Compliance with ICT Governance in Corporate South Africa

Rabelani Dagada
UNISA Graduate School of Business Leadership, Johannesburg, South Africa

dagadr@unisa.ac.za

Abstract: An extensive search through various scholarly databases has revealed that prior to this study, there was no conceptual model to guide corporate South Africa in the implementation of cybersecurity within the broader framework of the law. The proposed conceptual model combines legal requirements and cybersecurity operational needs in a single model. The study adopted a hypothetical company to demonstrate how the proposed model can be implemented in a corporate environment. Qualitative research was conducted, using in-depth interviews and document analysis as data collection techniques. Forty-five local organisations were purposively included in the study. Analysis of the data showed that organisations are not abreast of cybersecurity policies. Most cybersecurity practitioners are not familiar with the legal and policy aspects that they must adhere to when implementing cybersecurity, therefore most organisations do comply with the law in South Africa. The study proposed a conceptual model that can be implemented in real companies, irrespective of their governance and management structures, to improve the provision of the cybersecurity.

Keywords: Cybersecurity conceptual model, Corporate governance, Legal compliance, Policies

1. Introduction

While many South African organisations have adopted digital business transactions, they are not immune to risks, threats and crime owing to their inadequate integration and implementation of cybersecurity measures (Dagada, 2024a). Research shows that companies that succeed in digital commerce are those that implement cybersecurity policies (Saar & Dagada, 2024a). However, the internet revolution is developing so rapidly that it remains a challenge to most organisations to remain abreast of developments (Diamandis & Kotler, 2020).

In many organisations, there is a general trend to attach low probability to information and communications technology (ICT) risks and data disaster occurrence (Dagada & Eloff, 2013; Dagada, 2021). The reality is that ICT infrastructure is a high risk in itself that could lead to the loss of data, information and business intelligence (Chaka, 2023). Organisations cannot continue to perceive the establishment of cybersecurity policies, an ICT risk management framework and the implementation thereof as costly overheads that need to be downscaled.

According to Saar and Dagada (2024b), cybersecurity policy is meant to inform all individuals in an organisation about expected actions in relation to security issues involving ICT information. In some settings, cybersecurity policies are drafted to meet regulatory requirements (Dagada, 2024a), but merely drafting such policies for the sake of satisfying regulatory obligations is not good enough (Mailwald, 2004).

Literature in South Africa depicts the operational necessity and legislation requirements of the integration of legal aspects into cybersecurity policies in various companies (Dagada, 2024b; Dagada & Eloff, 2013; Armstrong & Lee, 2023). The evidence shows that prior to this study, there was no conceptual model to guide corporate South Africa in implementing cybersecurity within the broader framework of the law. By presenting a proposed conceptual model, this study synthesises legal requirements and cybersecurity operational necessities into a single model. It contributes to the body of cybersecurity theory.

The proposed model incorporates legal requirements with cybersecurity endeavours, including policy formulation and implementation, a risk management framework, and monitoring and evaluation. This model should be seen as a combination of theory, practice and cognitive perspectives gained over the author's years of research and practical experience. The model is the researcher's conceptualisation of a framework that could guide organisations in the country in implementing cybersecurity in their operations.

2. Research Design Issues and Context

Briefly, the aim of the study was to assess how South African companies integrate legal and policy aspects when dealing with cybersecurity issues. In the study, a qualitative research approach using semi-structured interviews as well as document and web analyses was used for data gathering.

Forty-five organisations from different industrial sectors in South Africa participated in the study. Analysis of the data showed that there was little participation by organisations in the provision of the cybersecurity policies. It further showed that many cybersecurity practitioners are not familiar with the legal and policy aspects that they are supposed to integrate into the implementation of cybersecurity.

This means many organisations are not complying with the law. A meta-analysis of the study revealed that both the government and corporate South Africa were not implementing some of the legal requirements pertaining to cybersecurity. It is hoped that the proposed model proves to be useful to policymakers, directors of boards, ICT executives and cybersecurity practitioners when incorporating legal requirements in their policy formulation.

It has already been stated that the proposed conceptual model combines theory and the author's extensive experience (as an academic and senior ICT manager) and cognitive perspectives gained over many years. It should be noted that this study was a product of an interplay between the researcher's ontological position and empirical findings. The researcher's perspective has influenced the research methodology employed in the study and, by implication, the findings of the study and the conceptual model. The model was necessitated by the main findings of the study.

To demonstrate how the proposed model can be implemented in a corporate environment, the study adopted a hypothetical company named Aifheli Group in which the model would be implemented. Aspects related to the model are real, while the descriptions of the phantom company are fictitious, but of significance for illustration purposes.

As part of illustrating how the conceptual model can be implemented, the researcher has dealt with macro and micro aspects of the organisational implementation of the conceptual model of legal compliance to cybersecurity law in the corporate environment. The macro-organisational initiatives are the foundation for the actual implementation of the concept model. These include:

- the establishment and implementation of the ICT enterprise architecture; and
- the implementation of the ICT governance structures.

At micro level, the study demonstrates components of the concept model and roles played by:

- the Board of Directors;
- the Group ICT Steering Committee
- the Group ICT Management Committee;
- the Board of Directors' Audit Committee; and
- all employees involved in the formulation, implementation, monitoring and evaluation of cybersecurity policies.

The proposed conceptual model presents a structured organisation that is generic in its disposition, is product independent and will cater for both sides of cybersecurity practice, namely governance and operations.

3. Aifheli Group of Companies

Aifheli Group of Companies (hereafter Aifheli or the group) has four entities (companies), as follows: Aifheli Mines, Aifheli SHERQ (Quality, Safety, Health, and Environment) Solutions, Aifheli HRD (Human Resources Development) Services, and Aifheli Autocatalytic Converter Solutions. See Figure 1.

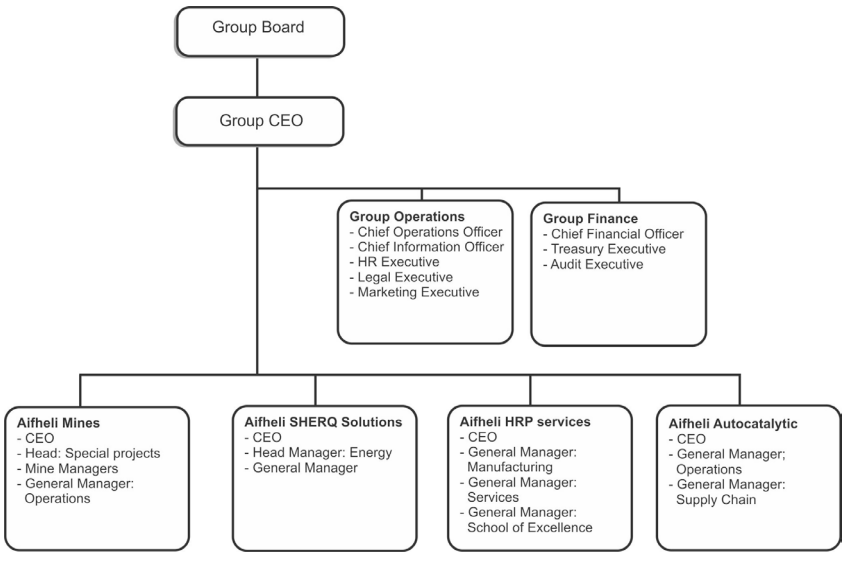

Figure 1: Diagrammatical representation of the structures of Aifheli Group of Companies

4. The Proposed Model of Legal Compliance

The conceptual model will be implemented on macro and micro levels. A major difference between macro and micro model implementations is that the macro level deals with overall information and communications technology (ICT) governance issues, while at the micro level, the focus is specifically on the integration of legal aspects into cybersecurity policies and the implementation thereof.

4.1 Macro-Organisational Model Implementation

The proposed model cannot be implemented in a vacuum and thus certain ICT macro-organisational initiatives should happen before the actual implementation. The aforesaid macro-organisational issues include the establishment and implementation of the ICT enterprise architecture, and the implementation of the ICT governance structures.

4.1.1 Establishment and implementation of the ICT enterprise architecture

A major concern emerging in the international environment, and in South Africa in particular, is that ICT has become disconnected from the business in more ways than one and is thus losing touch with the core activities (Dagada, 2024b).

The major causal factor is that when major institutions evolve and restructure, they temporarily tend to lose focus. This may result in support functions like ICT assuming a corporate life of their own without necessarily being aligned to the core business of the organisation. The disconnection between ICT and the business can be resolved by establishing an enterprise architecture as part of implementing the proposed conceptual model of legal compliance for cybersecurity in the group.

Aifheli should establish an enterprise architecture that would provide an organisational model for the deployment of ICT in the company. This enterprise architecture should articulate the required ICT infrastructure and its role in business processes.

In this instance, ICT should not only be seen as a support function, but also play a major role in the core business of the organisation. The enterprise architecture should recognise the crucial role of the technology user in the various group entities in the implementation and the overall management of the ICT infrastructure and applications. The provision of ICT should nevertheless be aligned with national and international best practices.

4.1.2 Establishment and Implementation of the ICT Governance Structures

As part of implementing the proposed conceptual model of legal compliance for cybersecurity in the corporate environment, it is suggested that Aifheli should have a five-tier ICT governance structure at the macro-level.

Board of Directors

The board of directors (hereafter "the board") is the highest level of governance in any company. The board also has fiduciary responsibilities. Between the shareholders' annual general meetings (AGMs) of any organisation, the board is the uppermost governance structure. This statement is in line with the provisions of the Companies Amendment Act 16 of 2024 and the King Report IV on Governance for South Africa (2016) (commonly known as and hereafter: King IV Report, 2016).

According to the Companies Amendment Act 16 of 2024, the duties of directors include both fiduciary responsibility and duty of reasonable care. The implication is that the business and activities of an organisation should be conducted under the management or direction of the board in accordance with the powers and authority provided by the aforesaid Act, common law and other relevant legislation. In line with the top–down approach, the board will make certain broad ICT pronouncements or policy directives that should be established and implemented at an operational level.

According to this study, the board should have five subcommittees, namely the audit, nomination and compensation, corporate governance, investment, and sustainable development subcommittees. Each of these subcommittees should play certain roles in ICT governance.

Group ICT Steering Committee

This group ICT steering committee should be constituted by all members of the executive committee of the organisation. In the context of Aifheli, the group ICT steering committee includes the following members: the group CEO, group chief operations officer (COO), group chief financial officer (CFO), group CIO, and the CEOs of

the group's four entities. The group ICT steering committee should be chaired by the group CEO; and an independent advisor should be appointed to advise the committee. The purpose of this committee is to:

- ensure that the ICT systems and infrastructure are in place to support the board in the execution of its responsibilities in terms of good corporate governance, accountability, and business performance;
- ensure that the ICT strategy and all major ICT initiatives are aligned with the company's business goals and success metrics;
- deal with ICT-related matters as per the board's directives;
- identify ICT priorities against the broad goals of the group and with the advice from the CEOs of the four entities in Aifheli;
- pay attention to the ICT-related risks and governance issues;
- consider the reports from the group CIO on the performance of the ICT function and budgets;
- determine the impact of ICT systems and infrastructure on business processes and performance; assume the highest-level governance role in projects; and consider reports on all projects and ICT initiatives in the group;
- identify major strategic directions and matters with regard to the company's needs in terms of ICT;
- determine, based on proposals presented by the group CIO, the ICT policy framework, and formulate and review the group ICT programme in relation to all rolling capital projects underpinning the shared services and the core business of the company.

The steering committee should meet every second month.

Group ICT Operations Committee (OpsCom)

OpsCom members must include the four CEOs and two general managers from each of the four group entities, the group CIO and the Group COO. OpsCom should be chaired by the Group COO and should meet once per month. The main purpose of OpsCom is to determine the ICT needs of the group entities, identify gridlocks in business processes and ensure the effective coordination of the ICT rollout across the entire group.

OpsCom should also establish action plans to promote the role of ICT in improving operations and pay attention to its risks. Appropriate attention should be paid to the deployment of ICT systems and infrastructure, and the determination of proper controls to be maintained by each entity throughout the decentralised ICT systems.

ICT Entity Committees

Each of the entities should have its own ICT committee chaired by its CEO. The chairperson should serve on OpsCom. The entity committee should be the main platform where the voices of users are heard regarding ICT issues in the group. The committee should submit ICT reports to OpsCom, reflecting each entity's needs and concerns. Other responsibilities of the committee should be to:

- serve as a platform for the departments in the entity where information about operational issues and how ICT can be an enabler is shared;
- align the entity ICT activities to optimise ICT and determine the alignment with the group enterprise architecture;
- assess the quality of ICT services on a quarterly basis and recommend service levels to OpsCom;
- provide input to OpsCom regarding to the crafting and implementation of ICT plans and policies;
- monitor ICT-related risks in the entity;
- serve as a safety vehicle to ensure that ICT-related operations are monitored and that interventions can be made before crises arise; and
- coordinate the entity's ICT activities, and forward issues of interest and concern to the OpsCom.

The ICT entity committee should bring matters of concern and interest to the attention of the group ICT management committee.

Group ICT Management Committee

The group ICT management committee should be chaired by the group CIO. The proposed organisational structure of Aifheli's group ICT management includes the group CIO; senior members of the office of the CIO (finance manager, programmes manager, project manager and an independent advisor); and heads of strategy and governance, user support, infrastructure and systems solutions, and enterprise information architecture. The purpose of the group ICT management committee is to:

- align the ICT strategy with the overall company's strategy; implement enterprise-wide best practices and monitor trends globally, nationally and in the group;
- ensure that ICT initiatives are linked with business priorities;
- assume overall responsibility for the selection, procurement, deployment, support, and maintenance of infrastructure and systems;
- make sure that all ICT initiatives have clear business objectives and success metrics; conduct regular monitoring of the ICT skills of employees on behalf of the entities and the group;
- make recommendations to the group ICT steering committee about the alignment of ICT investments and the strategic initiatives and operational needs of the entities and shared services;
- make recommendations to the group ICT steering committee to approve the implementation of large-scale ICT programmes and projects;
- establish and deploy a consolidated ICT service delivery model;
- establish and maintain an ICT disaster recovery and business continuation plan and procedure;
- establish and implement ICT policies;
- establish and implement ICT standards;
- establish and implement ICT procedures;
- establish and implement an ICT risk management framework; and
- operationalise and implement decisions taken through approved recommendations and directives from other governance structures.

4.2 Micro-Organisational Model Implementation

According to the King IV Report (2016), enterprise strategic planning, risk management and cybersecurity are the primary responsibilities of the board. It should make broader pronouncements in the business strategic direction and sustainability, corporate governance, standards and legislation framework. Other parties (components of the model) that play a role in the formulation, implementation, monitoring and evaluation are the board, the group ICT steering committee, the group ICT management committee and the whole organisation. Figure 2 illustrates the placement of each governance structure in the process of integrating legal aspects in cybersecurity policies and their implementation, and the interface between the governance structures.

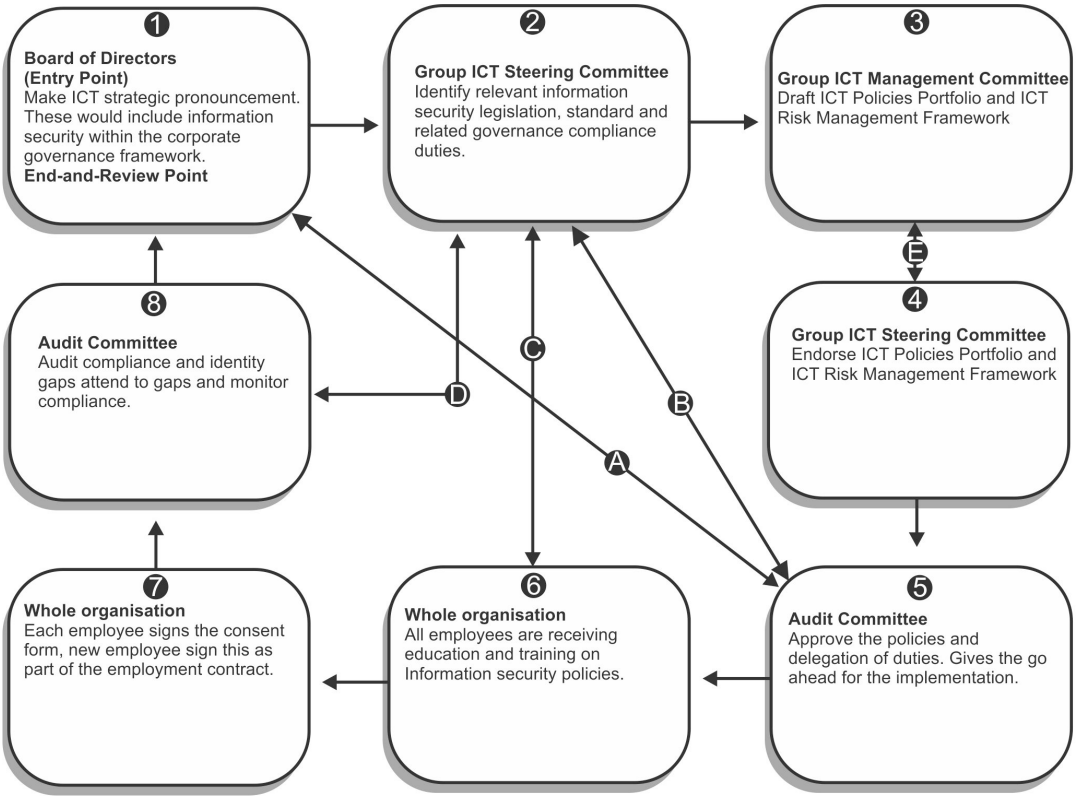

Figure 2: Diagrammatical representation of Concept Model of Legal Compliance for Cybersecurity at Corporate Environment (Source: Author's own)

Arrows A, B, C and D in the figure show that, in some instances, while following the steps of the model, collaboration and/or consultation may be direct between the highest and lowest levels/steps. For instance, arrow A shows that the board's subcommittee on risk management, which plays a role in step 5, may consult directly with the board, which is responsible for step 1.

The King IV Report (2016) and Companies Amendment Act 16 of 2024 require that a public company like Aifheli should have a board as the highest governance structure in the company.

The board (1) may have committees that serve as working groups focusing on specific governance areas. It is suggested that relevant cybersecurity and related compliance duties should be identified at this level. Once this has been done, the next governance structure is the group ICT management committee. The chairperson of this committee, that is the group CIO, should serve on both the group ICT steering committee (2) and the board as one of the members of the executive committee. This would enable the group CIO to translate the identified cybersecurity legal provisions, requirements and related compliance duties into cybersecurity policies. The drafted cybersecurity policies are then taken by the group ICT management committee (3) to the group ICT steering committee (4) for consideration and comment. The group ICT steering committee is responsible for allocating duties to the business units and/or individual positions. The policies are then taken to the board's subcommittee on risk management (5) for their approval. All employees (6) must then be trained on the cybersecurity policies. They are also asked to sign an employee acceptance form and the employee interception consent (7). The audit committee (8) assesses compliance and identify gaps. Thus, the overall intention of the model is to integrate legal aspects into the formulation, implementation, monitoring and evaluation of cybersecurity policies to elevate the benefits of business security and ultimately address corporate security lapses.

4.3 Components of the Model

4.3.1 Board of directors gives directives on ICT policies

ICT plays an important role in the functioning of a company, which is why its failure can threaten the sustainability of the organisation (Dagada, 2021). The board must therefore articulate broad ICT policy directives. The board does not need to get involved in the technical details of such pronouncements.

In its endeavour to conform with legislation, the board should be familiar with ICT risks as outlined in the King IV Report (2016) and by Buys Attorneys (2006): liability, risk or harm resulting from employees' abuse of electronic communication; risk resulting from a website and/or digital commerce; risk resulting from theft of ICT equipment; risk resulting from software risk; and risk presented by the failure of the board and/or company executives to deal with cybersecurity breaches.

The King IV Report (2016) and the Companies Amendment Act 16 of 2024 explicitly state that risk management is the board's responsibilities. Company management is accountable to the board for crafting, implementing and monitoring ICT policies in general and cybersecurity policies in particular. Owing to the pervasiveness and the critical role of ICT in the running of the company, part of the responsibilities of the board is to educate and acquaint themselves with ICT risks and how they can be mitigated by integrating legal aspects into cybersecurity policies.

It is the responsibility of the board and its various committees to ensure that the group complies with the legislation of the country. Note, however, that there are several pieces of legislation that have a direct impact on the manner in which cybersecurity policies should be crafted and implemented; also see Table 1.

Table 1: Synopsis of ICT Policies Portfolio

AREA OF CYBERSECURIT	RELEVANT POLICY	RELEVANT LEGISLATION
1) Hacking	• Cybersecurity Policy • Data Privacy Policy • Access to Cybersecurity Policy • Interception and Surveillance Policy • Records Management Policy • Digital Business Policy •	• Cybercrimes Act 19 of 2020 • Protection of Personal Information Act 4 of 2013 • Electronic Communications and Transactions Act 25 of 2002 • Regulation of Interception of Communications and Provision of Communication-related Matters Act 70 of 2002

AREA OF CYBERSECURIT	RELEVANT POLICY	RELEVANT LEGISLATION
2) Intellectual Property and Copyright	• Intellectual Property Policy • Cybersecurity Policy • Data Privacy Policy • Plagiarism Policy • Records Management Policy	• Intellectual Property Law Amendment Act 38 of 1997 • Copyright Act 98 of 1978 • Merchandise Marks Act 17 of 1941 • Films and Publications Act 65 of 1996 • National Archives and Records Service of South Africa Act 43 of 1996
3) Protection of trademarks	• Intellectual Property Policy • Digital Business Policy	• Intellectual Property Law Amendment Act 38 of 1997 • Copyright Act 98 of 1978 • Merchandise Marks Act 17 of 1941
4) Privacy	• Data Privacy Policy • ICT Acceptable Use Policy • Electronic Communications Policy • Interception and Surveillance Policy	• Constitution of the Republic of South Africa, 1996 • Protection of Personal Information Act 4 of 2013 •
5) Patents protection	• During the fieldwork, the researcher found that no organisation had a distinguishing policy on patent rights	• Patents Act 57 of 1978 • Common law • Intellectual Property Rights from Publicly Financed Research and Development Act 51 of 2008

The board may require the group CEO to ensure that the following areas of cybersecurity are addressed in terms of policy implementation: hacking; intellectual property; copyright; protection of trademarks; privacy; and patents protection.

4.3.2 Group ICT steering committee

This committee identifies cybersecurity areas and instructs the ICT management committee to establish an ICT governance portfolio. Almost all members of the group ICT steering committee serve on the board as executive directors, and thus the provisions of the Companies Amendment Act 16 of 2024 and the King IV Report (2016) on directors' responsibilities and liabilities are applicable to them. Directors' new liabilities according to the Companies Amendment Act 16 of 2024 equate the responsibilities of South Africa's executives with those of their counterparts in the United States of America, who have to contend with the governance and reporting responsibilities contained in the Sarbanes–Oxley Act of 2002, a United States federal law.

In reality, the Group ICT Steering Committee is actually the group executive, but in this instance the agendas of their meetings only focus on ICT-related matters. Once the board issues certain policy directives, it is the responsibility of the group ICT steering committee to delegate the actualisation of these directives to individuals and/or structures. In this instance, the group ICT steering committee will delegate the responsibility of crafting cybersecurity policies to the group CIO and the group ICT management committee.

4.3.3 Group ICT management committee

This committee has to unpack and put in place the details of the mandate from the group ICT steering committee by delving into the establishment of the ICT governance portfolio. The committee should be sensitive to the fact that ICT governance is a critical component of effective ICT strategies and functions. It is on this basis that ICT governance should be documented and communicated to the group to enable full implementation and compliance. A critical element of ICT governance is accountability in terms of cybersecurity. On the other hand, the group ICT management committee should ensure that ICT functions meet the requirements of a framework of policies and legal aspects.

A lack of policies that integrate legal aspects hinders the structured growth of the ICT function in the group and threatens its sustainability as the organisation would not be operating in a normalised operating environment. ICT governance should not solely be based on policies integrating different policy aspects – the group also needs to establish operating standards, identify operational risks, and be cognisant of the whole notion of quality management and alignment with the critical success factors for ICT initiatives (vision, people, process, and

technology). However, this study focuses only on the cybersecurity policies portfolio and the risk management framework.

4.3.4 Establishment of an ICT Policies Portfolio

The group ICT management committee should acknowledge that many pieces of legislation compel all organisations in South Africa, regardless of the method and form of their incorporation or founding, to comply with the provisions of legislation on the implementation of cybersecurity. This requirement is applicable to all companies as defined by the Companies Amendment Act 16 of 2024, that is for-profit companies (state-owned, private, personal liability and public companies) and not-for-profit companies.

Then again, the King IV Report (2016) argues that cybersecurity is a critical component of the whole business *and* its sustainability, and thus companies should address cybersecurity by addressing confidentiality, integrity and availability.

The group ICT management committee should also take into account that ICT policies integrating legal aspects of cybersecurity play an important role in corporate ICT governance as they guide the group position on more matters than only ICT operations. This is because ICT permeates the company at all levels and facilitates the flow of business processes.

Owing to the pervasive nature of ICT, employees' work tends to revolve around ICT. However, cybersecurity and its relevant pieces of legislation are generally neglected, which leads to corporate non-compliance. To avoid this, the group ICT management committee must establish an ICT policies portfolio by aligning information aspects with the relevant policies and legislation. Table 1 illustrates the aforementioned recommendation.

4.3.5 Establishment of an ICT risk management framework

ICT is pervasive throughout a group – it facilitates not only business processes, but also the group's relationships with its suppliers and customers. Therefore the group ICT management committee should establish measures to mitigate cybersecurity threats. These measures should align with the established ICT portfolio. In essence, the best way to counteract ICT threats is to implement approved policies. At face value, the point the researcher is making sounds obvious, but practically it is not so apparent.

During the fieldwork done for this study, the researcher came across some companies that had well-crafted policies which were never implemented, which meant that there was a huge disjuncture between cybersecurity policies and their actual implementation. The proposed ICT risk management framework should include standards, procedures and quality management measures.

4.3.6 Group ICT Steering Committee Endorsement Of Policies Portfolio And Risk Management Framework

If for any reason the group ICT steering committee does not endorse the policies portfolio and risk management framework, they should be returned to the group ICT management committee for refinement. However, once the ICT policies portfolio and ICT risk management framework have been endorsed by the group ICT steering committee, the group CEO should submit them on behalf of the group ICT steering committee to the audit committee for approval.

4.3.7 Board of Directors' audit committee approves policies and risk management framework

The audit committee should ensure that the ICT policies portfolio and ICT risk management framework that have been endorsed by the group ICT steering committee do not leave loopholes that could compromise the performance and sustainability of the organisation. The audit committee should satisfy itself that measures to deal with ICT security risks are integrated into the overall company strategy, and that various cybersecurity policies are aligned with this strategy. Furthermore, cybersecurity policies should integrate relevant legislation provisions. The audit committee should also ensure that ICT-related risks and security threats are identified and mitigated. The audit committee should appoint an independent ICT law firm or auditing company to assess their cybersecurity policies and advise the committee.

4.3.8 Group human resources conducts employees training

When formulating a corporate cybersecurity training programme, group human resources should take into consideration that ICT systems are dependent on employees. Dagada (2024a) argues that cybersecurity is more about people's behaviour than anything else. Despite the marketing line from ICT suppliers about the necessity of cybersecurity technology, many essential security actions cannot be automated and thus rely on correct usage

by employees. This means that companies rely on employees to attain a secure ICT environment. As humans are the weakest link in the security chain, group human resources must make sure that staff members are properly trained on the correct implementation of and compliance with cybersecurity policies.

4.3.9 All Employees Accept Cybersecurity Policies by Signing Consent Forms

Once the awareness and training programmes have been implemented, each staff member should sign the consent form and employee interception consent to ensure that employees will adhere to the principles of good corporate governance and network safety and security. The aim is to ensure a secure and healthy working environment. The consent form will enable the company to monitor employees' usage of group ICT systems when necessary.

The company should take into consideration that employees in South Africa have the constitutional right to privacy; consent forms enable a company to balance cybersecurity objectives and compliance with the Constitution of the Republic of South Africa, 1996.

4.3.10 The audit committee audits adherence to the cybersecurity policies

Following policy implementation, the group ICT committee should constantly monitor cybersecurity legal compliance. However, the actual audit of compliance should be done by the audit committee on behalf of the board of directors. It is advisable for the audit committee to get independent external assistance when carrying out the audit. The audit should look at compliance by employees as well as ICT infrastructure and systems.

According to Saar and Dagada (2024a), employees' compliance with policies can be determined by observing their behaviours and attitudes, for example by conducting password cracking; interviewing informally to obtain anecdotal evidence; and conducting clean desk audits. Audit committee should also audit the ICT infrastructure and systems to ascertain whether they satisfy the requirements of cybersecurity policies and the established risk management framework. Also note that backups are very important for mitigating ICT risks and cybersecurity threats, thus they too should be audited.

5. Conclusion

The significant point drawn from this study is that the governance aspect of ICTs should be taken seriously by the board and other governance structures, and should not continue to be given lower priority owing to its technical nature. Serious attention must be paid to the alignment of the ICT strategy with the overall business strategy and the impact of ICT on the sustainability of the Like any other business function, ICT is vulnerable to failure and should comply with the good corporate governance provisions of the King IV Report (2016).

The management of ICT must comply with responsible governance practices. Inadequate ICT security measures or the lack of such measures constitutes poor corporate governance; hence, the board should pay attention to this. An independent audit committee should audit the organisation's ICT infrastructure and systems to ensure that ICT-related policies are well crafted and implemented to mitigate cybersecurity risks. According to the proposed model, the process of establishing cybersecurity policies should be initiated by the board, up to the auditing and review stages.

The proposed conceptual model can be implemented in all companies, no matter which governance and management structures they have. The model is offered conceptually as it may not be implementable without its conceptual representation. The conceptual model was developed by integrating two traditionally exclusive concepts – cybersecurity and legislation.

References

Armstrong, B. & Lee, G.J. (2023). Digital transformation maturity. Johannesburg: Silk Route Press.

Buys Attorneys. (2006). ICT risk checklist with legal, IT and corporate governance solutions (2nd ed). Cape Town: Buys Inc. Attorneys.

Chaka, C. (2023). "Fourth industrial revolution: a review of applications, prospects, and challenges for artificial intelligence, robotics and blockchain in higher education." Research and Practice in Technology Enhanced Learning, 18(2):1-39. https://doi.org/10.58459/rptel.2023.18002

Dagada, R. (2021). Digital commerce governance in South Africa. Pretoria: UNISA Press.

Dagada, R. (2024a). Will employees and technology continue to coexist despite historic tensions? Available at: https://unisapressjournals.co.za/index.php/AJER/article/view/13466 (accessed on 7 February 2024).

Dagada, R. (2024b). The advancement of 4IR technologies and increasing cyberattacks in South Africa. Available at: https://unisapressjournals.co.za/index.php/sajs/article/view/15157 (accessed on 7 February 2025).

Dagada, R. & Eloff, M. (2013). Integration of policy aspects into information security issues in South African organisations. African Journal of Business Management, 7(31):3069–3077.

Diamandis, P.H. & Kotler, S. (2020). The future is faster than you think: How converging technologies are transforming business, industries, and our lives. New York: Simon & Schuster.

King Report IV on Governance for South Africa. (2016). Johannesburg: Institute of Directors Southern Africa.

Maiwald, E. (2004). Fundamentals of network security. New York: McGraw-Hill Technology Education.

Saar, G. & Dagada, R. (2024a). Building cybersecurity capacities in Zambia's business sector: guideline for SMEs. Proceedings of 19th International Conference on Cyber Warfare and Security, 19(1):317–326, 26–27 March 2024. University of Johannesburg. DOI: https://doi.org/10.34190/iccws.19.1.2051.

Saar, G. & Dagada, R. (2024b). Securing Zambia's business future: cybersecurity guidelines for SMEs. Journal of Information Warfare, 23(3):1–16.