector cybersecurity governance framework, the national cybersecurity system and all its key role players must be understood. According to Malatji et al. (2021a) the national cybersecurity system includes the national cybersecurity legislative and policy environment. The key role players within this system include the water sector. In other words, the water sector in its entirety should be considered a stakeholder or one of the key role players within the national cybersecurity legislative and policy environment governed by the National Cybersecurity Policy Framework (NCPF). Therefore, the water sector as a system includes the water and wastewater legislative and policy environment. Currently the wastewater legislative and policy environments do not delineate any cybersecurity responsibilities of the sector whatsoever (Malatji et al., 2021a). The application of the water sector cybersecurity governance framework as discussed in this document therefore has meaning only when the sector in its entirety is considered a stakeholder within the national cybersecurity system as governed by the NCPF.

Derived from Malatji et al. (2021a), Figure 1 contextualises the different cybersecurity levels of implementation, with the sector level as the main focus of the study.

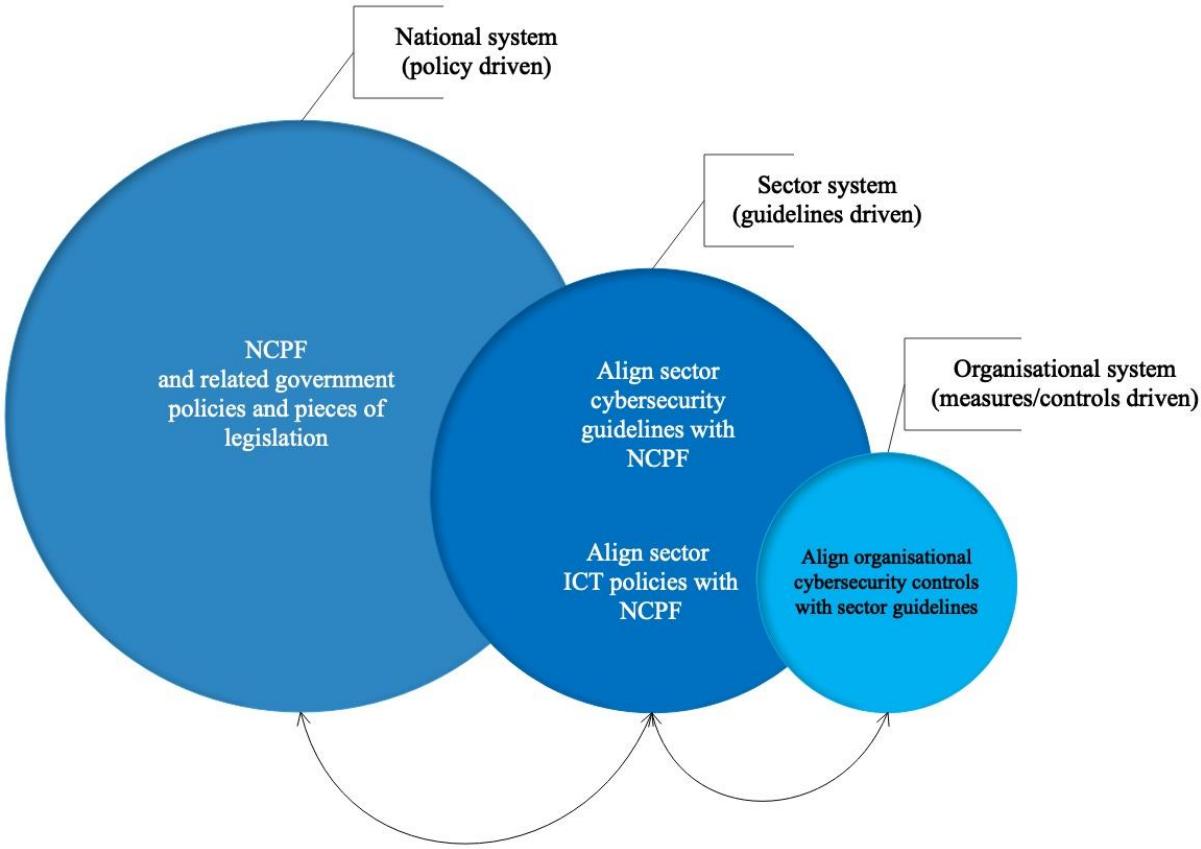

Figure 1: Cybersecurity levels of implementation

As shown in Figure 1, the national system/level of cybersecurity is anchored by the NCPF, which in turn is supported by other government policies and legislation. According to Malatji et al. (2021b), the national system of cybersecurity is the focus of the Cybersecurity Centre (located in the Ministry of State Security) and the Justice, Crime Prevention and Security (JCPS) cluster's Cybersecurity Response Committee (CRC).

As it pertains to the sector level, section 6.3.6(1-8) and section 5.3.6(i) of the NCPF provide for the establishment of a sector CSIRT in general terms with eight high-level cybersecurity responsibilities that must be confined to a specific sector (South African State Security Agency, 2015). According to Malatji et al. (2021b), these are the government policy stipulations that provide for the establishment of the water sector CSIRT. It is in this regard that this study focused mainly on the sector level to develop a suitable CI cybersecurity governance framework with a clear governing body, governance structure and mode for the water sector.

1.6 Terms of reference

This work report focuses on the strategic sectoral level of responsibility within the water and sanitation context. All practices referred to apply to this sectoral level and exclude operational

and implementation level detail for which numerous practice guides, standards and certifications already exist.

1.7 Report layout

The structure of this report is as follows:

- Chapter 1 presents the aim and objectives of this deliverable (WP3).
- In Chapter 2 the water sector cybersecurity governance framework development approach is described.
- In Chapter 3 the application of the cybersecurity governance framework is discussed as national policy basis.
- Chapter 4 deals with the process of obtaining content for the governance framework from the identified knowledge sources.
- In Chapter 5 the identified governance practices are collated, they are analysed for suitability and categorised for the establishment of the framework.
- The study concludes with Chapter 6 providing recommendations.

2. DEVELOPMENT OF THE FRAMEWORK FOR THE GOVERNANCE OF CYBERSECURITY

2.1 Introduction

The development of a framework for cybersecurity governance necessitates an unpacking of various core terms: cybersecurity, framework and governance. These foundational principles will be applied to the sector level for the South African water and sanitation function.

Cybersecurity is deemed to be a broad term that encompasses the practices, processes and activities required to safeguard electronic data resources against unauthorised access while maintaining availability and data integrity (Coronel & Morris, 2016; Craigen et al., 2014; Sarker et al., 2020). This and associated definitions have been applied in various instances among the various work packages and have been described.

A framework assists its users by providing guidelines on what to implement to achieve a desired goal or outcome (Erasmus, 2020). Therefore, a framework provides the answer to the "what" question and leaves the "how" to the practitioners in specific contexts of implementation.

These three foundational terms must be applied to the sector level. This implies a framework that must provide guidance at an overarching strategic level as it relates to governance of cybersecurity. As such, the framework will remain agnostic as it relates to the actual measures and standards at the operational levels of cybersecurity implementation and management. It is from the strategic perspective appropriate to the sector level that a coherent framework for the governance of cybersecurity is developed.

2.2 Framework development methodology

The process to develop a coherent framework in this context can be illustrated as follows:

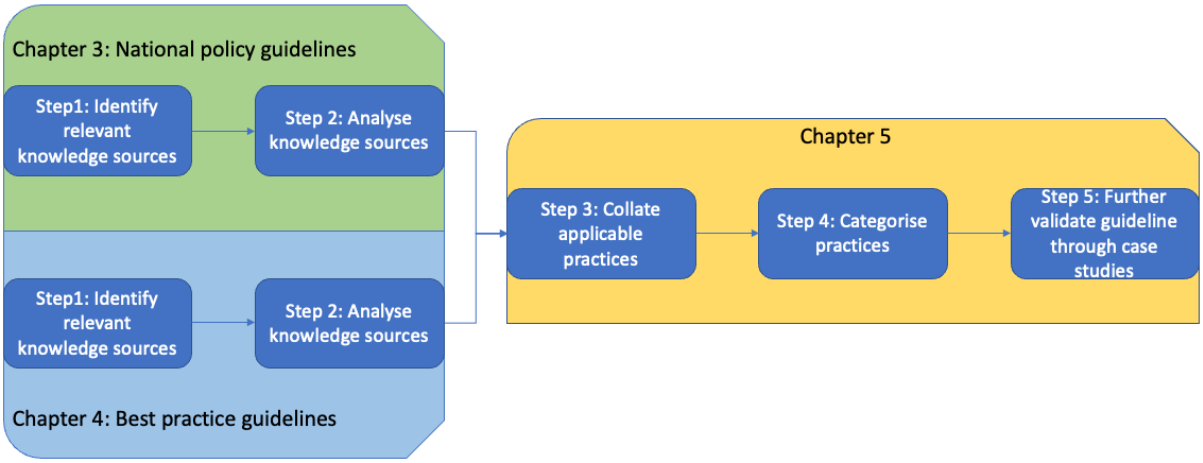

Figure 2: Framework development process

It is believed that in following this process, a comprehensive and coherent framework for the sectoral level has been derived.

Step 1 – Identify relevant knowledge sources

The content for the relevant knowledge had to relate to practices, policies and procedures for the governance of cyberpractices. In this context, the sources were limited to those that could have strategic and governance impact on the organisation at sector level.

The water and sanitation sector has many sets of regulations and national requirements that influence it. This set of knowledge sources informed the framework from the policy perspective as well is internationally recognised best practice. The identification of knowledge source for the national policy guideline perspective will occur in Chapter 3. The identification of knowledge sources from an international best practices perspective will be discussed in Chapter 4.

The framework developed in this work package consists of the practices identified in the sources of knowledge to provide a baseline. It is acknowledged that there are numerous International Standardisation Organisation (ISO) standards, guides and technical implementation guides that have a direct impact on the implementation of cybersecurity. However, these are not considered as primary sources of knowledge for a cybersecurity governance framework, especially at sectoral level, due to the high level of implementation-oriented detail and operational characteristics of these sources of knowledge.

Step 2 – Analyse knowledge sources

Applicable processes, practices and activities related to sector level governance of cybersecurity by way of relevant knowledge sources were identified. These knowledge sources were analysed to identify what aspects they contained that directly address

cybersecurity governance. This was done by searching for terms such as “information security” and “cybersecurity” to identify relevant sections in the knowledge sources identified. Each was then evaluated and analysed to determine if it was applicable in the context of a governance framework for water CI at sectoral level. These terms are sometimes used interchangeably, and it was thought important to include information security as that encompasses the area of cybersecurity. The net was cast wide in order to collect as many best practices as possible that may have existed in the knowledge sources. Chapter 3 will address this analysis from the national policy perspective whereas Chapter 4 will address the analysis from the international best practice perspective.

Step 3 – Collate applicable practices and validate

The identified and analysed governance practices were collated in preparation for establishing a governance framework in Chapter 5. Literature contains guidance on the development of frameworks. The proposed framework was mapped against guiding requirements of what constitutes a coherent framework as a validation process. COBIT 2019 provides guidance on the development of bespoke governance frameworks. The recommendation is that any governance framework in IT contexts should address the following seven components:

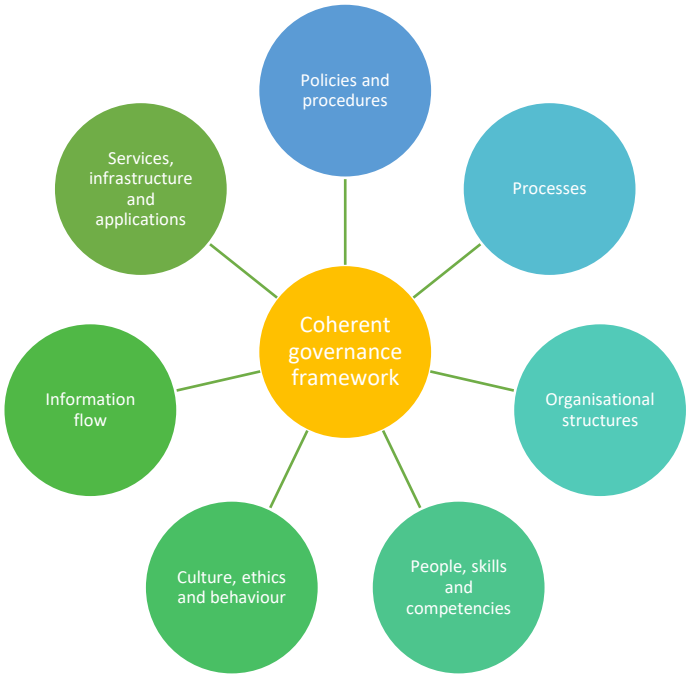

Figure 3: Seven components of governance frameworks (Information Systems Audit and Control Association, 2018)

COBIT defines each of these components as follows:

- Processes describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs that support achievement of overall IT-related goals.
- Organisational structures are the key decision-making entities in an enterprise.
- Policies and procedures translate desired behaviour into practical guidance for day-to-day management.
- Information is pervasive throughout any organisation and includes all information produced, transmitted and used by the enterprise. COBIT focuses on the information required for the effective functioning of the governance system of the enterprise through effective information flow.
- Culture, ethics and behaviour of individuals and of the enterprise are often underestimated as factors in the success of governance and management activities.
- People, skills and competencies are required for good decisions, execution of corrective action and successful completion of all activities.
- Services, infrastructure and applications include the infrastructure, technology and applications that provide the enterprise with the governance system for information and technology processing.

After the initial framework was developed as per Step 4, the mapping to the seven components of COBIT was done, reported on in Chapter 5.

If, during framework validation in Chapter 5, it is found that the collated governance practices do not address a component of the framework validation schema, the authors would have addressed these by consulting additional knowledge sources. This will serve to close off Chapter 5 and confirm a comprehensive governance framework.

Step 4 – Categorise practices

The identified practices were grouped into a set of practices to determine overlapping sections. Overlaps in the identified knowledge sources were expected and this assisted in categorising the various governance practices into coherent groupings to build the framework. This is described in Chapter 5.

Step 5 – Further validate framework through case studies and lessons learnt

The identified and collated best practices were investigated in Chapter 5 for use in case studies to determine if these are of value when they have been implemented previously. This

provided further confidence that the proposed framework will be of real-world value and practical use to the water and sanitation sector.

The following sections detail the national requirements (Chapter 3) and governance best practices (Chapter 4).

3. IDENTIFICATION AND ANALYSIS OF KNOWLEDGE SOURCES: POLICY AND NATIONAL GUIDELINES

3.1 Introduction

The water and sanitation sector has various external and internal guidelines to adhere to. All governmental sectoral bodies are required to adhere to these guidelines. These include various pieces of legislation and specifically IT policies and guiding documents. The legislative universe is excluded from this discussion, as this has been reported on in previous work packages. As for the mandated polices and guidelines, this specifically referred to the National Cybersecurity Policy Framework. This formed the main source of knowledge to inform the first leg of content for the proposed cybersecurity governance framework for the sectoral level.

3.2 NCPF as policy knowledge source

Although there is no credible central register of cyberincidents or successful attacks in South Africa, it is known that cyberattacks are also directed at CI of the country, including water and sanitation facilities. It is for this reason that the NCPF was developed. Its key objectives can be summarised in the following four principles (Malatji et al., 2021b):

- Centralise coordination of cybersecurity activities in the country.
- Facilitate the establishment of relevant structures, policy frameworks and strategies to address the national security imperative.
- Combat cybercrime.
- Enhance the information society and knowledge-based economy.

As the national cybersecurity governance framework, the NCPF outlines the cybersecurity roles and responsibilities of each key role player in the country, including the water sector. Specifically, the water sector is represented by what the NCPF (South African State Security Agency, 2015:15) refers to as the *"additional sector cybersecurity incidents response teams (CSIRTs)".* The national cybersecurity role of the water sector is therefore, as outlined in section 6.3.6(1-8), to first establish the sector CSIRT which will be charged with the following responsibilities:

- Be a point of contact for the sector-specific cybersecurity matters.
- Coordinate cybersecurity incident response activities within the sector.
- Facilitate information and technology sharing within the sector.
- Facilitate information sharing and technology exchange with other sector CSIRTs.
- Establish national security standards and best practices for the sector in consultation with the Cybersecurity Centre (located in the Ministry of State Security) and the JCPS CRC

that are consistent with guidelines, standards and best practices developed in line with the NCPF.

- Develop agreed upon measures for the sector.
- Conduct cybersecurity audits, assessments and readiness exercises for the sector.
- Provide sector entities with best practice guidance on ICT security.

Section 5.3.6(i) of the NCPF (South African State Security Agency, 2015:16) states, *"promote and provide guidance to the process of the development and implementation of establishment of sector, regional and continental CSIRTs".* Moreover, section 6.3.6 (South African State Security Agency, 2015:18) states, *"encourage and facilitate the development of appropriate additional sector CSIRTs".* Thus, the water CSIRT must be established within the guidelines, standards and best practices of the NCPF through interaction and in conjunction with the Cybersecurity Hub located in the Department of Communications and Digital Technologies. As section 7(e) of the NCPF (South African State Security Agency, 2015:6) indicates, this policy was developed for the *"coordination of the promotion of cybersecurity measures by all role players (State, public, private sector, and civil society and special interest groups) in relation to cybersecurity threats, through interaction with and in conjunction with the Cybersecurity Hub".*

The following summary lists governance practices that must be addressed in establishing such a governing body:

Table 1: NCPF as policy knowledge source

Source	No.	Governance practice
NCPF	1.1	The governing body should govern technology and information in a way that supports the organisation setting and achieving its strategic objectives
	1.2	Roles and responsibilities for critical infrastructure
	1.3	Direction setting policy approval
	1.4	Management delegation
	1.5	Ongoing oversight of the results of cybersecurity initiatives

These main governance practices form part of the proposed governance framework for cybersecurity and were analysed to determine overlaps with best practice. It must be noted that there is a strong emphasis even in these practices that a governing or controlling body is required to be responsible for the practices in the sector.

4. IDENTIFICATION AND ANALYSIS OF KNOWLEDGE SOURCES: BEST PRACTICE GUIDELINES

The main knowledge sources provided insight and guidance as to what would be included in the proposed governance framework. Each was analysed to determine the best practices that could be incorporated into this proposed framework as they related to the governance of cybersecurity.

4.1 CGICTPF

This general ICT policy issued by the South African government provides some guidance to government sectors on addressing cybersecurity concerns; however, it is based on older standards. Government structures are expected to implement this guidance. The framework contains content referenced in the South African Local Government Association (SALGA) ICT guidelines, which are also based on these older standards and guidelines. This policy identifies security as one of the essential pillars in the House of Values. It also espouses various outcomes as a direct result of the good governance of ICT as a whole. There are numerous specific outcomes that relate directly to the governance of cybersecurity (South African Department of Human Settlements, 2012):

- Outcome 2 – A long and healthy life for all: This objective is obviously impossible without access to clean water.
- Outcome 3 – All people in SA are safe and feel safe: It is hard to imagine that South African citizens could feel safe if their water and sanitation services are under threat.
- Outcome 8 – Sustainable human settlements and improved quality of household life: Clean water and efficient sanitation are primary in achieving this outcome.
- Outcome 10 – Protect and enhance our environmental assets and natural resources: Water is arguably South Africa's most valuable natural resource in everyday life.
- Outcome 12 – An efficient, effective and development-oriented public service and empowered, fair and inclusive ownership: This outcome speaks directly to how well the water and sanitation sector needs to be governed in order to achieve all other outcomes.

Outcome 12 has a direct bearing on the governance of cybersecurity in that it sets the direction and the mandate for requiring effective cybersecurity measures in the sector. It specifically references the bodies required to defend these resources and requires them to be effective and efficient. This requirement will have to have metrics attached to it to monitor whether the public body responsible in the water and sanitation sector is in fact efficient and effective. It

was therefore important to ensure that Outcome 12 was explicitly referred to in the cybersecurity governance framework as a direction-setting policy.

Outcomes 2, 3, 8 and 10 also raise the notion of water resources to be protected. However, the language contained in them refers rather to various supporting activities outside of the use of IT and cybersecurity measures. As such, these can be considered to support the entire endeavour of the governance of cybersecurity, but they do not directly impact their understanding. Therefore, these four outcomes were not explicitly included in the sectoral framework for cybersecurity governance.

The CGICTPF (South African Department of Human Settlements, 2012) leans heavily on the ISO27000 Information Technology series of international standards which provide operational level best practices. Some of these can contribute to a governance perspective in cybersecurity. A principle is espoused that the heads of departments are responsible for the corporate governance of ICT. That would imply that the heads of departments are also responsible for the governance and implementation of cybersecurity and for contributing to achieving the above outcomes. Therefore, executive management is to ensure that:

- An information security strategy is approved
- Intellectual property in information systems is appropriately protected
- ICT assets, privacy, security and the personal information of employees are managed effectively

Executive management is to appoint practitioners tasked with the implementation and management of cybersecurity and to monitor its effectiveness, which is the greater governance concern. Executive management, rightfully being concerned about strategic aspects of the organisations, is to ensure that these implemented tasks are always in alignment with the approved information security strategy. This strategy must be informed by the overarching IT strategy, which is in turn informed by the sector strategy.

This translates to an environment being created for the governance of the ICT environment as mandated by the so-called Phase 1 of the CGICT policy plan. As it relates to the governance of cybersecurity, it requires management to be active in aligning the departmental information security strategy, IT security plan and ICT security policy in a series of stages. This alignment, once achieved, must be maintained even after the implementation of projects that affect the enterprise architecture. The way that these various policies, strategies and plans are to link up is demonstrated in the figure below:

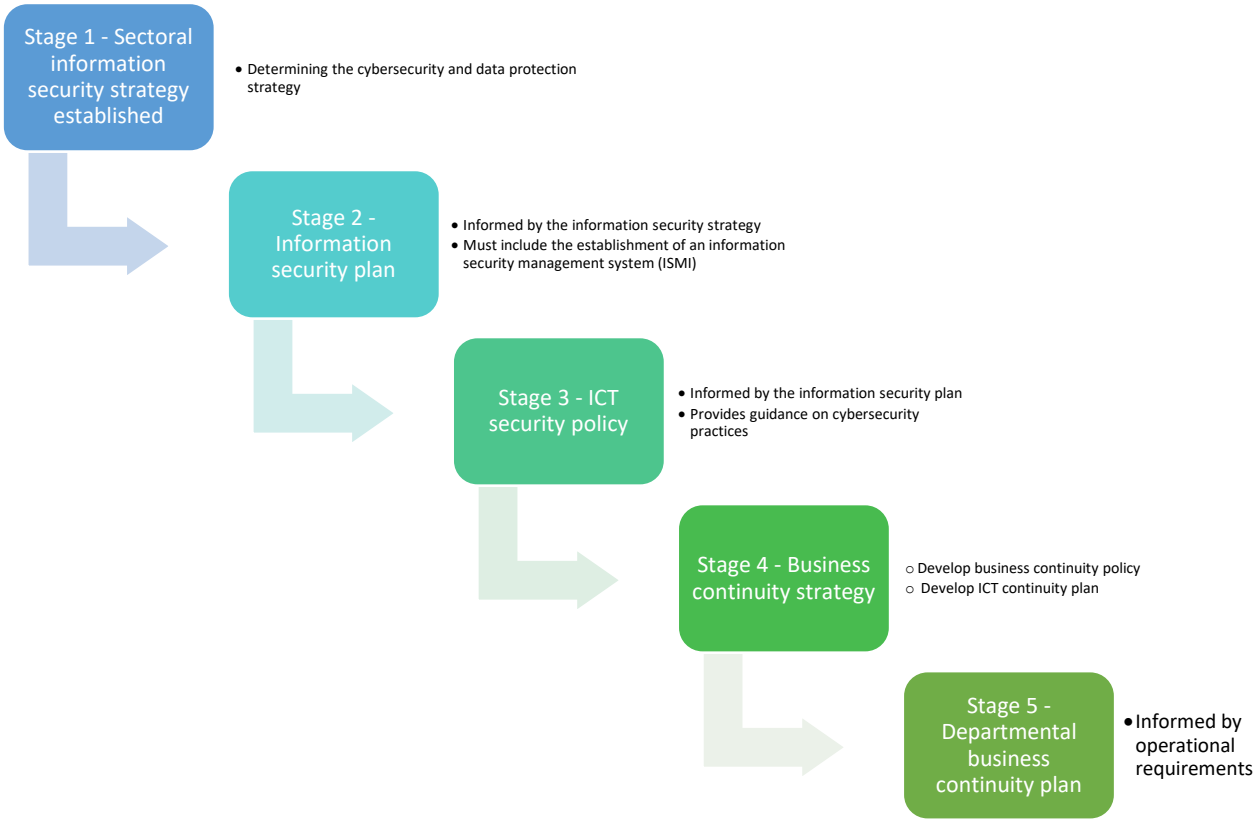

Figure 4: CGICT governance alignment

This approach is consistent with the best practices recommended by ISO38500: Standard for Corporate Governance of IT and espoused under principle 6 of the CGICTPF. This principle recommends that boards and executives establish bodies and processes for the development of the above plans and policies. As such, these bodies require the following for the establishment of proper cybersecurity governance:

- Stage 1 – A coherent information security strategy must include a strategy for data protection and cybersecurity.
- Stage 2 – An information security plan must include cybersecurity, mandate the establishment of an ISMI and be aligned with the information security strategy as described in Stage 1.
- Stage 3 – An ICT security policy must provide guidance to sectoral bodies on what needs to be implemented to have effective and efficient cybersecurity processes in place. This must align with Stage 2.
- Stage 4 – A business continuity strategy must be developed to provide guidelines on the objectives for restoring services and arrangements for ensuring that business can continue to a specified extent. This must translate into an ICT continuity plan based on Stage 3 considerations.

- Stage 5 – Each organisational unit or department must then develop its own business continuity plan as required by its own operational requirements and objectives. This is an implementation level consideration and as such will only be mandated by the sectoral level and created by the implementation or organisational level.

These five stages represent elements that must be aligned in order to achieve a coherent response to cybersecurity threats. This should address the metrics of "an efficient and effective" public service as it relates to cybersecurity objectives for the sectoral level. It is therefore proposed that these elements of the CGICTPF be included as a dimension of the proposed framework for the governance of cybersecurity:

Table 2: CGICT policy governance practices

Source	No.	Governance practice
CGICT policy	2.1	Establish cybersecurity strategy based on the sectoral IT security strategy
	2.2	Develop a cybersecurity plan that includes the development and oversight of an information security management system (ISMS) for the sector
	2.3	Develop a coherent cybersecurity policy to provide guidance for the sector
	2.4	Develop the sectoral ICT continuity strategy based on the sectoral business continuity strategy

The critical assumption is that the sector has already developed and tested a coherent IT strategy upon which the entire notion of cybersecurity is based. Without this IT strategy, which must already be in place and which is based on the overall sectoral strategy, any attempt at strategising around cybersecurity will result in incoherent and disjointed responses to cybersecurity issues.

The CGICTPF provides sounds guidance on the bodies that need to be implemented to address cybersecurity concerns and informed the proposed governance framework on that basis. As this dimension refers to corporate governance as an important element for policy setting, it was prudent to establish what the prevailing corporate governance code could contribute to the governance of cybersecurity. The next section turns to the King IV Report on Corporate Governance.

4.2 King IV

The fourth King Report on Corporate Governance provides numerous principles and guidance on various governance functional areas (Institute of Directors Southern Africa, 2016). Of greater focus in the latest iteration is the governance of IT in the organisation, specifically cybersecurity. The latest iteration of this report, published in 2016, has given greater guidance on ICT matters and information security in particular. The aim of implementing these recommendations is to achieve good governance. The Corporate Governance of Information

and Communication Technology Policy Framework (CGICTPF) refers to a previous iteration of the King reports in the form of King III. An opportunity for updating to latest best practices is available in this area. The most applicable governing principle in King IV as it relates to the governance of cybersecurity is Principle 12.

Principle 12 recommends that an established governing body govern technology and information in a way that supports the organisation setting and achieving its strategic objectives. This strongly implies a strategic alignment between organisational strategy and IT strategy. This should filter down to all the necessary information security strategies and plans mentioned under the CGICTPF in the previous section. Under this principle there are six applicable and recommended sets of governance practices:

1. The governing body should assume responsibility for the governance of technology and information by setting the direction for how technology and information should be approached and addressed in the organisation.
2. The governing body should approve policy that articulates and gives effect to its set direction on the employment of technology and information.
3. The governing body should delegate to management the responsibility to implement and execute effective technology and information management.
4. The governing body should exercise ongoing oversight of technology and information management to effect the following:
    - 4.1 Integration of technology and information risks into organisation-wide risk management
    - 4.2 Business resilience
    - 4.3 Proactive monitoring of intelligence to identify and respond to incidents, including cyberattacks and adverse social media events
    - 4.4 The responsible disposal of obsolete technology and information in a way that has regard to the environment and cybersecurity
    - 4.5 Ethical and responsible use of technology
    - 4.6 Compliance with relevant laws
    - 4.7 Information architecture supports confidentiality, integrity and availability of information
    - 4.8 Protection of personal information
    - 4.9 Continual monitoring of security of information

These practices were included and categorised in a corporate governance dimension of the proposed framework as follows:

Table 3: King IV governance practices

Category	No.	Governance practice
King IV Code on Corporate Governance	3.1	The governing body must assume responsibility for the governance of technology through coherent strategy
	3.2	The governing body must approve policy to support direction setting
	3.3	The governing body must delegate responsibility to management to implement and execute effective management
	3.4	The governing body must oversee technology management to ensure the following:
	3.4.1	Integrate IT risks into enterprise-wide risk management
	3.4.2	Arrange for business resilience
	3.4.3	Proactively monitor intelligence to identify and respond to cyberthreats
	3.4.4	Dispose of obsolete technology responsibly to ensure that cybersecurity is not threatened
	3.4.5	Ensure that technology and information are used responsibly and ethically
	3.4.6	Comply with relevant laws
	3.4.7	Ensure that the information architecture supports confidentially and availability of information
	3.4.8	Ensure the protection of personal information
	3.4.9	Ensure continuous monitoring of the security of information

4.3 COBIT 2019

The CGICT policy is based on the previous COBIT 5 edition published in 2012. As many foundational principles may be similar, COBIT 2019 presents an opportunity for a significant update. The updated version of COBIT 2019 provides greater alignment with global focus areas as it pertains to risk management and security standards, frameworks and protocols. As such, this knowledge source was uniquely positioned to provide great insight into crafting a bespoke governance framework for cybersecurity (Information Systems Audit and Control Association, 2018).

COBIT consists of various governance and management objectives made up of underlying components that help achieve the objectives. These objectives are:

- Governance objective
    - Evaluate, Direct, Monitor (EDM)
- Management objectives
    - Align, Plan, Organise (APO)
    - Build, Acquire, Implement (BAI)
    - Deliver, Service, Support (DSS)
    - Monitor, Evaluate, Assess (MEA)

For the creation of a governance framework for the sector, the EDM objectives form a necessary part of such a framework as they relate directly to the strategic perspective of an organisation. The APO management objectives relate to the managerial concerns and practices at organisational level. The same can be said for MEA management objectives as they relate to monitoring implementation and operational aspects of cybersecurity. BAI and DSS control objectives relate far more closely to the detailed implementation-type tasks. As such, the primary governance framework focuses on the EDM governance objectives.

Each of the above management and governance objectives is supported by numerous control objectives. To identify the relevant control objectives for this framework, enterprise goals (EGs) had to be identified from which to derive alignment goals (AGs). The applicable control objectives could then be derived from these AGs.

As it stands, there are 13 EGs. The four most relevant for this project are:

- EG02: Managed business risk
- EG03: Compliance with external laws and legislation
- EG06: Business service continuity and availability
- EG10: Staff skills, motivation and productivity

These EGs line up well with a risk-based approach and ensuring that business continues uninterrupted (or at least with as little interruption as possible) in the event of a cybersecurity event. They also address skills elements as well as the imperative of complying with the regulatory environment. In these EGs there is also scope to put preventative measures in place in order to establish a robust cybersecurity strategy.

To find the applicable AGs, Appendix A.1.1 of COBIT 2019 was used. Each EG is associated with primary and secondary alignment goals (AGs). For the selected EGs, these primary (P) AGs are presented in the following adapted table:

Table 4: Enterprise and alignment goal mapping (Information Systems Audit and Control Association, 2018)

	EG02 - Managed business risk	**EG03 - Compliance with external laws and legislation**	**EG06 - Business service continuity and availability**	**EG10 - Staff skills, motivation and productivity**
AG01 - IT compliance and support for business compliance with external laws and regulations		P		
AG02 - Managed IT and related risk	P			
AG07 - Security of information, processing infrastructure and applications, and privacy	P		P	
AG11 - IT compliance with internal policies		P		
AG12 - Competent and motivated staff with mutual understanding of technology and business				P

The four EGs were mapped to five AGs that ought to be achieved, namely AG01, 02, 07, 11 and 12. An overlap was then found between EG02 and EG06 where both emphasise AG07 as a primary AG. The control objectives that make up the five AGs had to be examined to

determine which governance and management objectives were relevant. Using Appendix A.1.2 from COBIT 2019, the following primary control objectives for the above AGs were identified:

Table 5: Alignment goals - Control objectives mapping

	AG01 - IT compliance and support for business compliance with external laws and regulations	**AG02 - Managed IT and related risk**	**AG07 - Security of information, processing infrastructure and applications, and privacy**	**AG11 - IT Compliance with internal policies**	**AG12 - Competent and motivated staff with mutual understanding of technology and business**
EDM01 - Ensured governance framework setting and maintenance	P (Governance objective)				
EDM03 - Ensured risk optimisation			P (Governance objective)		
APO1 - Managed IT management framework				P (Management objective)	
APO07 - Managed human resources					P (Management objective)
APO08 - Managed relationships					P (Management objective)
APO12 - Managed risk		P (Management objective)	P (Management objective)		
APO13 - Managed security			P (Management objective)		
MEA02 - Managed system of internal control				P (Management objective)	
MEA03 - Managed compliance with external requirements	P (Management objective)				
MEA04 - Managed assurance				P (Management objective)	

This resulted in two governance objectives to be considered:

- EDM01 – Ensured governance framework setting and maintenance
- EDM03 – Ensured risk optimisation

Various other APO and MEA management objectives are also highlighted to demonstrate the difference in focus between the governance and management objectives. The governance objectives clearly refer to direction setting and guiding behaviour, whereas the management objectives explicitly refer to managerial implementation and monitoring that must take place

at organisational level. As indicated earlier, the focus must be on the governance objectives. As a result, the AGs that were relevant to the framework at sectoral level are AG01 and AG07. However, all five of the derived AGs are relevant to the organisational level and should not be ignored by management at that level.

The two derived governance objectives each have three control sub-objectives:

- EDM01 – Ensured governance framework setting and maintenance:
    - The current governance arrangements and implemented frameworks must be evaluated to determine if they are still fit for purpose and whether there are currently any gaps. A process of optimisation must take place.
    - The established governance system must be used to direct leaders, employees and systems towards established strategic goals. In this context, these are cybersecurity related strategies and goals.
    - The optimised governance system must be monitored for performance and effectiveness. Corrective action must be taken if necessary and the governance arrangement must be amended as circumstances and needs change.
- EDM03 – Ensured risk optimisation has three control sub-objectives:
    - Evaluating risk management: This entails examining current risk issues and the risk appetite of the organisation and current risk procedures.
    - Directing risk management: This section largely emphasises determining risk principles applicable to the organisation and developing mitigation tools.
    - Monitoring risk management: This section requires the organisation to conduct a risk analysis and to determine if the above are fit for purpose in the organisation.

Therefore, a focus on current governance arrangement and risk management strategy yields the following governance practices necessary at sectoral level:

Table 6: COBIT 2019 governance practices

Source	No.	Governance practice
COBIT 2019	4.1	Analyse current governance arrangements to determine effectiveness and gaps
	4.2	Use optimised governance arrangements to direct behaviour
	4.3	Oversee and monitor implemented governance arrangement performance and amend when necessary
	4.4	Evaluate current risk management strategies to determine if risk appetite and current procedures are appropriate
	4.5	Direct risk management by selecting appropriate risk principles and develop risk mitigation tools
	4.6	Monitor risk management through ongoing risk analysis and amend risk strategy approach if necessary

Each of these specific governance practices can be applied to the sphere of cybersecurity and were included in the proposed framework.

These sources of knowledge were drawn upon in the various government mandates on cybersecurity, IT management and ICT governance. The updated content is presented here and categorised to demonstrate what minimum practices ought to be in place at sector level. It might, however, be useful to very briefly demonstrate how these knowledge sources aid lower-level implementation concerns at local government level.

Adoption of the above and subsequent content would align with the following principles from the SALGA roadmap to ICT governance (Smith, 2012):

- Principle 2: Strategic mandate is supported by any ICT activities and plans
- Principle 3: Corporate governance of IT is created in an enabling environment
- Principle 4: ICT strategic alignment allowing and enabling the achieving of goals in the water sector
- Principle 6: Risk management and assurance

As such, there is an assurance that sector level governance implementation aligns with the entire cybersecurity value chain.

5. COLLATING & CATEGORISATION OF PRACTICES AND VALIDATION OF GUIDELINE

The following steps were taken to create a validated framework for the governance of cybersecurity at sectoral level:

- The governance practices identified (Chapters 3 and 4) were collated into one list.
- It was validated that these identified governance practices addressed all seven dimensions of a governance framework as per COBIT 2019 guidance.
- The validated governance practices were categorised into coherent groupings.
- The final framework was validated from literature.

5.1 Collating and validating governance practices

With the identification and analysis of relevant knowledge sources complete, the following practices were identified (Chapter 4) as having special significance for cybersecurity governance in the water and sanitation function at sectoral level:

Table 7: Consolidated governance practices

Source	No.	Governance practice
NCPF	1.1	The governing body should govern technology and information in a way that supports the organisation setting and achieving its strategic objectives
	1.2	Roles and responsibilities for critical infrastructure
	1.3	Direction setting policy approval
	1.4	Management delegation
	1.5	Ongoing oversight of the results of cybersecurity initiatives
CGICTPF	2.1	Establish cybersecurity strategy based on the sectoral IT security strategy
	2.2	Develop a cybersecurity plan that includes the development and oversight of an information security management system (ISMS) for the sector
	2.3	Develop a coherent cybersecurity policy to provide guidance for the sector
	2.4	Develop the sectoral ICT continuity strategy based on the sectoral business continuity strategy
King IV	3.1	The governing body must assume responsibility for the governance of technology through coherent strategy
	3.2	The governing body must approve policy to support direction setting
	3.3	The governing body must delegate responsibility to management to implement and execute effective management
	3.4	The governing body must oversee technology management to ensure the following:
	3.4.1	Integrate IT risks into enterprise-wide risk management
	3.4.2	Arrange for business resilience
	3.4.3	Proactively monitor intelligence to identify and respond to cyberthreats
	3.4.4	Dispose of obsolete technology responsibly to ensure that cybersecurity is not threatened
	3.4.5	Ensure that technology and information are used responsibly and ethically
	3.4.6	Comply with relevant laws
	3.4.7	Ensure that the information architecture supports confidentially and availability of information
	3.4.8	Ensure the protection of personal information
	3.4.9	Ensure continuous monitoring of the security of information
COBIT 2019	4.1	Analyse current governance arrangements to determine effectiveness and gaps
	4.2	Use optimised governance arrangements to direct behaviour
	4.3	Oversee and monitor implemented governance arrangement performance and amend when necessary
	4.4	Evaluate current risk management strategies to determine if risk appetite and current procedures are appropriate
	4.5	Direct risk management by selecting appropriate risk principles and develop risk mitigation tools
	4.6	Monitor risk management through ongoing risk analysis and amend risk strategy approach if necessary

These practices can be mapped to the seven dimensions of a coherent governance framework as per COBIT 2019:

Table 8: Governance practices mapped to the seven dimensions of a governance framework

No.	Governance practice	Policies and procedures	Processes	Organisational structures	People, skills and competencies	Culture, ethics, behaviour	Information flows	Services, infrastructure and applications
1.1	The governing body should govern technology and information in a way that supports the organisation setting and achieving its strategic objectives			x				
1.2	Roles and responsibilities for critical infrastructure			x				
1.3	Direction setting policy approval	x						
1.4	Management delegation		x		x	x	x	
1.5	Ongoing oversight of the results of cybersecurity initiatives						x	x
2.1	Establish cybersecurity strategy based on the sectoral IT security strategy	x		x				x
2.2	Develop a cybersecurity plan that includes the development and oversight of an information security management system (ISMS) for the sector		x				x	x
2.3	Develop a coherent cybersecurity policy to provide guidance for the sector	x				x		
2.4	Develop the sectoral ICT continuity strategy based on the sectoral business continuity strategy	x	x	x				x
3.1	The governing body must assume responsibility for the governance of technology through coherent strategy			x		x		
3.2	The governing body must approve policy to support direction setting	x						
3.3	The governing body must delegate responsibility to management to implement and execute effective management			x	x			
3.4	The governing body must oversee technology management to ensure the following:		x				x	
3.4.1	Integrate IT risks into enterprise-wide risk management			x		x		
3.4.2	Arrange for business resilience		x		x			
3.4.3	Proactively monitor intelligence to identify and respond to cyberthreats		X				x	x
3.4.4	Dispose of obsolete technology responsibly to ensure that cybersecurity is not threatened		x			x		
3.4.5	Ensure that technology and information are used responsibly and ethically		x		x	x		
3.4.6	Comply with relevant laws	x				x		
3.4.7	Ensure that the information architecture supports confidentially and availability of information	x				x		x
3.4.8	Ensure the protection of personal information	x					x	x
3.4.9	Ensure continuous monitoring of the security of information	x					x	
4.1	Analyse current governance arrangements to determine effectiveness and gaps	x		x		x		

No.	Governance practice	Policies and procedures	Processes	Organisational structures	People, skills and competencies	Culture, ethics, behaviour	Information flows	Services, infrastructure and applications
4.2	Use optimised governance arrangements to direct behaviour	x				x		
4.3	Oversee and monitor implemented governance arrangement performance and amend when necessary	x				x		
4.4	Evaluate current risk management strategies to determine if risk appetite and current procedures are appropriate		x				x	x
4.5	Direct risk management by selecting appropriate risk principles and develop risk mitigation tools	x	x					
4.6	Monitor risk management through ongoing risk analysis and amend risk strategy approach if necessary		x				x	

The above table indicates that all seven dimensions of a governance framework are addressed by the governance practices identified. It is therefore verified that all the identified practices that were deemed relevant contribute to the content of the framework for cybersecurity governance at sector level. In the following section, these practices are categorised into coherent groupings to finalise the proposed governance framework.

5.2 Governance practice categorisation

The validated practices were grouped into similar categories and transformed into a coherent framework. Each of these practices can be categorised according to the general theme it represents. The following table groups similar and related governance practices by colour:

Table 9: Categorisation of governance practices

Source	No.	Governance practice	Category
NCPF	1.1	The governing body should govern technology and information in a way that supports the organisation setting and achieving its strategic objectives	A (Strategy)
	1.2	Roles and responsibilities for critical infrastructure	B (Delegation)
	1.3	Direction setting policy approval	C (Policy)
	1.4	Management delegation	B (Delegation)
	1.5	Ongoing oversight of the results of cybersecurity initiatives	D (Oversight)
CGICT	2.1	Establish cybersecurity strategy based on the sectoral IT security strategy	A (Strategy)
	2.2	Develop a cybersecurity plan that includes the development and oversight of an information security management system (ISMS) for the sector	D (Oversight)
	2.3	Develop a coherent cybersecurity policy to provide guidance for the sector	C (Policy)
	2.4	Develop the sectoral ICT continuity strategy based on the sectoral business continuity strategy	E (Resilience)
King IV	3.1	The governing body must assume responsibility for the governance of technology through coherent strategy	A (Strategy)
	3.2	The governing body must approve policy to support direction setting	C (Policy)
	3.3	The governing body must delegate responsibility to management to implement and execute effective management	B (Delegation)
	3.4	The governing body must oversee technology management to ensure the following:	D (Oversight)
	3.4.1	Integrate IT risks into enterprise-wide risk management	F (Risk management)
	3.4.2	Arrange for business resilience	E (Resilience)
	3.4.3	Proactively monitor intelligence to identify and respond to cyberthreats	F (Risk management)
	3.4.4	Dispose of obsolete technology responsibly to ensure that cybersecurity is not threatened	F (Risk management)
	3.4.5	Ensure that technology and information are used responsibly and ethically	F (Risk management)
	3.4.6	Comply with relevant laws	F (Risk management)
	3.4.7	Ensure that the information architecture supports confidentially and availability of information	F (Risk management)
	3.4.8	Ensure the protection of personal information	F (Risk management)
	3.4.9	Ensure continuous monitoring of the security of information	D (Oversight)
COBIT 2019	4.1	Analyse current governance arrangements to determine effectiveness and gaps	D (Oversight)
	4.2	Use optimised governance arrangements to direct behaviour	A (Strategy)
	4.3	Oversee and monitor implemented governance arrangement performance and amend when necessary	D (Oversight)
	4.4	Evaluate current risk management strategies to determine if risk appetite and current procedures are appropriate	F (Risk management)
	4.5	Direct risk management by selecting appropriate risk principles and develop risk mitigation tools	F (Risk management)
	4.6	Monitor risk management through ongoing risk analysis and amend risk strategy approach if necessary	D (Oversight)

The above table is transformed into the following proposed framework to highlight the categories as aspects to be addressed:

Table 10: Categorisation of governance practices and referencing

Category	Practice group	Sources
Strategy	1.1, 2.2, 3.1, 4.2	NCPF, CGICT, King IV, COBIT 2019
Delegation	1.2, 1.4, 3.3	NCPF, King IV
Policy setting	1.3, 2.3, 3.2	NCPF, CGICT, King IV
Oversight	1.5, 2.2, 3.4, 3.4.9, 4.1, 4.3, 4.6	NCPF, CGICT, King IV, COBIT 2019
Resilience	2.4, 3.4.2	CGICT, King IV
Risk management	3.4.1, 3.4.3, 3.4.4, 3.4.5, 3.4.6, 3.4.7, 3.4.8, 4.4, 4.5	King IV, COBIT 2019

Each thematic category is constituted by the numbered practices and supported by their sources of knowledge. Visually, the proposed governance framework can be represented by the following figure:

Figure 5: Components of the proposed cybersecurity governance framework for the water and sanitation sector

Each of these is defined by the cybersecurity context and what they would entail in general. Brief definitional explanations for each of the six components are as follows:

- Strategy: Contains all the activities required to set the direction for cybersecurity within the overall sectoral strategy as informed by the IT strategy of the water and sanitation sector. The CSIRT would be ideally suited to drive this effort. This direction setting effort provides the environment in which all other activities operate and to which they direct their efforts.

- Delegation: The CSIRT must identify management resources and assign roles and responsibilities that aim at achieving the objectives derived from strategy. These designated roles and responsibilities translate the governance of cybersecurity practices into operational activities that can be managed at the appropriate organisational level.
- Policy setting: The formalising of strategic intent should be the aim of policy setting. This is achieved by providing and communicating guiding principles to the entire body to which a policy applies. It is, however, important for policy setting to evolve with the needs of the sector as well as any changes in strategy. Policy setting allows for automated decision making in that guidance is already provided on what to do in specific contexts and situations. Therefore, policies support strategy in that it is a direction-setting instrument.
- Oversight: This is a monitoring activity intended to gauge the effectiveness of current strategy, policy setting, risk management and delegation at sectoral level. Oversight at lower organisational levels is intended to ensure that practices are implemented effectively and achieve the purpose for which they are implemented. In either case, this function should provide direction in taking corrective action when and where required.
- Resilience: Any organisation will be under continuous threat of debilitating events that could cause interruption to operations. At sectoral level, the systems and processes in place must allow for the sector and the underlying organisations to be able to carry on with operations to a stated level of performance and be able to withstand the effects of these events.
- Risk management: Risk management requires the foresight to identify potential adverse events and provide an avenue for managing these risks to an appropriate degree, depending on the probability of a risk event occurring and the severity of the impact of a realised risk. Risk management supports sectoral resilience in this regard.

5.3 Examples of proposed framework component adoption

Examples of implemented governance regimes for cybersecurity that include the above six components are to be found in literature. These are briefly highlighted in various public and private sector contexts in the following section in order to demonstrate a holistic approach that covers the best practices wherever they may exist.

As the water and sanitation department is almost exclusively based in the governmental public sector, this would of be great importance in order to determine the validity of the above

concepts in similar contexts. This would also include examples of public-private partnership arrangements. As such, it would be valid to consider private sector governance regime adoptions as this would almost certainly have an impact on how the public sector must govern implementations.

Public sector – Cyber Assessment Framework (CAF) and National Institute of Standards and Technology (NIST) Cybersecurity Framework (CF) for public-private partnerships

To validate the proposed water sector cybersecurity governance framework, the authors contrasted the developed framework against CI cybersecurity governance frameworks from two developed countries: the CAF of the United Kingdom (UK) as developed by the National Cyber Security Centre (NCSC) and NIST Cybersecurity Framework (CF) for CI protection of the United States of America (USA). These frameworks are used in the governance of CI cybersecurity at both sector and organisational levels. But first, we contextualise relations between the state (national government) and sector actors in terms of CI cybersecurity governance.

CI systems embody a variety of ownership structures and operating models, and often function in both a cyberspace and physical capacity (Martin & San Juan, 2019). Unlike in the UK, USA and other developed countries, some key CI in South Africa (e.g. electricity, water and aviation) is owned and/or operated by the state through state-owned companies. However, other key CI (e.g. finance, transport and ICT) is owned and/or operated by private industry. These ownership structures and operating models demonstrate the complex nature of governing CI systems which may include different authorities, responsibilities and regulations (Martin & San Juan, 2019). Therefore, variations in cybersecurity governance arrangements may reflect more distinctive state-sector and state-private industry relations than anything else (Calcara & Marchetti, 2021).

In the UK, for example, the NCSC is an organ of state responsible for the central coordination and management of national cyberincidents and for setting the regulatory and policy framework of national CI operators (Calcara & Marchetti, 2021). After leaving the European Union (EU), which developed the Network and Information Systems Security (NIS) Directive for all EU members, the UK is continuing with the implementation of the NIS Directive (Calcara & Marchetti, 2021). The NIS Directive aims to improve the baseline level of CI cybersecurity for all EU member states (Michalec, Milyaeva & Rashid, 2021). Water in the UK is regulated by two bodies: the economic regulator, Water Services Regulation Authority or Ofwat, and the water quality assessor, Drinking Water Inspectorate (DWI) (Michalec et al., 2021).

The DWI audits the sufficiency and quality of drinking water supplies in addition to water provision incidents (Michalec et al., 2021). It has also been given the responsibility for implementing the NIS in the water sector of the UK (Michels & Walden, 2018; Michalec et al., 2021). According to Michels and Walden (2018), the DWI's current responsibility in this regard is to provide guidance and ensure the appropriateness and proportionality of cybersecurity measures. In other words, the DWI oversees the UK's water sector cybersecurity governance ecosystem. In this regard, water entities in the UK were asked to submit their cybersecurity self-assessment reports throughout 2020 utilising the NCSC's CAF (Michalec et al., 2021). The CAF is a cybersecurity tool for organisations responsible for vitally important services and activities in the UK (National Cybersecurity Centre, 2021a). It is utilised as a guideline to carry out cyber resilience assessments of the different CI sectors in the UK (Michalec et al., 2021). Upon completion of the cyber resilience assessments, the water entities agreed on investment plans to improve and upgrade their assets with security in mind (Shukla et al., 2019). Michels and Walden (2018) point out that the CAF is a principles-based regulation tool, which means that organisations only strive to meet government's cybersecurity objectives rather than being prescribed which steps to follow to meet these objectives.

Because much of the UK's CI is owned and/or operated by the private sector (Martin & San Juan, 2019), the cyber resilience assessments exercise in the water sector demonstrated that the public-private partnership (PPP) model is a leading mode of governance in that country (Carr, 2016; Topping et al., 2021). The state should not be the sole actor responsible for ensuring CI protection and security (Martin & San Juan, 2019). It is a shared responsibility between the state and private industry, with the state responsible for providing a national security governance framework and private industry responsible for ensuring protection of assets and provision of critical services (Martin & San Juan, 2019). Indeed, the lines between what is public and private, national and global are waning in cyberspace (Collier, 2018). This is important to highlight as the governance of CI cybersecurity is more about security of the information systems that underpin CI (Martin & San Juan, 2019).

However, the National Cybersecurity Centre (2021b) cautions that there is no one-size-fits-all approach to cybersecurity governance. At one end a more formalised cybersecurity governance approach may be adopted with clearly defined roles and business processes (National Cybersecurity Centre, 2021b). At the other, an informal approach to governance may be chosen. At EU level, the NIS Directive is sector agnostic and devolves to sector-specific authorities the implementation guidelines with the water sector overseen by DWI (Michalec et al., 2021). Therefore, the CAF governance goal in the UK (National Cybersecurity Centre, 2021b) – putting in place the policies and processes which govern the organisation's approach to the security of network and information systems – leaves the cybersecurity

implementation responsibilities of the water sector to the DWI. In this regard, the CAF refers CI operators to ISO 27001 and IEC 62443-2-1:2010 for their own implementations (National Cybersecurity Centre, 2021b). The CAF only delineates the CI cybersecurity governance objectives of the state. As contained in the CAF cybersecurity objectives to protect national CI in the UK, good governance principles should (National Cybersecurity Centre, 2021b):

- Clearly link cybersecurity activities to an organisation's goals and priorities.
- Identify the individuals, at all levels, who are responsible for making cybersecurity decisions and empower them to do so.
- Ensure accountability for decisions.
- Ensure that feedback is provided to decision makers on the impact of their choices.
- Ensure that the approach to cybersecurity governance aligns with organisation-wide governance strategies and business priorities, such as financial governance or health and safety.

The above CAF governance principles were utilised to validate the proposed water sector cybersecurity governance framework of South Africa as shown in Table 11:

Table 11: SA water sector cybersecurity governance framework validation against CAF

CAF governance principles	Strategy	Delegation	Policy setting	Oversight	Resilience	Risk manage-ment
Organisational goals and activities	X					
Roles and responsibilities set		X				
Accountability				X		
Feedback and information flow		X	X	X		
Alignment with other governance activities in the organisation	X		X			

Created through collaboration between private industry and government, the NIST CF, on the other hand, is a voluntary framework – based on existing standards, guidelines and practices – for reducing cyberrisks to CI (National Institute for Standards and Technology, 2021). In the USA, the NIST CF's role was reinforced through Presidential Executive Order 13636 by the Cybersecurity Enhancement Act of 2014 (National Institute for Standards and Technology, 2021). It consists of 23 categories which represent the cybersecurity functional areas and operational cyber technologies and processes (Donaldson et al., 2018) which Malatji et al. (2021a) have since modified to 29 cybersecurity capabilities. One of these cybersecurity capabilities is governance (Malatji et al., 2021a). The NIST CF governance category or cybersecurity capability provides guidelines for an organisation to design its cybersecurity governance for CI protection at organisational and/or sector level.

In particular, the NIST CF governance category provides guidelines for organisations or CI sectors to develop the policies, procedures and processes to manage and monitor regulatory,

legal, risk, environmental and operational requirements that inform the management of cybersecurity risk (National Institute for Standards and Technology, 2018). As contained in the NIST CF (National Institute for Standards and Technology, 2018) and CI Cybersecurity Capability Framework (Malatji et al., 2021a), organisations and/or CI sectors should carry out the following activities to ensure cybersecurity governance:

- Organisational cybersecurity policy is established and communicated.
- Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.
- Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
- Governance and risk management processes address cybersecurity risks.

The above NIST CF governance principles were utilised to validate the proposed water sector cybersecurity governance framework of South Africa as shown in Table 12:

Table 12: SA water sector cybersecurity governance framework validation against NIST CF

NIST CF governance principles	Strategy	Delegation	Policy setting	Oversight	Resilience	Risk manage-ment
Cybersecurity policy			X		X	X
Roles and responsibilities set and aligned	X	X				
Legal and regulatory requirements			X	X		X
Risk management processes					X	X

The combined NCSC CAF (UK) and NIST CF (USA) validation of the proposed water sector cybersecurity governance framework of South Africa is shown in Table 13:

Table 13: SA water sector cybersecurity governance framework validation

NIST CF governance principles	Strategy	Delegation	Policy setting	Oversight	Resilience	Risk manage-ment
CAF	X	X	X	X		
NIST CF	X	X	X	X	X	X

The proposed water sector cybersecurity governance framework of South Africa has therefore been validated through the UK's NCSC CAF and USA's NIST CF for CI protection as adopted in the water CI sectors of the respective countries. While CAF and NIST focus on implementation level issues, there are governance considerations that align with the six components of the proposed framework.

Private sector – General Data Protection Regulations (GDPR) in the EU financial industry

The EU requires all organisations to adhere to GDPR requirements (Serrado, Pereira, Da Silva & Bianchi, 2020). Financial institutions are expected to use their own appropriate information security frameworks to achieve alignment with EU GDPR requirements. The GDPR is at heart data protection legislation. It is specifically noted that data protection and cybersecurity as fields are distinct areas of study. However, there is enough overlap in the protection of personal information as digital assets from cybersecurity threats and other adverse effects. The governance of information security would have some effect on the governance of cybersecurity and vice versa. Given the focus on cybersecurity, it is acceptable to refer to certain sections of information security frameworks as cybersecurity would be addressed. Apart from obvious organisational repercussions should cybersecurity fail in a financial institution, there is an additional motivation to avoid massive fines of up to EUR20 million as stipulated in the GDPR. In this instance, it is specifically applicable to personal data of individuals. It is then of particular importance to the water and sanitation sector as millions of personal records could be at risk of cyberattacks.

The GDPR has four main focus areas:

- Accountability: Data may only be used for the purpose for which it is collected and the entity collecting data is responsible for safeguarding the data. This must be explicit in policy and derived from strategy as to what the intent and objectives ought to be.
- Transparency: The person consenting to their personal data being collected must be treated in such a manner as to maintain trust between the collecting organisation and the consenting individual. All persons mandated or authorised to use personal data are therefore required do so in a responsible manner as guided by policy.
- Protection: The collected data must be kept safe from unauthorised access or use. It must be safely and securely deleted or disposed of when no longer needed or when the individual revokes consent for personal data to be kept. This is required to be monitored.
- Reliability: The person consenting to their personal data being collected does so in order to receive some sort of stated benefit that must have an economic consequence. As such, the organisations collecting the data must make decisions based on correct data that is available at the time of decisions being made on behalf of the consenting individual.

These components of the GDPR are difficult to implement without the use of an information security framework such as COBIT 2019 or ISO27001, especially in the financial services

industry. Given these stringent requirements and that financial services organisations view their data as part of CI in their context, there are certain similar needs that the water and sanitation sector can relate to. The research in this example found that COBIT 2019 is useful for governance aspects of data protection and aids in establishing the implementation level of cybersecurity in this context.

Table 14: GDPR governance context

GDPR principles	Strategy	Delegation	Policy setting	Oversight	Resilience	Risk manage-ment
Accountability	X		X	X		
Transparency			X	X		
Protection				X	X	X
Reliability		X			X	X

It is seen in aligning the EU's GDPR legalisation with internal information security frameworks that there are examples of how the six components of the proposed governance of cybersecurity frameworks are adopted by these organisations.

Private sector – Private governance regulation by cyberinsurance organisations

It is clear that most cybersecurity governance requirements are initially set by public regulatory bodies (Herr, 2021). However, with the rise of insurance firms underwriting cybersecurity risks, a new source of regulation or standards has come to the fore, namely a form of private governance of cybersecurity that is enforced by non-governmental actors.

The cybersecurity insurance firms provide cover should adverse cybersecurity events take place. The monetary value of the cover and the premiums organisations pay are typically tied to the expected impact of a specific event occurring and modulated on a scale of probability. The insured organisation is then also expected to adhere to the insurer's rules and regulations. This external source of cybersecurity requirements then also impacts on the type of governance regime the insured organisation is to adopt.

As cybersecurity adverse events are generally not costly or rare, the exercise invariably adopts a risk-based approach. The insurer and insured need to evaluate their own contexts to determine which types of events are critical and which risks can be absorbed or accepted. Due to the uncertainty of the extent of coverage, the cyberinsurance industry shrank pre-2010 but surged again after major laws were passed in the USA placing certain limits on coverage and new major threats in the cybersecurity landscape were discovered. The premium pool has increased, making risk transfer and client coverage far more feasible than what it was prior to 2015.

Cyberinsurance is increasingly being viewed as a tool for the governance of cybersecurity. Insurance firms conduct an assessment of current cybersecurity needs and the current cybersecurity governance regime to determine a risk profile for an organisation. Therefore, the organisations taking out this insurance are required to adhere to current legislation as well as any additional rules the insurance company imposes.

As it relates to the components of the proposed governance framework, the following can be said: Organisations wishing to pursue a risk-averse strategy in achieving their objectives may decide to adopt a cyberinsurance product and make it an integral part of their organisation. However, as the insurer makes the rules, the insured organisation would have to create policies that reflect and adopt these rules in order for full cover to be in effect. Motivation for effective oversight is increased as a lapse may result in the repudiation of a claim and the full effect of the adverse risk event will fall on the organisation itself. Being insured against significant adverse cyberevents increases the resilience of the organisation in that it may be able to recover quicker from such a disaster. Although in itself, the lapse in service may not immediately be restored, the organisation is protected against financial repercussions of such an event. This is a strong risk management approach in that risk is transferred.

Table 15: Cyberinsurance context

	Strategy	Delegation	Policy setting	Oversight	Resilience	Risk manage-ment
Private cyberinsurance	X		X	X	X	X

However, the responsibility for implementing a cybergovernance regime cannot be transferred to the insurer and the organisation will remain accountable for any decisions they may make in this regard. In addition, if the guidance provided by the insurer for setting up such a governance regime is adopted wholesale by the organisation and it turns out to be incomplete or incorrect, the organisation remains liable in the eyes of the law. As such, there would be no delegation in such a context.

The proposed framework consolidates the governance practices identified in Chapters 3 and 4 to include national policy guidelines from the NCPF as well as best practices from the CGITPF, King IV and COBIT 2019 sources of knowledge. As such, the impact of these knowledge sources on the development of this framework can be illustrated in the following manner:

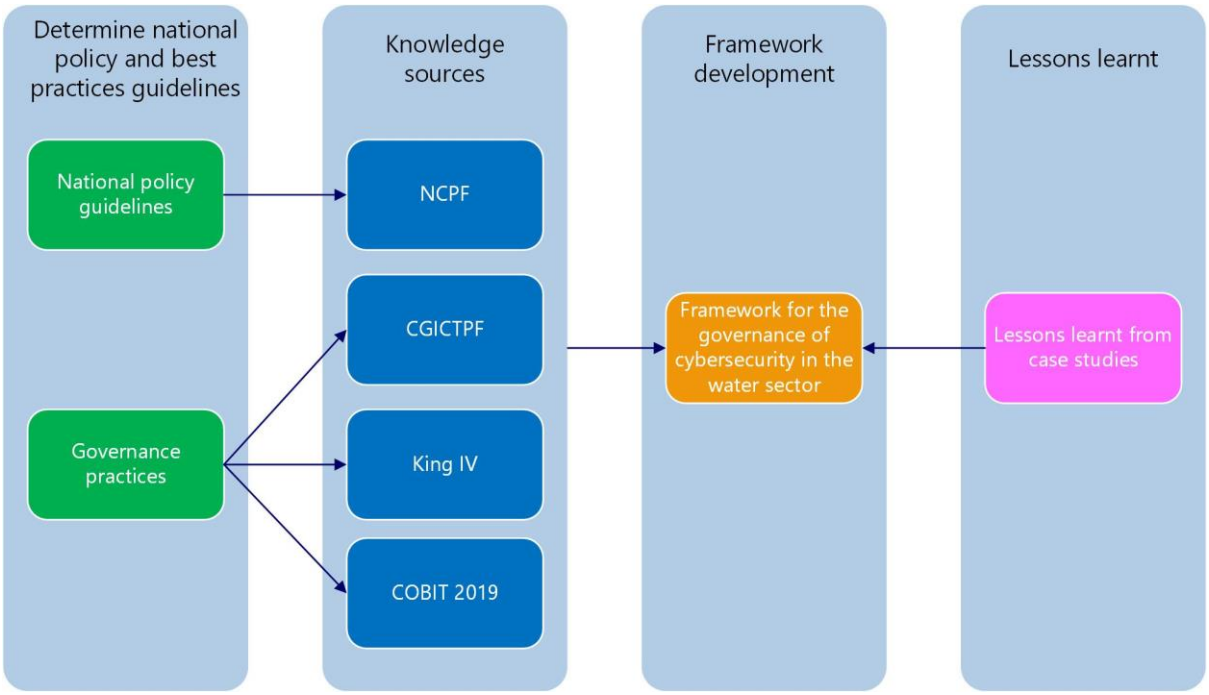

Figure 6: Sources of knowledge in framework development

The above illustrates the fulfilment of the steps delineated in Chapter 2. The content of the governance framework for cybersecurity has been validated against the COBIT 2019 requirement for a governance framework. All the identified practices were thematically grouped into six components: strategy, delegation, policy setting, oversight, resilience and risk management. These six components form categories of governance practices that ought to be considered and governed within the context of the cybersecurity of the water and sanitation sector.

The examples presented, of which there are many more, suggest that the six thematic components that comprise the proposed sectoral governance framework for cybersecurity are present in effective implementations. These six components are present in the proposed framework that can be adopted by the water and sanitation sector governing body for cybersecurity. What is abundantly clear is that the governance of cybersecurity at sectoral level is a complex and multi-stakeholder matter that requires interplay and coordination between national policy, the sector body and public or private security service providers.

6. RECOMMENDATIONS

6.1 Introduction

Guidance is provided in Chapter 3 for sectoral governance arrangements for national policy considerations. This provided content for the governance framework for cybersecurity at sectoral level that relates to a governing body that could fulfil such a role in the sector. This further supports the adoption of the conclusions reached in WP1 as they relate to the establishment of a mandated CSIRT that should take on this governing body role and be the custodian of the cybersecurity governance framework.

The discussion now proceeds to the structure this governing body is recommended to take in order to support and fulfil the needs of cybersecurity at sectoral level. This governing body is mandated by the adoption of the proposed governance framework while at the same time would be responsible to ensure that the objectives of this proposed framework are achieved. Recommendations are made for the adoption of the proposed cybersecurity governance framework.

6.2 Establishment of sector cybersecurity governing body

WP1 recommended the establishment of a national water CSIRT. For ease of reference, the discussion below is presented to highlight the governance role of such a governing body termed a national water CSIRT. It was also found as part of the NCPF mandate that such a body should be established.

To establish the national water CSIRT in conjunction with the national Cybersecurity Hub and with its main cybersecurity responsibilities as defined in section 6.3.6 of the NCPF (South African State Security Agency, 2015:18), a clear understanding of the institutional arrangement of the sector is required. These are the main role players in the water sector as an actor (system element) within the national cybersecurity system (Malatji et al., 2021a). Furthermore, Malatji et al. (2021a) found that the cybersecurity purpose (system function) and legislation and policies (system interconnections) of the water sector are only defined if the water sector remains an actor within the national cybersecurity system governed by the NCPF. In other words, the water sector cannot operate outside of the national cybersecurity system without the need to enact new laws. Thus, the water CSIRT, as the proposed body to represent the water sector as an actor within the national cybersecurity system, must define the following for itself, as alluded to by Malatji et al. (2021a):

- Purpose (system function)
- Stakeholders (actors/system elements)
- Legislation and policies (system interconnections)

The purpose of the water CSIRT has been defined in section 6.3.6(1-8) of the NCPF (South African State Security Agency, 2015:18) as follows:

1. Be a point of contact for the specific sector on cybersecurity matters.
2. Coordinate cybersecurity response activities within the sector.
3. Facilitate information and technology sharing in the sector.
4. Facilitate information sharing and technology exchange with other sector CSIRTs.
5. Establish national standards and best practices for the sector in consultation with the Cybersecurity Centre and the JCPS CRC that are consistent with guidelines, standards and best practices adopted in line with the NCPF.
6. Develop agreed upon measures.
7. Conduct cybersecurity audits, assessment and readiness exercises for the sector.
8. Provide sector entities with best practice guidance on ICT security.

These eight purpose statements address needs at governance and implementation level. At governance level, these mandated objectives provide direction on the implementation of governance practices while also delegating routine activities to lower-level actors in the sector.

The legislation and policies that will govern the water CSIRT once it has been established were outlined in WP1 and can also be found in Malatji et al. (2021b). Thus, in this section only an outline of the stakeholders (actors/system elements) or institutional arrangement of the water sector will be presented to provide context for the proposed governance structure. As governed by national water legislation and policies in South Africa, the institutional arrangement of the water sector is as follows (Malatji et al., 2021b; World Wide Fund for Nature South Africa, 2016):

- Parliament Portfolio Committee – Provides oversight over the Minister's departmental work
- National Department of Water and Sanitation (DWS) – Through the Minister/Executive, it is responsible for water legislation, policies, regulation and budgets
- Regional DWS offices – Responsible for water policies, planning, infrastructure, information and regulations
- Provincial governments – Supply water through local governments' water services authorities (WSAs), which can concurrently be water services providers (WSPs) themselves through municipal water utilities, or subcontract this responsibility to other WSPs, including the private sector
- Local governments – Supply water as WSPs themselves and through subcontractors,

and regulate other WSPs as they are concurrently WSAs by law – not all municipalities are WSAs though

- Water boards/regional water utilities – Through own infrastructure, distribute raw and potable water across vast distances to multiple users via regional water supply schemes or contractual relationships with WSAs
- Catchment management agencies (CMAs) – Coordinate activities of water management institutions as well as those of general water users
- Water user associations (WUAs) – Prevent unlawful use of water resources and regulate the flow of any water course
- Water Research Commission – Coordinates, promotes, encourages and undertakes water-related research on behalf of the DWS
- Water Tribunal – A statutory body mandated to hear appeals against decisions and directives made in terms of the National Water Act 36 of 1998
- Water trading entity – Develops, operates and maintains specific water resources infrastructure
- Trans-Caledon Tunnel Authority (TCTA) – Finances and implements bulk raw water infrastructure

According to the Department of Water and Sanitation (2018), the institutional arrangement of the water sector in South Africa is overly complex, resulting in inefficiencies and lack of transformation in certain areas. In this regard, consultation processes with various role players within and outside the water sector system have been underway since 2018 to create a possible future institutional arrangement that will be effective. As proposed in the National Water and Sanitation Master Plan (Department of Water and Sanitation, 2018), the future governance structure of the water sector, which includes the key stakeholders listed above, is shown in Figure 7:

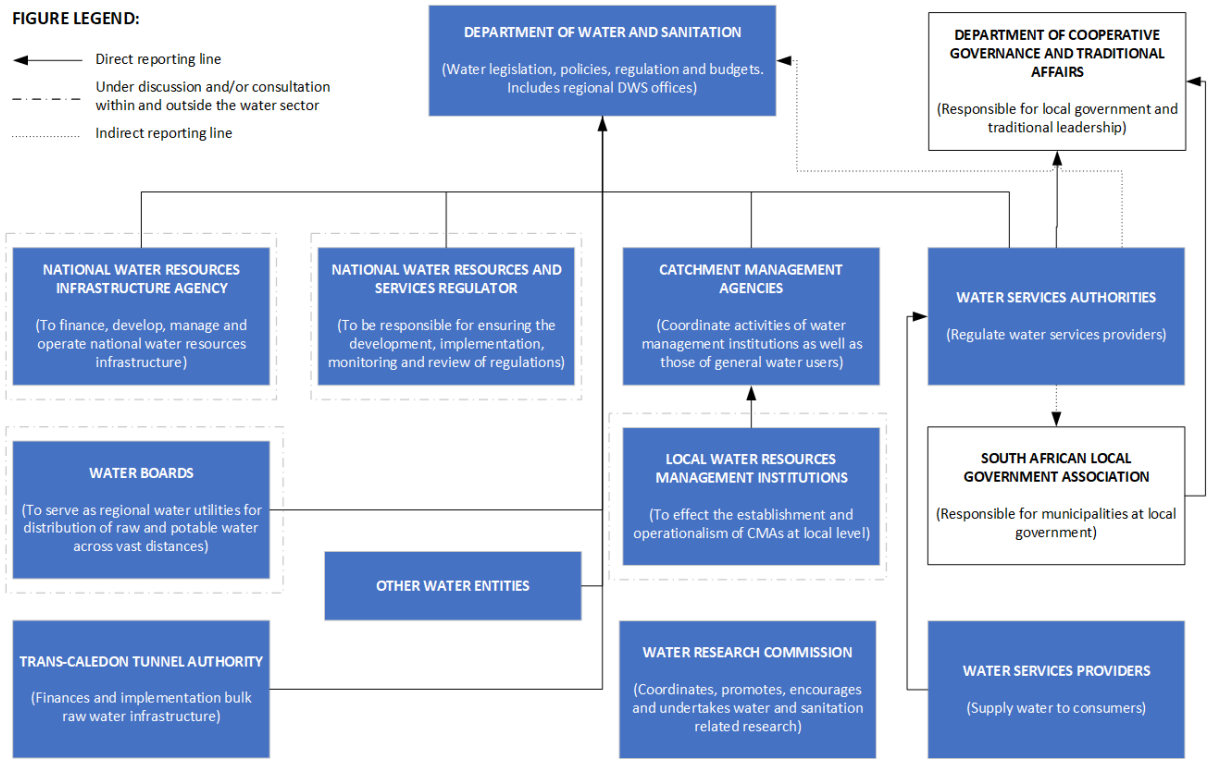

Figure 7: Water sector institutional arrangement

With reference to Figure 7, the TCTA is of particular interest to the proposed establishment of the cybersecurity governing body of the sector. In his State of the Nation address on 11 February 2021, the President of South Africa, Cyril Ramaphosa, mentioned that the establishment of the National Water Resources Infrastructure Agency (NWRIA) to holistically manage the national water resources infrastructure would be expedited (Odendaal, 2021; Department of Water Affairs and Forestry, 2008). This is because a draft Bill had already been gazetted a few years earlier on 30 March 2007 as the South African National Water Resources Infrastructure Agency Limited Draft Bill (Department of Water Affairs and Forestry, 2008). The Bill provides for the disestablishment of the TCTA and transfer of the assets and functions of the national water resources infrastructure and the incorporation of the TCTA into the NWRIA.

The TCTA is an existing agency of the DWS charged with financing and implementing bulk raw water infrastructure projects (Trans-Caledon Tunnel Authority, 2021). Once established, the NWRIA would operate as a state-owned entity, with appropriate governance structures, to ensure accountability and greater efficiency in the management of national water resources infrastructure (Odendaal, 2021; Department of Water Affairs and Forestry, 2008). The authors are of the opinion that the NWRIA would be best placed to host the water CSIRT on behalf of the water sector as the NWRIA Limited Draft Bill empowers it to manage all assets and functions of the national water resources infrastructure. The proposed water sector cybersecurity governance structure is shown in Figure 8:

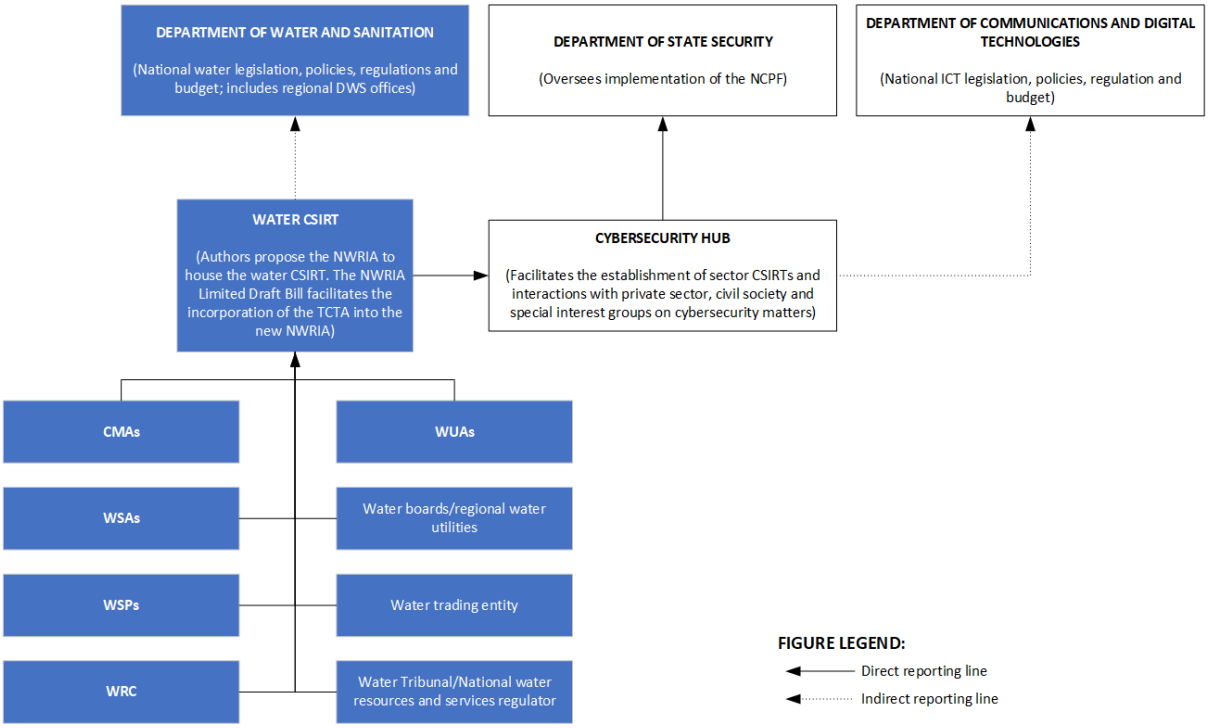

Figure 8: Proposed water sector cybergovernance structure

The water CSIRT governs the sector's cybersecurity responsibilities through interaction and in conjunction with the Cybersecurity Hub located in the Ministry of Communications and Digital Technologies as required by section 7(e) of the NCPF (South African State Security Agency, 2015). This is how the water sector, as an actor within the national cybersecurity system, interrelates with other stakeholders. The cybersecurity governance mode of the water sector, through the water CSIRT, is proposed in the next section.

6.3 Proposed sector cybersecurity governance structure

It is misleading to conceive of cybersecurity governance as a single practice (Eggenschwiler, 2019). For the most part it resembles a set of different but aligned problems, implying various steering mechanisms and role players (Keohane & Victor, 2011). Nye (2014) encourages practitioners and academics alike to think of domains and layers of governance, as Eggenschwiler (2019) asserts that no individual governance model is capable of effectively addressing all the different cybersecurity facets. In this regard, Eggenschwiler (2019) proposes a three-pronged conceptualisation of cybersecurity governance. According to this researcher, cybersecurity governance entails multiple modes of governance including the following (Keast, Mandell & Brown, 2006; Meuleman, 2008; Osborne, 2010; Van Dijk & Winters-van Beek, 2009):

- *Hierarchical governance mode*. This is a top-down governance approach characterised by authoritative systems of centralised command and control where actors are predominantly from government and state-owned entities.
- *Multistakeholder governance mode.* This is a consensus-based governance approach characterised by interactions between various actors from the government, private sector, civil society and non-governmental organisations.
- *Market-driven governance mode.* This is a bottom-up governance approach characterised by decentralisation, independence and autonomy in decision making where the actors are mainly non-governmental.

The advantages and disadvantages of the three governance modes listed above can be summarised as shown in Table 16.

Table 16: Advantages and disadvantages of different governance modes

	Advantages	Disadvantages
Hierarchical	- Valuable for matters directly linked to national CI protection and/or security) - Valuable for matters of national crises - Valuable for matters that tend to require controlled action, which governmental actors can enforce by means of regulatory interventions - Likely to incur lower coordination costs as interventions are generally top-down in nature	- Likely to be rigid and ineffective due to rules and regulations - Corrective actions seldom effect the desired outcomes on time, if at all - Not very transparent
Multistakeholder	- Valuable for complex matters requiring multiple actors - Informal efforts by all actors help minimise costs under unstructured and pervasive circumstances - Levels of expertise, knowledge and skill set increase efficiency and quality of outcomes - Useful for finding solutions to cybersecurity problems of a national, regional and global nature	- Its unstructured collaborative response nature may battle with issues of scalability and sustainability - Its informal structure implies that cooperation and commitment can only go as far as members are willing to contribute resources - Its informal structure may lead to having endless discussions about mitigation efforts because of unclear goals and guidelines - In situations where zero tolerance for error or omission is necessary, informal communications may not be appropriate; this is the case for some global incident response efforts
Market-driven	- Appropriate for routine security activities such as information or endpoint protection - Considerable room for scalability - Provision of security solutions follow a contract-based, competitive approach	- Under considerable risk and high uncertainty circumstances, contract-based and competitive approaches are hard to sustain

Meuleman (2008) summarises the three modes of governance by considering problem types, outcomes, failures or limitations and main actors for each mode. The results are shown in Table 17:

Table 17: Summary of governance modes

	Problem types	Outcomes	Failures/limitations	Main actors
Hierarchical	Disasters, crises and problems that are likely to be resolved only through force	Compliance; regulations; laws; procedures; control	Bureaucratic; ineffectiveness	State actors
Multistakeholder	Complex, unstructured multi-actor issues	Consensus; alliances; agreements; social exchange	Never-ending talks; no decisions; scalability	State and non-state actors
Market-driven	Routine and non-sensitive issues	Services; products; contracts; voluntary agreements	Market failures; inefficiency	Non-state actors; private actors

The three-pronged cybersecurity governance modes discussed above have policy implications against a background of ever-increasing technical complexity and heterogeneity of stakeholders (Tropina & Callanan, 2015). It is clear in Table 17, as described by Meuleman (2008), that depending on the problem type, different controlling and directing mechanisms may be more effective than others (Eggenschwiler, 2019). The question then becomes: what would the most appropriate cybersecurity governance mode be for the water CSIRT of South Africa? To answer this question, the authors examined the cybersecurity system within which the water CSIRT will be embedded. For the water CSIRT to be effective, its operational procedures and human interactions must be governed by, and be in tandem with, the system within which it is embedded: the national cybersecurity system or NCPF.

Section 1.9(a) of the NCPF states that *"…the State is charged with implementing a government led, coherent and integrated cybersecurity approach which, amongst others, will promote a cybersecurity culture and demand compliance with minimum security standards"* (South African State Security Agency, 2015:11-12).

Section 1.10 (South African State Security Agency, 2015:12) provides that *"…this framework (i.e. the NCPF) will be supported by a National Cybersecurity Implementation Plan which will be developed by the State Security Agency in consultation with relevant stakeholders…"*.

Section 4.1.1 (South African State Security Agency, 2015:15) provides for *"centralise[d] coordination of cybersecurity activities, by facilitating the establishment of relevant structures, policy frameworks and strategies…"*. Lastly, section 5.3.5 (South African State Security Agency, 2015:15) states, *"oversee and guide the functioning of the Cybersecurity Hub…and any other CSIRT established in South Africa".*

It is apparent from these statements that at national level, South Africa has adopted a hierarchical mode of cybersecurity governance. However, section 11.2.2 of the NCPF (South African State Security Agency, 2015:23) promotes *"the establishment of collaboration with local stakeholders"*, with a focus on 11.2.2 (c) Bringing private sector and government together in trusted forums; and 11.2.2 (d) Creating a common understanding of the threats and vulnerabilities that the country faces, and the responses required. Based on Tables 16 and

17, the NCPF also encourages a multistakeholder cybersecurity governance mode. Although not discouraged nor explicitly prohibited, there is no explicit reference to a market-driven (non-state actor) cybersecurity governance mode in the NCPF either. It is therefore concluded that the national cybersecurity system within which the water sector is embedded, as an actor in the system, utilises both the hierarchical and multistakeholder modes of cybersecurity governance.

Even without the NWRIA not yet established to manage all assets and functions of the national water resources infrastructure, the bulk of water resources infrastructure in the country is owned and/or managed by the state. This includes waterworks on land owned by another as stipulated in section 135 of the National Water Act 36 of 1998 (South African Government, 1998). The most appropriate cybersecurity governance structure for the water sector, through the water CSIRT, is therefore a combination of the hierarchical and multistakeholder governance modes. The market-driven governance mode will not be necessary to add to the mix as most stakeholders are organs of the state.

Therefore, the water CSIRT should adopt the hierarchical governance mode, as empowered through the NCPF and other national legislation, regulations and policies detailed in Malatji et al. (2021a), to govern the sector's cybersecurity activities. In addition, the water CSIRT should utilise the multistakeholder governance mode to resolve occasionally complex and unstructured CI cybersecurity issues that could be addressed quickly through the expertise of multiple actors, especially from the private sector, nationally, regionally and internationally. These issues could include capacity building, especially in the ICS cybersecurity domain, information sharing and the urgent need to quickly restore critical services from a cyberattack. The water CSIRT's proposed cybersecurity governance mode is summarised in Table 18.

Table 18: Water CSIRT governance mode focus

Governance mode	Focuses on	Strategy	Delegation	Policy setting	Oversight	Resilience	Risk management
Hierarchical	Facilitating information sharing within the sector	X		X		X	X
	Facilitating the sharing of technology tools within the sector			X		X	
	Being a point of contact on water sector cybersecurity matters				X		X
	Developing agreed upon cybersecurity measures for the sector	X		X			X
	Coordinating cybersecurity		X			X	X

Governance mode	Focuses on	Strategy	Delegation	Policy setting	Oversight	Resilience	Risk management
	incident response activities for the sector						
	Providing sector entities with best practice guidance on cybersecurity	X		X			
	Establishing national security standards and best practices for the sector		X	X			
	Conducting cybersecurity audits, assessments and readiness exercises for the sector		X		X	X	X
Multistakeholder	Facilitating information sharing with other sector CSIRTs	X				X	X
	Facilitating the sharing of technology tools with other sector CSIRTs			X		X	
	Coordinating cybersecurity incident response activities for the sector					X	X

The sector-specific governance function/purpose has been discussed in this section and summarised again in Table 18. According to COBIT 2019, what is summarised in Table 18 can be considered the cybersecurity governance objectives of the water sector that the water CSIRT must help realise. Each governance objective can be achieved through execution of process practices and, in turn, each process practice is carried out through a set of practice activities (Information Systems Audit and Control Association, 2018).

It is the opinion of the authors that establishing the water and sanitation CSIRT, as mandated by the NCPF, in the above manner would have a considerable and positive impact on governing cybersecurity effectively in this context. This would require the CSIRT to:

- Be established by the required national guidelines to achieve the eight objectives
- Be established on a hierarchical and multistakeholder governance mode

- Be constituted to be the governing body to specifically adopt the proposed governance framework for cybersecurity to guide and monitor the delegated implementation processes at sector level.

REFERENCES

Alker, H., & Biersteker, T. (2011). The powers and pathologies of networks – insights from the political cybernetics of Karl W. Deutsch and Norbert Wiener. *European Journal of International Relations, 17*(2), 354-378.

Amsler, L. B. (2016). Collaborative governance: Integrating management, politics, and law. *Public Administration and Law*, *76*(5), 700-711.

Ani, U. D., Daniel, N., Oladipo, F., & Adewumi, S. E. (2018). Securing industrial control system environments: The missing piece. *Journal of Cyber Security Technology*, *2*(3-4), 131-163.

Bevir, M. (Ed.) (2013). *The SAGE handbook of governance*. London, United Kingdom: Sage.

Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2021). Global Cybersecurity Index (GCI) and the role of its 5 pillars. *Social Indicators Research*, 1-19.

Calcara, A. & Marchetti, R. (2021). State-industry relations and cybersecurity governance in Europe. *Review of International Political Economy*, DOI:10.1080/09692290.2021.1913438.

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43-62.

Collier, J. (2018). Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision. *Politics and Governance, 6*(2), 13-21.

Coronel, C., & Morris, S. (2016). *Database systems: design, implementation & management.* Cengage Learning.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

Department of Water Affairs and Forestry. (2008). South African National Water Resources Infrastructure Agency Limited Bill: Draft. Retrieved 10 May 2021 from https://www.gov.za/documents/south-african-national-water-resources-infrastructure-agency-limited-bill-draft.

Department of Water and Sanitation. (2018). Department of Water and Sanitation Master Plan. Retrieved July 2021 from https://www.gov.za/documents/national-water-and-sanitation-master-plan-28-nov-2019-0000.

Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2018). *Enterprise Cybersecurity Study Guide: How to Build a Successful Cyberdefense Program Against Advanced Threats*. New York: Apress.

Eggenschwiler, J. (2019). An incident-based conceptualisation of cybersecurity governance. In R. Ellis & V. Mohan (Eds.), *Rewired: Cybersecurity governance.* (pp. 81-96). Hoboken, NJ: Wiley.

Erasmus, W. (2020). An information systems portfolio, programme and project management governance framework: University of Johannesburg (South Africa).

Ferreira, J., Mueller, J., & Papa, A. (2018). Strategic knowledge management: Theory, practice and future challenges. *Journal of Knowledge Management,* Vol. 24 No. 2, pp. 121-126.

Heinimann, H. R., & Hatfield, K. (2017). Infrastructure resilience assessment, management and governance – state and perspectives. In I. Linkov & J. M. Palma-Oliveira (Eds.), *Resilience and risk, NATO science for peace and security series C: environmental security* (pp. 147-185). Springer: Cham, Switzerland.

Herr, T. (2021). Cyber insurance and private governance: The enforcement power of markets. *Regulation & Governance, 15*(1), 98-114.

Information Systems Audit and Control Association. (2018). *COBIT 2019 Framework: governance and management objectives*. Illinois.

Institute of Directors Southern Africa. (2016). The King IV Report on Corporate Governance for South Africa. Retrieved from http://www.iodsa.co.za/?page=AboutKingIV.

Jackson, S. (2015). Overview of resilience and theme issue on the resilience of systems. *Insight*, *18*(1), 7-9.

Janke, R., Tryby, M., & Clark, R. M. (2014). Protecting water supply critical infrastructure: An overview. In R. M. Clark & S. Hakim (Eds.), *Securing water and wastewater systems: Protecting critical infrastructure* (pp. 29-85). Cham: Springer International.

Keast, R., Mandell, M., & Brown, K. (2006). Mixing state, market and network governance modes: The role of government in “crowded” policy domains. *International Journal of Organization Theory and Behavior*, *9*(1), 27-50.

Keohane, R. O., & Victor, D. G. (2011). The regime complex for climate change. *Perspectives on Politics*, *9*(1), 7-23.

Malatji, M., Marnewick, A. L. & Von Solms, S. (2021a). Cybersecurity capabilities for critical infrastructure resilience. *Information and Computer Security*, https://doi.org/10.1108/ICS-06-2021-0091.

Malatji, M., Marnewick, A. L. & Von Solms, S. (2021b). Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa. *Sustainability*, *13*(1), 291.

Martin, A., & San Juan, V. (2019). Cyber governance and the financial services sector: The role of public-private partnerships. *Rewired*, 97-115.

Michalec, O., Milyaeva, S., & Rashid, A. (2021). Reconfiguring governance: How cyber security regulations are reconfiguring water governance. *Regulation & Governance*, https://doi.org/10.1111/rego.12423.

Michels, J. D., & Walden, I. (2018). How safe is safe enough? Improving cybersecurity in Europe's critical infrastructure under the NIS Directive (December 7, 2018). Queen Mary School of Law Legal Studies Research Paper No. 291/2018. Retrieved 27 November 2021 from https://web.archive.org/web/20210417093335/https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3297470.

Meuleman, L. (2008). *Public management and the metagovernance of hierarchies, networks and markets: The feasibility of designing and managing governance style combinations*. Berlin: Springer.

Mueller, M. (2017). Is cybersecurity eating internet governance? Causes and consequences of alternative framings. *Digital Policy, Regulation and Governance*, *19*(6), 415-428.

Muller, R. (2009). *Project governance*. Surrey: Gower.

National Cybersecurity Centre. (2021a). NCSC CAF guidance. Retrieved 27 November 2021 from https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance.

National Cybersecurity Centre. (2021b). Risk management guidance: Guidance to help organisations make decisions about cyber security risk. Retrieved 27 November 2021 from https://web.archive.org/web/20210121184504/https://www.ncsc.gov.uk/collection/risk-management-collection/governance-cyber-risk/security-governance-introduction.

National Institute for Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. Retrieved 27 November 2021 from https://web.archive.org/web/20201122005055/https://www.nist.gov/cyberframework.

National Institute for Standards and Technology. (2021). Getting started. Retrieved 27 November 2021 from https://web.archive.org/web/20211105021332/https://www.nist.gov/cyberframework/getting-started.

Nye, J. S. (2014). The regime complex for managing global cyber activities. Retrieved 2 October 2021 from https://web.archive.org/web/20210628035424/https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

Odendaal, N. (2021). TCTA put forward as new water agency implementor. Retrieved 10 May 10 2021 from https://web.archive.org/web/20210324105831/https://www.engineeringnews.co.za/article/tcta-put-forward-as-new-water-agency-implementor-2021-03-23/rep_id:4136.

Osborne, S. P. (2010). *The new public governance? Emerging perspectives on the theory and practice of public governance*. New York, NY: Routledge.

Peters, G. B. (2013). Institutional theory. In M. Bevir (Ed.), *The SAGE handbook of governance* (pp. 576). London: Sage.

Sarker, I. H., Kayes, A., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data, 7*(1), 1-29.

Serrado, J., Pereira, R.F., Mira da Silva, M. and Scalabrin Bianchi, I. (2020), "Information security frameworks for assisting GDPR compliance in banking industry", *Digital Policy, Regulation and Governance*, Vol. 22 No. 3, pp. 227-244. https://doi.org/10.1108/DPRG-02-2020-0019

Shukla, M., Johnson, S. D., & Jones, P. (2019), Does the NIS implementation strategy effectively address cyber security risks in the UK? In 2019 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2019. Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/CyberSecPODS.2019.8884963.

Singh, N. A., Gupta, M., & Ojha, A. (2014). Identifying factors of organizational information security management. *Journal of Enterprise Information Management*, *27*(5), 644-667.

Smith, P. (2012). *A municipal guide/roadmap to successful ICT governance*. Pretoria: South African Local Government Association.

South African Department of Human Settlements. (2012). Corporate governance of information and communication technology policy framework. Retrieved October 2021 from http://www.nwpg.gov.za/Community_Safety_and_Transport_Management/new/documents/policies/Corporate%20%20Governance%20of%20Information%20Communication%20Technology%20Policy%20Framework.pdf

South African Government. (1998). National Water Act 36 of 1998. Retrieved 2 October 2021 from https://web.archive.org/web/20210826112547/https://www.gov.za/sites/default/files/gcis_document/201409/a36-98.pdf.

South African State Security Agency. (2015). National Cybersecurity Policy Framework (NCPF). Retrieved 10 April 2020 from https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf.

Spathoulas, G., & Katsikas, S. (2019), Towards a secure Industrial Internet of Things. In C. Alcaraz (Ed.), *Security and privacy trends in the Industrial Internet of Things: Advanced sciences and technologies for security applications* (pp. 29-45). Berling: Springer

Trans-Caledon Tunnel Authority. (2021). About us: Who are we? Retrieved 18 June 2021 from https://web.archive.org/web/20210302154236/https:/www.tcta.co.za/about-us.

Topping, C., Dwyer, A. C., Michalec, O., Craggs, B., & Rashid, A. (2021). Beware suppliers bearing gifts! Analysing coverage of supply chain cyber security in critical network infrastructure sectorial and cross-sectorial frameworks. *Computers and Society*, *108*, 102324.

Tropina, T., & Callanan, C. (2015). *Self- and co-regulation in cybercrime, cybersecurity and national security*. Springer, Cham, Switzerland.

Van Dijk, J., & Winters-van Beek, A. (2009). The perspective of network government: The struggle between hierarchies, markets and networks as modes of governance in contemporary government. In A. Meijer, K. Boersma, & P. Wagenaar (Eds.), *ICTs, citizens and governance: After the hype!* (pp. 235-255). Lancaster: Gavelle Books.

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, *26*(1), 2-9. https://doi.org/10.1108/ICS-04-2017-0025.

Weiss, J. (2014). Industrial control system (ICS) cyber security for water and wastewater systems. In R. M. Clark & S. Hakim (Eds.), *Securing water and wastewater systems: Protecting critical infrastructure* (pp. 87-105). https://doi.org/10.1007/978-3-319-01092-2_3.

World Wide Fund for Nature South Africa. (2016). Facts and futures – rethinking South Africa's water future. Retrieved 2 October 2021 from https://web.archive.org/web/20210910084629/http://awsassets.wwf.org.za/downloads/wwf009_waterfactsandfutures_report_web__lowres_.pdf.